АКАДЕМИК ОРДЕНОНОСЕЦ
Д. А. ГРАВЕ
ЗАСЛУЖЕННЫЙ ДЕЯТЕЛЬ НАУКИ

ТРАКТАТ ПО АЛГЕБРАИЧЕСКОМУ АНАЛИЗУ

ТОМ ПЕРВЫЙ

НАЧАЛА НАУКИ

ИЗДАТЕЛЬСТВО АКАДЕМИИ НАУК УССР
КИЕВ — 1938

АКАДЕМИЯ НАУК СССР
ІНСТИТУТ МАТЕМАТИКИ

АКАДЕМИК ОРДЕНОНОСЕЦ
Д. А. ГРАВЕ
ЗАСЛУЖЕННЫЙ ДЕЯТЕЛЬ НАУКИ

ТРАКТАТ ПО АЛГЕБРАИЧЕСКОМУ АНАЛИЗУ

ТОМ ПЕРВЫЙ

НАЧАЛА НАУКИ

ИЗДАТЕЛЬСТВО УКРАИНСКОЙ АКАДЕМИИ НАУК
КИЕВ — 1938

Библиографическое описание этого издания помещено в „Летописи украинской печати", „Карточном репертуаре" и других указателях Украинской книжной палаты.

Ответственный редактор *К. А. Бреус*

Литредактор и корректор *І. М. Коган* Выпускающий *Е. Ц. Каганов*

Типо-литография Академии Наук УССР, Киев

Настоящая книга является первым томом задуманного мною большого трактата по Алгебраическому Анализу.

Алгебраический анализ я понимаю не в устаревшем смысле слова, как науки о решении уравнений высших степеней, а в более широком смысле слова, как, если так можно выразиться, классическую математику, проходящую мощным потоком через всю историю науки, от древних времен до наших дней.

Понимаемая в этом смысле классическая математика вызвала к жизни следующие дисциплины:

1. Арифметику древних.
2. Классическую теорию чисел.
3. Высшую алгебру.
4. Теорию групп.
5. Теорию Галуа.
6. Алгебраические функции и числа.
7. Абелевы интегралы.
8. Классические трансцендентные функции.
9. Высшую теорию чисел в связи с идеальными числами.
10. Группы непрерывные.
11. Приложение обобщенной теории Галуа к линейным диференциальным уравнениям.

Возможно, что ввиду моего преклонного возраста моей жизни не хватит для выполнения полностью всей программы, но я надеюсь, что мои ученики доведут начатое дело до конца.

15. X 1937.

Д. Граве

ОБОБЩЕНИЕ ПОНЯТИЯ О ЧИСЛЕ

§ 1. Основой всей математики являются *числа натуральные*, образующие бесконечный ряд:

$$1,\ 2,\ 3,\ 4,\ 5, \ldots$$

и являющиеся результатом простого счета предметов.

Уже на самых первоначальных стадиях развития математики было ясно, что эти числа не достаточны для решения практических задач. Математика пошла по пути *обобщения понятия о числе*. Кроме чисел натуральных стали еще называть числами новые предметы.

§ 2. Первым по времени обобщением явились *числа дробные* или просто — *дроби*, как их называют в арифметике.

Эти часла имеют вид

$$\frac{m}{n}$$

где m и n числа натуральные. Число m носит название *числителя дроби*, а n — *ее знаменателя*.

При дробных числах обнаруживается новый факт, что представление дробного числа при помощи дроби *не однозначно*.

Например

$$\frac{3}{2}=\frac{6}{4}=\frac{9}{6}=\frac{12}{8}=\ldots$$

Поэтому мы различаем понятие о дробном числе и понятие о соответствующей ему дроби.

Дробные числа вводятся для того, чтобы сделать возможным всегда деление одного натурального числа на всякое другое.

Напр., от деления числа 5 на число 3 получается дробь $\frac{5}{3}$.

§ 3. Вторым обобщением явились числа *отрицательные*:

$$-3, -\frac{2}{5},$$

вводимые обыкновенно в началах алгебры. Отрицательные числа вводятся для того, чтобы сделать возможными вычитание большего числа из меньшего.

Например, если вычесть 5 из 3, то получится -2.

§ 4. Совокупность чисел натуральных

$$1, 2, 3, 4, \ldots$$

по своему отношению к первым четырем арифметическим действиям: сложения, вычитания, умножения, деления подходит под понятие, которое называется в настоящее время рингом (кольцом) чисел.

Рингом называется такая совокупность чисел, которые воспроизводятся через действия, которые мы будем называть сложением и умножением.

Что это значит, что числа воспроизводятся? Это значит, что каковы бы ни были два элемента a, b ринга, то их сумма $a+b$ и произведение ab представляют элемент того же ринга.

Этого мало. Действия над элементами ринга должны удовлетворять известным свойствам, которые можно назвать законами действий ринга.

Эти законы суть:

I. Законы сложения:

1) ассоциативный закон $a+(b+c)=(a+b)+c$

2) коммутативный закон $a+b=b+a$.

II. Закон умножения:

1) ассоциативный закон $a(bc)=(ab)c$.

III. Распределительные законы:

1) $a(b+c)=ab+ac$

2) $(b+c)a=ba+ca$

и еще дополнительный закон:

Коммутативный закон умножения.

$$ab=ba$$

Если этот последний закон существует, то ринг называется коммутативным.

§ 5. Рассмотрим теперь отношение ринга к обратным действиям деления и вычитания.

Действие деления не применимо к рингу 1, 2, 3, 4, ..., потому что, если мы возьмем, например, элементы 5 и 3, то деление одного на другое даст дробное число $\frac{5}{3}$, которое не принадлежит к элементам ринга.

Если мы желаем ринг пополнить числами, так чтобы действие деления сделалось возможным, то мы должны к рингу присоединить все дробные числа. Если мы в ринге будем предполагать число 0, то оно даст единственное исключение, ибо на него делить нельзя.

Подобным образом если мы присоединим отрицательные числа $-a, -\frac{c}{d}$, то действие вычитания сделается всегда возможным.

Такое пополнение ринга натуральных чисел числами дробными и отрицательными приводит нас к совокупности чисел, которую мы будем называть полем*) (Körper), областью рациональности.

Мы пришли, таким образом, к простейшему полю R, к полю так называемых рациональных чисел. Элементами этого поля являются взятые с тем или другим знаком числа целые или арифметические дроби, числители и знаменатели которых суть числа целые. К полю принадлежит также нуль, который является границей между положительными и отрицательными числами.

Понятие о поле подлежит широким обобщениям. Могут существовать поля, элементы которых—не числа рациональные, и даже более того, могут существовать поля, элементы которых суть не числа, а предметы другой природы. Если дело идет о нечисловых полях, то для элементов таких полей надо установить действия, которые надо назвать действиями сложения, вычитания, умножения и деления. Для того чтобы можно было назвать совокупность таких предметов полем, необходимо, чтобы действия удовлетворяли формальным законам, изложенным в § 4, причем надо добавить только закон о действии деления.

Обобщенные поля рассматривал серьезно Steinitz **). Необходимо подчеркнуть, что поле R будет входить как часть во всякое другое поле.

---

*) Термин „поле" введен мною. Есть авторы, которые называют поле корпусом в связи с немецким термином Körper.

**) Есть изданный на русском языке перевод его мемуара о полях в виде отдельной книги.

Пусть, например, мы имеем какое-нибудь более общее числовое поле. Возьмем какой-нибудь отличный от нуля элемент α, тогда в поле должно находиться число $\frac{\alpha}{\alpha}$, т. е. единица. Далее, складывая число 1 сколько угодно раз с самим собой, получим, что в поле должны находиться все натуральные числа, а деление одного натурального числа на другое дает все дроби. Вычитание из нуля полученных чисел дает отрицательные числа. Таким образом, все поле R находится в заданном поле как часть. Ее называют делителем поля.

Сказанное относится также к нечисловым полям, только тогда $\frac{\alpha}{\alpha}=1$ не будет числовой единицей. Но все элементы поля R_1, полученного предыдущим способом, будут между собою относиться как числа поля R. Говорят, что поля R и R_1 изоморфны. В теории полей изоморфные поля считаются равными $R_1=R$.

§ 6. Поле R можно упорядочить с точки зрения понятия больше — меньше.

Если разность $a-b$ положительна, то элемент поля a больше элемента b, что можно выразить знаками:

$$a>b, \quad b<a$$

Далее мы увидим, что поле R можно упорядочить более общим образом. А именно, можно расположить все числа поля в одну последовательность, причем будет точно установлено, который элемент следует за другим.

ЧИСЛА НЕСОИЗМЕРИМЫЕ

§ 7. Числа поля R не могут решать все прикладные задачи; есть потребность ввести еще новые числа, так называемые несоизмеримые или иррациональные.

Потребность в этих числах является с самых начал математики. Например, число

$$\sqrt{2}$$

не есть соизмеримое с единицей.

Соизмеримыми с единицей мы называем дробные числа поля R:

$$\frac{P}{Q}, \tag{1}$$

где P и Q суть целые числа, потому что число (1) имеет с единицей общую меру $\frac{1}{Q}$, которая Q раз заключается в единице $(1 = Q \cdot \frac{1}{Q})$ и P раз в числе (1).

Чтобы доказать, что $\sqrt{2}$ число несоизмеримое, допустим обратное:

$$\sqrt{2} = \frac{P}{Q} = \frac{p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}}{q_1^{\beta_1} q_2^{\beta_2} \ldots q_l^{\beta_l}}, \tag{2}$$

где p_i суть простые множители целого числа P, а q_i простые множители целого числа Q; эта дробь не может сокращаться и обращаться в целое число, ибо $\sqrt{2}$ не может равняться целому числу.

Возведем равенство (2) в квадрат; получим:

$$2 = \frac{p_1^{2\alpha_1} p_2^{2\alpha_2} \ldots p_k^{2\alpha_k}}{q_1^{2\beta_1} q_2^{2\beta_2} \ldots q_l^{2\beta_l}};$$

но новая дробь не может сокращаться и обратиться в целое число 2.

Итак, число $\sqrt{2}$ есть несоизмеримое.

§ 8. Существуют три способа трактовать числа несоизмеримые: 1) способ Дедекинда, 2) способ десятичных дробей, 3) способ Кантора.

Я изложу вкратце все три способа. Способ Дедекинда важен, потому что он основан на мысли знаменитого греческого математика Эвклида. Способ десятичных дробей важен как самый естественный, ибо в математике все числа изображаются десятичными дробями. Наконец, способ Кантора связывается с теорией пределов.

АЛГОРИТМ ЭВКЛИДА

§ 9. В геометрии число является как отношение между отрезками.

Если

$$a = \frac{\overline{AB}}{\overline{CD}},$$

где $\overline{AB}$ и $\overline{CD}$ два отрезка, то если мы принимаем отрезок $\overline{CD}$ за единицу длины, то число a является длиной отрезка $\overline{AB}$.

Нахождение отношения двух отрезков подробно и обстоятельно изложено в бессмертной книге греческого математика Эвклида (2 век до нашей эры) под заглавием Στοίχεια (Начала).

Весьма важно обратить внимание на то, что Эвклид не ограничился рассмотрением отношения двух отрезков, а рассматривал также отношение двух целых чисел и получил замечательное правило для нахождения общего наибольшего делителя двух целых чисел при помощи последовательного деления. Под этим названием правило Эвклида сохранилось в средней школе до настоящего времени.

Начнем с правила, относящегося к целым числам, а потом перейдем к отрезкам.

Пусть заданы два натуральных числа a, b и пусть $a > b$. Делим a на b. Если деление происходит нацело, т. е.

$$a = bq,$$

где q число целое, то очевидно, что b есть общий наибольший делитель двух заданных чисел, так сказать, общая мера этих двух чисел: b заключается один раз в самом себе и q раз в числе a. Вычисление общего наибольшего делителя закончено.

Если деление a на b происходит с остатком r, так что $r < b$, то мы имеем:

$$a = bq + r$$

Очевидно, что общий наибольший делитель чисел a и b будет и общим наибольшим делителем b и r. Тогда продолжаем процесс последовательного деления. Пусть от деления b на r получается частное q_1 и остаток $r_1 < r$:

$$b = rq_1 + r_1$$

Продолжая процесс последовательного деления далее, мы приходим к равенствам:

$$\begin{aligned} a &= bq + r \\ b &= rq_1 + r_1 \\ r &= r_1q_2 + r_2 \\ &\dots\dots\dots \\ r_{n-2} &= r_{n-1}q_n + r_n \end{aligned} \tag{1}$$

Последовательные остатки r, r_1, r_2... следуют убывая. Но целых чисел, меньших r, конечное число, следовательно, наш процесс последовательного деления должен закончиться, и мы приходим к остатку r_n, равному нулю. Тогда, очевидно, предыдущий остаток r_{n-1} должен быть общим наибольшим делителем чисел a и b.

Параллельно мы замечаем, что r_{n-1} будет наибольшим общим делителем каждых двух рядом стоящих остатков

$$r_k, \quad r_{k+1}$$

В математике каждый процесс действий, приводящий окончательно к решению некоторой задачи, называется **алгоритмом**, решающим задачу. Процесс Эвклида есть алгоритм нахождения общего наибольшего делителя.

Равенства (1) можно переписать так:

$$\begin{aligned} \frac{a}{b} &= q + \frac{r}{b} \\ \frac{b}{r} &= q_1 + \frac{r_1}{r} \\ \frac{r}{r_1} &= q_2 + \frac{r_2}{r_1} \\ &\dots\dots \\ \frac{r_{n-2}}{r_{n-1}} &= q_n \quad (r_n = 0) \end{aligned} \tag{2}$$

Равенства (2) приводят к непрерывной дроби

$$\frac{a}{b} = q + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cdots \cdots + \cfrac{1}{q_n}}}$$

Поэтому алгоритм Эвклида носит название также алгоритма **непрерывных дробей**.

Алгоритм непрерывных дробей имеет, конечно, большое практическое значение, например для сокращения дробей. Но его теоретическое значение гораздо выше и выясняется вполне в науке, называемой **теорией чисел**.

ОТНОШЕНИЯ ПО ЭВКЛИДУ

§ 10. Перейдем теперь от чисел к отрезкам.

Пусть a и b длины отрезков, тогда, если $a > b$, мы откладываем на отрезке a отрезок b столько раз q (целое число), чтобы остался отрезок $r < b$.

Тогда, подобно случаю целых чисел, мы приходим к ряду равенств:

$$\begin{aligned} a &= bq + r_1 \\ b &= rq_1 + r_1 \\ r &= r_1 q_2 + r_2 \\ &\ldots\ldots \\ r_{n-2} &= r_{n-1} q_n + r_n \\ &\ldots\ldots\ldots \end{aligned} \tag{1}$$

Здесь q, q_1, $q_2, \ldots$, $q_n, \ldots$ — числа целые, все же остальные буквы обозначают длины отрезков. Остаточные отрезки r, r_1, $r_2, \ldots$, $r_n, \ldots$ убывают. Но *теперь* может существовать бесконечное число отрезков, меньших r. Поэтому нет обязательности, чтобы один из отрезков сделался равным нулю, что бывает лишь в редких случаях, а обычно процесс продолжается до бесконечности. Если случится, что $r_n = 0$, тогда r_{n-1} будет общей мерой двух отрезков. В этом случае отрезки называются *соизмеримыми*. Их отношение, как в случае двух целых чисел, выразится конечною непрерывною дробью, величина которой будет $\frac{P}{Q}$, где P и Q — целые числа.

Соизмеримые с единицей числа называются также *рациональными*.

В случае отсутствия общей меры отношение $\frac{a}{b}$ раскладывается в бесконечную непрерывную дробь:

$$\frac{a}{b} = q + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cdots \cdots + \cfrac{1}{q_n + \cdots}}} \tag{2}$$

В этом случае отношение $\frac{a}{b}$ является числом несоизмеримым или иррациональным.

§ 11. Всякая бесконечная непрерывная дробь (2) § 10, у которой неполные частные q, q_1, q_2, ... — числа целые и положительные, представляет **конечное** иррациональное число.

В самом деле, из элементарной теории непрерывных дробей следует, что подходящие дроби нечетного порядка:

$$q, \quad q+\cfrac{1}{q_1+\cfrac{1}{q_2}}, \quad q+\cfrac{1}{q_1+\cfrac{1}{q_2+\cfrac{1}{q_3+\cfrac{1}{q_4}}}}, \ldots \text{ и т. д.} \tag{1}$$

меньше величины $\frac{a}{b}$ всей непрерывной дроби, а подходящие дроби четного порядка:

$$q+\frac{1}{q_1}, \quad q+\cfrac{1}{q_1+\cfrac{1}{q_2+\cfrac{1}{q_3}}}, \ldots \text{ и т. д.} \tag{2}$$

больше $\frac{a}{b}$. Кроме того числа (1) возрастают и приближаются снизу к величине $\frac{a}{b}$, а числа (2) убывают и приближаются сверху к $\frac{a}{b}$.

Продолжая достаточно далеко числа рядов (1) и (2), получим числа сколь угодно близкие к числу $\frac{a}{b}$.

Итак, мы получаем способ вычислять иррациональное число $\frac{a}{b}$ с какою угодно степенью точности при помощи рациональных чисел (1) или (2).

§ 12. Покажем теперь на одном простом примере случай несоизмеримого отношения.

Покажем, что сторона квадрата $b=AE$ не соизмерима с его диагналью $a=AC$.

Проведем окружность EB из точки A, как из центра, радиусом, равным b, до пересечения с диагональю; таким образом мы откладываем на диагонали отрезок AB, равный стороне квадрата:

$$AC = AB + BC,$$

или

$$a = b + r$$

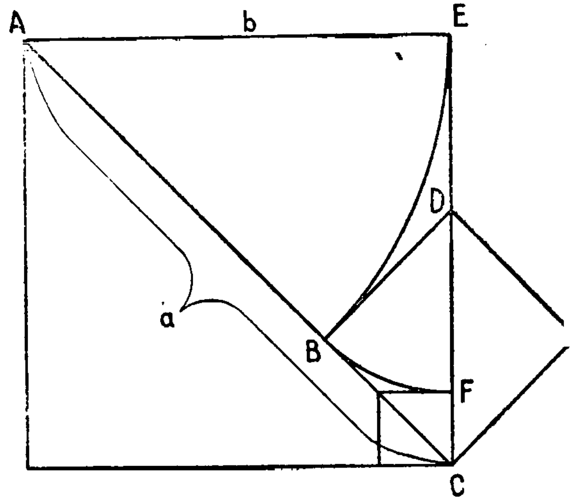

Рис. 1.

Сторона EC касается в точке E проведенного круга; проведем с другого конца дуги EB касательную BD, которая будет перпендикулярна к диагонали. Мы получим другой, меньший квадрат, сторона которого будет $r = BC$. Мы имеем, очевидно,

$$ED = DB = BC$$

Проводим из точки D дугу круга BF радиусом, равным стороне r малого квадрата. Другими словами, мы отложим на диагонали DC малого квадрата его сторону r.

Мы получаем:

$$DC = DF + FC,$$

или

$$CE = ED + DF + FC,$$

т. е.

$$b = 2r + r_1,$$

где $r_1 = FC$.

Продолжая подобные построения для все меньших и меньших квадратов, получим ряд равенств:

$$\begin{aligned} a &= b + r \\ b &= 2r + r_1 \\ r &= 2r_1 + r_2 \\ r_1 &= 2r_2 + r_3 \\ &\cdots\cdots \end{aligned}$$

Этот процесс построения будет бесконечен, ибо существуют все меньшие и меньшие квадраты.

Мы приходим к бесконечной непрерывной дроби с постоянным неполным частным 2:

$$\frac{a}{b} = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cdots \cdots + \cfrac{1}{2 + \cdots}}}$$

Отношение $\frac{a}{b}$ оказывается несоизмеримым. Нетрудно его вычислить. Пусть $\frac{a}{b} = x$, тогда

$$x = 1 + \cfrac{1}{1 + \left\{1 + \cfrac{1}{2 + \cdots} \cdots \right\}} = 1 + \frac{1}{1 + x},$$

откуда

$$x = \sqrt{2}$$

Вычислим теперь приближенно $\sqrt{2}$. Возьмем пятую подходящую дробь:

$$1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2}}}} = \frac{41}{29} = 1{,}413\ldots,$$

а настоящее значение $\sqrt{2} = 1{,}4142\ldots$

Если взять 7-ую подходящую дробь, то получим:

$$\sqrt{2} = \frac{239}{169} = 1{,}414201\ldots$$

ОШИБКА У ДАВЫДОВА

§ 13. Эвклид развил свою теорию отношения отрезков в связи с основной теоремой геометрии, что параллельные прямые отсекают на сторонах угла отрезки пропорциональные.

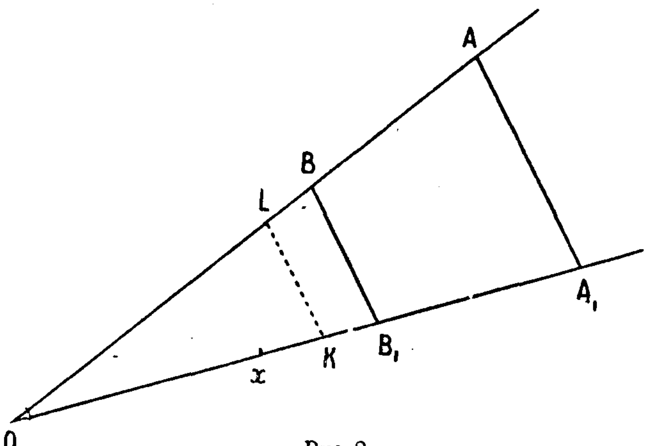

Рис 2.

Мой покойный учитель, профессор Петербургского университета А. Н. Коркин обратил мое внимание на то обстоятельство, что в элементарном курсе геометрии профессора Давыдова при доказательстве теоремы для случая иррациональных отношений допущена довольно грубая ошибка, *которой нет у Эвклида*.

Я воспроизведу доказательство Давыдова.

Доказав теорему для случая соизмеримых отношений, Давыдов переходит к случаю отношений несоизмеримых.

Итак, требуется доказать, что существует пропорция:

$$\frac{AO}{BO} = \frac{A_1O}{B_1O}$$

Давыдов хочет вести доказательство от противного. Он рассуждает так: пусть $\frac{AO}{BO}$ не равно $\frac{A_1O}{B_1O}$. Предположим, что

$$\frac{AO}{BO} > \frac{A_1O}{B_1O}$$

Чтобы достичь пропорциональности, увеличим $\frac{A_1O}{B_1O}$; для этой цели можно, например, уменьшить знаменатель B_1O, заменив точку B_1 на точку x, так что

$$\frac{AO}{BO} = \frac{A_1O}{xO} \tag{1}$$

Разделим линию OA_1 на столь большое число равных частей, чтобы одна из точек деления попала между точками B_1 и x. Пусть это будет точка K. Проведем через точку K прямую KL, параллельную AA_1. Так как отношение $\frac{A_1O}{KO}$ соизмеримо, а теорема для случая соизмеримости доказана, то мы имеем пропорцию

$$\frac{AO}{LO} = \frac{A_1O}{KO} \tag{2}$$

Из (1) и (2) через деление получаем

$$\frac{LO}{BO} = \frac{KO}{xO},$$

что невозможно, ибо

$$\frac{LO}{BO} < 1, \quad \frac{KO}{xO} > 1$$

Порочность этого доказательства состоит в том, что предполагается существование точки x, исправляющей пропорцию. Если же мы предположим, что такой точки не существует, то все доказательство падает.

§ 14. У Эвклида никакой ошибки нет и доказательство самое простое.

Эвклид дает определение пропорциональности четырех величин, которое годится как для соизмеримых, так и для несоизмеримых отношений. Он прилагает это определение к доказательству теоремы, что площади треугольников, имеющих одну и туже высоту, относятся как основания. Когда он установил эту пропорциональность, он переходит к доказательству теоремы. В книге 6-ой „Начал“ мы видим теорему 2-ую такого содержания.

„Если в треугольнике провести прямую, параллельную одной стороне, то она разделит пропорционально две другие стороны, и обратно“.

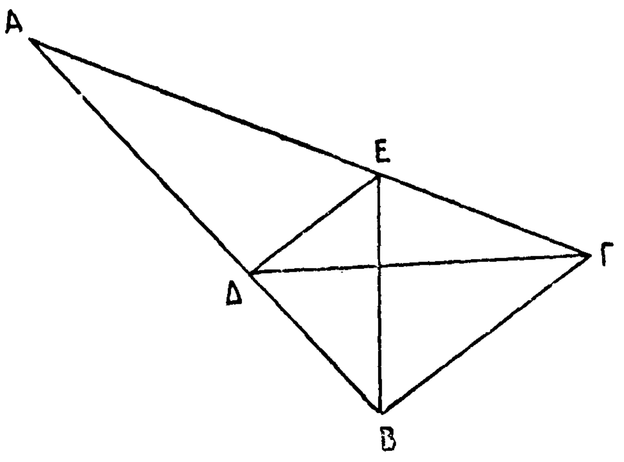

Рис. 3.

На основании доказанной пропорциональности оснований площадям треугольников мы имеем

$$\frac{A\Delta}{\Delta B} = \frac{\text{тр. } A\Delta E}{\text{тр. } \Delta EB}, \quad \frac{AE}{E\Gamma} = \frac{\text{тр. } A\Delta E}{\text{тр. } \Delta E\Gamma},$$

но тр. $\Delta EB =$ тр. $\Delta E\Gamma$, ибо эти треугольники имеют одно и то же основание ΔE, а их вершины Γ и B лежат на прямой $B\Gamma$, параллельной основанию ΔE.

Итак, получаем:

$$\frac{A\Delta}{\Delta B} = \frac{AE}{E\Gamma},$$

что и требовалось доказать.

ОПРЕДЕЛЕНИЕ ПРОПОРЦИОНАЛЬНОСТИ

§ 15. Обращаемся теперь к знаменитому определению Эвклида пропорциональности четырех величин.

Это определение имеет поистине мировой характер, потому что оно в продолжение 2000 лет не подверглось изменению и привело в последнее время к ряду блестящих следствий.

Я приведу это определение в подлиннике и дам его перевод с комментариями. Вот это определение (5-ое определение, 5-ая книга. Издание August'a, Berlin 1826):

ε. Ἐν τῷ αὐτῷ λόγῳ μεγέθη λέγεται εἶναι, πρῶτον πρὸς δεύτερον καὶ τρίτον πρὸς τέταρτον, ὅταν τὰ τοῦ πρώτου καὶ τρίτου ἰσάκις πολλαπλάσια τῶν τοῦ δευτέρου καὶ τετάρτου ἰσάκις πολλαπλασίων καθ' ὁποιονοῦν πολλαπλασιασμὸν ἑκατέρον ἑκατέρου, ἢ ἅμα ὑπερέχῃ, ἢ ἅμα ἴσα ᾖ, ἢ ἅμα ἐλλείπῃ ληφθέντα κατάλληλα.

В переводе:

Говорят, что (четыре) величины имеют одно и то же отношение—первая (a) ко второй (b), как третья (c) к четвертой (d), когда одинаковые кратности первой и третьей (am, cm) относительно одинаковых кратностей второй и четвертой (bn, dn) по произвольной кратности (целые числа m и n произвольны) или одновременно больше ($am > bn$, $cm > dn$), или одновременно равны ($am = bn$, $cm = dn$), или одновременно меньше ($am < bn$, $cm < dn$), т. е. если существуют одновременно неравенства:

$$am \gtreqless bn, \quad cm \gtreqless dn \tag{1}$$

при всяких целых m и n, то существует пропорция:

$$\frac{a}{b} = \frac{c}{d} \tag{2}$$

§ 16. Для доказательства пропорциональности площадей треугольников с одинаковыми высотами их основаниям Эвклид рассуждает так.

Возьмем два треугольника ГВА и ГΔА с одинаковой высотой АГ. Отложим несколько раз основание ВГ, например ВН, НΘ; тогда длина ГΘ будет некоторою кратностью ВГ:

$$\Gamma\Theta = m\,\mathrm{B}\Gamma$$

Треугольники ВГА, ВНА, ΘНА будут равные, а потому треугольник ГΘА будет одинаковою кратностью треугольника:

$$\Gamma\Theta A = m \, B\Gamma A$$

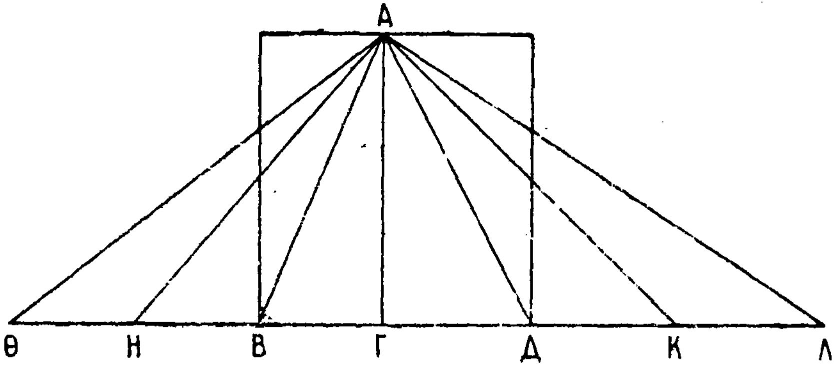

Рис. 4.

Подобным же образом отложим несколько раз сторону ГΔ, т.-е. ГΔ, ΔК, КΛ; тогда получим:

$$\Gamma\Lambda = n \, \Gamma\Delta,$$

и соответственным образом:

$$\Gamma\Lambda A = n \, \Gamma\Delta\Lambda$$

Но если

$$\Gamma\Lambda \gtreqless \Gamma\Theta,$$

то будет, очевидно,

$$\Gamma\Lambda A \gtreqless \Gamma\Theta A,$$

а тогда по определению Эвклида:

$$\frac{\Gamma\Delta}{\Gamma B} = \frac{\Gamma\Delta A}{\Gamma B A},$$

что и требовалось доказать.

ТЕОРИЯ ДЕДЕКИНДА

§ 17. Перейдем теперь к изложению теории чисел иррациональных, следуя Дедекинду.

Теория Дедекинда интересна тем, что она примыкает к изложенным мыслям Эвклида.

Изменим несколько формулировку § 15. Перепишем неравенства (1) § 15 так:

$$\frac{a}{b} \gtreqqless \frac{n}{m}, \quad \frac{c}{d} \gtreqqless \frac{n}{m};$$

тогда мы можем сказать, что существует равенство двух чисел:

$$\frac{a}{b} = \frac{c}{d},$$

если всякая *рациональная* дробь

$$\frac{n}{m}$$

или одновременно больше *обоих* чисел, или равна им, или же меньше их.

Отсюда мы сразу приходим к знаменитой теории Дедекинда иррациональных чисел.

Дадим этой теории геометрическое толкование.

Возьмем на прямой линии произвольную точку O за начало.

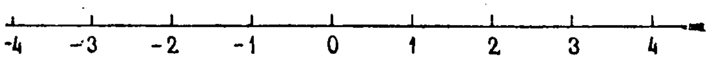

Рис. 5.

Возьмем произвольный отрезок за единицу длины и отложим его произвольное число раз от точки O в обе стороны. Получим точки, соответствующие числам целым:

$$\ldots -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots$$

Если каждый из этих отрезков мы разделим пополам, то получим точки, соответствующие дробным числам со знаменателем 2. Вставляя точки, соответствующие дробным числам со знаменателями 3, 4, 5,... и продолжая так далее до бесконечности, заполним прямую точками, соответствующими всем рациональным числам. Назовем эти точки *рациональными*. Совокупность рациональных точек равносильна совокупности рациональных чисел. Мы обозначим обе эти совокупности буквою R. Точечная совокупность дает хорошее наглядное представление.

Прежде всего мы замечаем, что совокупность R заполняет прямую *всюду плотно* (überall dicht). Это значит, что между точкмаи R не существует пробелов конечной длины. В самом деле, допустим, что между точками R существует пробел длины δ, не заполненный точками. Возьмем натуральное число n столь большое, что

$$n > \frac{1}{\delta},$$

тогда $\delta > \frac{1}{n}$. Возьмем рациональные числа, образующие арифметическую прогрессию с разностью $\frac{1}{n}$, тогда по крайней мере одна из соответствующих этим числам точек попадет внутрь нашего пробела, что указывает на то, что этого пробела не существует.

§ 18. Является важный вопрос, исчерпывают ли точки R все точки прямой. Ответ на этот вопрос должен быть отрицательный. В этом можно убедиться на простом примере.

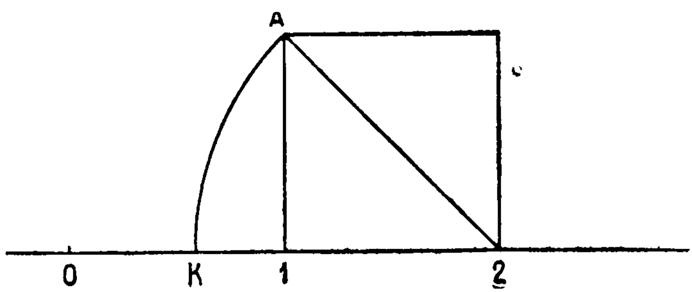

Рис. 6.

Построим на отрезке (1, 2), как на основании, квадрат, тогда, по доказанному в § 12, диагональ (2, A) будет иметь длину иррациональную. Проведем из точки 2 окружность круга радиуса (2, A). Эта окружность пересечет прямую (0,1) в точке K, причем точка K, как иррациональная, не принадлежит к R. Итак, окружность наша проходит через какой-то разрез между точками R. Этот разрез должен иметь длину, равную нулю, ибо, как мы уже видели, между точками R не могут существовать разрезы конечной длины. Мы приходим к заключению, что в каждом разрезе длины нуль находится только одна и р р а ц и о н а л ь н а я точка. Если мы к точкам R присоединим все иррациональные точки, то получим совокупность так называемых вещественных или действительных точек (чисел) W.

Совокупность точек W заполняет прямую уже без пропусков, или, как говорят, непрерывно.

§ 19. Теория Дедекинда чисел иррациональных может быть изложена так.

Каждое рациональное число a рассекает всю совокупность чисел R на два класса

$$A \quad \text{и} \quad B,$$

причем все числа класса A меньше a, а все числа класса B больше a.

Точки класса A находятся слева от точки a, а точки B — справа.

В классе A нет наибольшего числа, ибо, если мы допустим, что такое наибольшее число существует, пусть оно будет a_1, тогда $a_1 < a$, но число $a_2 = a_1 + \frac{a - a_1}{2}$ — больше a_1, но меньше a. Значит a_2 принадлежит к классу A и больше чем a_1, так что a_1 не наибольшее число класса A. Подобным же образом покажем, что в классе B нет наименьшего числа.

Таким образом, рациональное число a есть граница между двумя классами A и B. Мы получаем такое сечение всех чисел R на два класса, если присоединим границу a к классу A или к классу B, безразлично:

$$(Aa, B) = (A, Ba);$$

граница a будет наибольшим числом категории Aa и наименьшим числом категории Ba.

Иррациональное число α, как находящееся в промежутке между двумя категориями, может быть определено сечением

$$(A, B)$$

всех рациональных чисел, не имеющим границы.

§ 20. Соображения начала § 17 привели Дедекинда к такому определению равенства двух иррациональных чисел α и β.

Эти числа должны определяться одним и тем же сечением

$$\alpha = (A, B), \quad \beta = (A, B)$$

Такое определение упорядочивает иррациональное число α в смысле величины его, в смысле больше и меньше среди чисел рациональных.

Если возьмем две точки, безразлично рациональные или иррациональные, то очевидно, что точка, лежащая справа, должна соответствовать большему числу.

Иррациональное число $\alpha=(A, B)$ должно считаться большим всякого рационального числа категории A и меньшим всякого рационального числа категории B.

Если мы сравним два иррациональных числа

$$\alpha=(A, B), \quad \beta=(A_1, B_1),$$

то очевидно, что для неравенства

$$\alpha<\beta$$

должно существовать по крайней мере одно рациональное число k, большее чем α и меньшее чем β. Т. е. число k должно принадлежать к классу B и в то же время к классу A_1. Около каждой точки α должны существовать по разные ее стороны две точки $a_0<\alpha$, $b_0>\alpha$, такие, что разность

$$b_0-a_0$$

может быть сделана сколь угодно малою.

§ 21. Чтобы ввести сечения как вычислительный элемент, надо определить четыре арифметических действия над ними.

Определим правило сложения двух сечений

$$(A, B)+(A_1, B_1) \tag{1}$$

Под суммой этих сечений придется разуметь сечение

$$(A+A_1,\ B+B_1), \tag{2}$$

где под $A+A_1$ надо разуметь все суммы элементов A и A_1 и точно так же под $B+B_1$ — суммы элементов B и B_1. Если оба заданные сечения представляют числа рациональные a и a_1, то можно считать, что a есть наибольший элемент A, а a_1—наибольший элемент A_1, тогда очевидно, что $a+a_1$ будет наибольший элемент $A+A_1$. Сечение (2) будет равно, очевидно, рациональному числу $a+a_1$ и будет действительно суммой сечений (1).

Мы тогда вводим как определение, что (2) есть сумма сечений (1), также и когда они иррациональные.

Обращаясь к правилу вычитания, мы можем рассуждать так. Если мы изменим знаки $+$ на $-$ и обратно во всех элементах сечения

$$(A,\ B),$$

то это можно обозначить так:

$$(-A, -B)$$

Последнее сечение надо переписать так:

$$(-B,\ -A)$$

и оно равно взятому со знаком минус числу, определенному сечением $(A,\ B)$, т. е.

$$(-B, -A) = -(A, B)$$

Отсюда получаем непосредственно правило вычитания:

$$(A_1,\ B_1) - (A, B) = (A_1, B) + (-B, -A) = (A_1 - B,\ B_1 - A)$$

Так же просто определяется правило умножения

$$(A, B)\cdot(A_1,\ B_1) = (AA_1,\ BB_1),$$

где знаками AA_1 и BB_1 указывается совокупность чисел, которые получаются от перемножения всевозможных элементов A и B с элементами A_1 и A_1.

Для указания правила деления обратим внимание на то обстоятельство, что если $(A, B) = \alpha$, то

$$\left(\frac{1}{B}, \frac{1}{A}\right) = \frac{1}{\alpha}$$

§ 22. Покажем теперь, что совокупность всех вещественных чисел есть совокупность непрерывная.

Это утверждение Дедекинд высказывает в виде теоремы, которую называет *большой теоремой Дедекинда.*

Эта теорема такая:

Все сечения совокупности вещественных чисел имеют границы.

Т. е. для произвольного сечения $(\mathfrak{A},\ \mathfrak{B})$ чисел вещественных существует всегда число рациональное или иррациональное, которое является или наибольшим числом в категории $\mathfrak{A}$ или наименьшим в категории $\mathfrak{B}$.

Для доказательства, что сечение совокупности чисел рациональных

$$(A,\ B), \tag{1}$$

(которое получается из сечения ($\mathfrak{A}$, $\mathfrak{B}$) таким образом, что A представляет все рациональные числа из категории $\mathfrak{A}$ и $\mathfrak{B}$ — все рациональные числа из категории $\mathfrak{B}$),—будет границей сечения ($\mathfrak{A}$, $\mathfrak{B}$). Будет ли число (1) рациональным или иррациональным, оно обязательно должно входить в одну из категорий $\mathfrak{A}$ или $\mathfrak{B}$, ибо эти категории обнимают все вещественные числа.

Пусть число

$$\alpha = (A, B)$$

входит в категорию $\mathfrak{A}$; тогда можно показать, что оно есть большее в этой категории. Допустим обратное, что существует в категории $\mathfrak{A}$ число β, большее числа α. Между числами α и β будет существовать рациональное число l такое, что

$$\alpha < l < \beta$$

Рациональное число l должно входить в категорию A, что невозможно, ибо по определению сечения все числа A меньше α.

ИРРАЦИОНАЛЬНЫЕ ЧИСЛА И ДЕСЯТИЧНЫЕ ДРОБИ*)

§ 23. Мы выяснили теорию Дедекинда с точки зрения ее происхождения из гениальных соображений Эвклида.

Теория Дедекинда на вычислительной практике слишком громоздка, а потому действия над числами иррациональными удобнее производить через определение иррациональных чисел непериодическими десятичными дробями. Такой способ изложения некоторые авторы называют Вейерштрассовым. Я считаю, что этот способ стар, как стара арабская **) десятичная система исчисления, как старо употребление десятичных дробей.

---

*) Способ изложения теории иррациональных чисел, который мы здесь приводим, был введен еще в начале 90-х годов прошлого столетия В. В. Марковым в 5-ой гимназии в быв. Петербурге.

**) Я должен обратить внимание читателей на то обстоятельство, что современные арабские цифры отличаются по внешнему виду от наших, они суть

٠.١.٢.٣.٤.٥.٦.٧.٨.٩

По способу десятичных дробей я изложил теорию иррациональных чисел в моем курсе элементарной алгебры, напечатанном в 1915 году*) под заглавием „Начала алгебры“.

Я изложу вкратце мои мысли, не придерживаясь строгости изложения.

Мы придем самым простым и естественным путем к числам иррациональным, если будем рассматривать бесконечные десятичные дроби.

Из всего, что известно из арифметики, мы приходим к заключению, что положительные рациональные числа раскладываются или в *конечные* или в *периодические* десятичные дроби.

$$\frac{3}{4} = 0{,}75\,, \quad \frac{5}{7} = 0{,}(714285) = 0{,}714285714285\ldots$$

Можно себе представить *заданную* бесконечную *непериодическую* дробь. Задать подобную дробь значит указать правила, по которым можно было бы узнать, какая цифра стоит на любом указанном месте.

Например, дробь

$$0{,}1010010001000010000010\ldots \tag{1}$$

можно считать заданною. Единицы стоят на первом месте после запятой, на третьем, на шестом, на десятом, на пятнадцатом и так далее, вообще говоря, на месте $1+2+3+\ldots+n$ Остальные цифры нули.

Дробь (1) непериодическая, следовательно, она не может быть разложением рационального числа; она представляет число новой природы.

Определение иррационального числа

§ 24. *Всякая бесконечная непериодическая десятичная дробь представляет положительное*

Наши цифры могут быть названы арабскими, ибо все арифметические действия над ними совершаются по тем же правилам

Например

٤٠٩٢ = 4092

*) Существует украинский перевод этого курса.

иррациональное число. Та же дробь, взятая со знаком минус впереди, представляет отрицательное иррациональное число.

Определение равенства иррациональных чисел

Два иррациональных числа мы будем считать равными тогда и только тогда, когда оба имеют одинаковое представление в виде бесконечной дроби и одинаковые знаки.

Например:

$$-3{,}1415926\ldots = -3{,}1415926\ldots$$

Если мы захотим распространить это определение на периодические десятичные дроби, т. е. на числа рациональные, то тут встретилось бы одно исключение, а именно дроби с периодом 9 равны конечным дробям, например,

$$0{,}567 = 0{,}5669999\ldots$$

Если мы согласимся не писать дробей с периодом 9, то можно будет установить определение равенства как чисел рациональных, так и иррациональных при помощи тождественности их представлений десятичными дробями.

Дальнейшие определения будут относиться одновременно и к числам рациональным и к числам иррациональным.

Определение неравенства

Два числа не равны, если их разложения в десятичную дробь не одинаковы.

То из двух неравных чисел больше, у которого первая слева неодинаковая цифра одного и того же разряда больше.

Например:

$$142{,}56789412\ldots < 142{,}56789583\ldots$$

Мы не встретим никакого затруднения в установлении действий над числами иррациональными, если сохраним для чисел иррациональных те же самые правила, которые относятся к действиям над периодическими десятичными дробями.

§ **25.** Чтобы проще изложить действия над иррациональными числами, вернемся к самым началам арифметики и скажем несколько слов о производстве действий сложения и вычитания над многозначными целыми числами.

В арифметике даются правила для сложения целых чисел, причем действие совершается справа налево: начиная складывать единицы, мы переходим к сложению десятков, сотен, тысяч и т. д., причем получающиеся единицы высшего разряда прибавляются к сумме следующих слева цифр. Точно так же производится и вычитание.

Лица, которым приходится много вычислять, находят более практичным складывать *числа по два*, причем сложение при некотором навыке можно производить с удобством *слева направо*.

То же самое относится также к вычитанию.

Вследствие привычки европейских народов писать слова слева направо является удобным сразу писать цифры суммы или разности в привычном направлении.

Небольшого упражнения достаточно, чтобы привыкнуть складывать и вычитать числа слева направо. Будем называть такое сложение и вычитание действием, *произведенным в обратном направлении*.

Определение сложения

Для того чтобы сложить два числа рациональных или иррациональных, представленных десятичными дробями, необходимо произвести над их цифрами сложение в обратном направлении: Например,

$$\begin{array}{r} 135{,}67089267541 \\ +\ \ 72{,}36609885145 \\ \hline 208{,}0369915\ldots \end{array}$$

Цифры шестого разряда после запятой в заданных числах суть 2 и 8. После сложения они дадут цифру 0 суммы, но настоящая шестая после запятой цифра суммы будет 1, ибо следующий разряд имеет цифры 6 и 8.

Из данного определения сложения следует, как теорема, то обстоятельство, что вычитание иррациональных чисел должно производиться как обычное вычитание целых чисел в обратном направлении.

Например:

$$\begin{array}{r} -\;135{,}67089267541\ldots \\ 72{,}26609883145\ldots \\ \hline 63{,}30479384\;\ldots\ldots \end{array}$$

Пусть положительное иррациональное число разложено в десятичную дробь

$$A = a_0{,}a_1a_2a_3\ldots,$$

где a_0 целая часть числа A, а буквы a_1, a_2, $a_3, \ldots$ представляют цифры дробной части числа.

Число a_0 есть или нуль, или натуральное число, которое может быть и многозначным. Цифры же a_1, a_2, $a_3, \ldots$ суть натуральные числа, меньшие 10, или нули.

Пусть A_k обозначает конечную десятичную дробь, которую мы получим из иррационального числа A, если бесконечную дробь оборвем на k-ой цифре после запятой:

$$A_k = a_0{,}a_1a_2a_3\ldots a_k$$

Так как

$$A - A_k = 0{,}\underbrace{00\ldots0}_{k \text{ нулей}}\,a_{k+1}\,a_{k+2},$$

то эта разность положительная.

Далее

$$A - A_k < 0{,}\underbrace{00\ldots0}_{k-1 \text{ нулей}}1\;, \text{ или} < \frac{1}{10^k}$$

С увеличением значка k A_k приближается к числу A. Пусть рассматриваются две бесконечные дроби

$$A = a_0{,}a_1a_2a_3a_4\ldots$$

$$B = b_0{,}b_1b_2b_3b_4\ldots$$

Пусть приближения будут

$$A_k \quad \text{и} \quad B_k$$

Их произведение

$$A_k\, B_k \tag{1}$$

может быть вычислено по правилам арифметики как произведение двух конечных десятичных дробей.

Если мы вычислим следующие произведения:

$$A_{k+1}B_{k+1}, \quad A_{k+2}B_{k+2}, \tag{2}$$

то мы увидим, что число общих цифр произведения (1) со всеми следующими произведениями (2) увеличивается с возрастанием значка k.

Например, рассмотрим два числа:

$$A = 2{,}3409050137\ldots$$

$$B = 3{,}4500867042\ldots$$

Получаем:

$$
\begin{aligned}
A_0B_0 &= 2{,}3 && = 6\\
A_1B_1 &= (2{,}3)\,(3{,}4) && = 7{,}82\\
A_2B_2 &= (2{,}34)\,(3{,}45) && = 8{,}0730\\
A_3B_3 &= (2{,}340)\,(3{,}450) && = 8{,}073000\\
A_4B_4 &= (2{,}3409)\,(3{,}4500) && = 8{,}07610500\\
A_5B_5 & && = 8{,}076292720\\
A_6B_6 & && = 8{,}076323567\\
A_7B_7 & && = 8{,}076325206\\
A_8B_8 & && = 8{,}076325240
\end{aligned}
$$

Определение умножения

Под произведением AB двух чисел A и B, определяемых двумя бесконечными десятичными дробями, разумеется число, составленное из бесконечно продолженного ряда сохраняющихся при возрастании значка k цифр произведения A_kB_k.

В нашем примере получаем:

$$AB = 8{,}0763252\ldots$$

Что касается действия деления, то нам остается немного прибавить к тому, что сказано относительно умножения.

Действие деления бесконечных десятичных дробей не отличается по существу от деления целых чисел.

Например:

$$\begin{array}{r|l} 3{,}14159262\ldots & 5{,}20315426\ldots \\ \underline{3{,}12189255\ldots} & 0{,}6037 \\ 197000\ldots & \\ \underline{156094\ldots} & \\ 4090\ldots & \\ \underline{3642\ldots} & \end{array}$$

и т. д.

ПРИБЛИЖЕННАЯ МАТЕМАТИКА

§ 26. Все, что мы до сих пор говорили об обобщенном понятии о числе, относится, если так можно выразиться, к теоретической математике. Но та же самая математика имеет другой вид, когда мы ее применяем к конкретным практическим задачам. Так как в этих случаях приходится изображать числа десятичными дробями, а бесконечное число цифр писать нельзя, то приходится ограничиваться конечным числом цифр, обыкновенно не очень большим, и наша математика обращается в приближенную.

Отношение окружности к диаметру есть известное иррациональное число, которое обозначают греческой буквой π (пи). Лудольф Ван-Цейлен вычислил это число с 35-ю десятичными знаками.

Это число есть:

$$3{,}14159265358979323846264338327950288,$$

которое называют „лудольфовым".

Последующие математики вычислили это число с большею степенью точности. Дазе нашел 200 цифр, Рихтер—500, а Шенкс даже 700. Однако такое точное вычисление не имеет ни теоретического, ни практического значения.

Вообразим шар, радиус которого равен расстоянию Сириуса от Земли (около 132 биллионов километров), наполненный микробами так тесно, что в каждом кубическом миллиметре их помещается целый биллион (10^{10}). Вообразим далее, что все эти микробы выравнены на прямой, и расстояние между каждыми двумя соседними равно расстоянию Сириуса от Земли. Примем теперь эту прямую за диаметр круга и вычислим длину окружности этого круга при помощи π со 100 десятичными знаками. Полученное число даст длину этой окружности с ошибкой против истины лишь в одну миллионную миллиметра.

Ясно, что столь большое число цифр брать не имеет смысла. При приложениях обычно редко приходится брать более 5 цифр, так как ошибка заключается уже в данных, полученных из наблюдений и измерений.

Разность между истинным значением a некоторой величины и приближенным ее значением u, полученным или по измерениям или по вычислениям, называется абсолютной погрешностью величины u.

Абсолютная погрешность недостаточно характеризует достоинство результата. Необходимо указать процентное отношение абсолютной погрешности к самой величине a. Т. е. необходимо указать отношение

$$\frac{a-u}{a},$$

которое называется относительною погрешностью.

Относительная погрешность есть отвлеченное число. Чем меньше относительная погрешность, тем больше точность, с которой величина известна, поэтому относительная погрешность и принимается за меру точности результата.

Если относительная погрешность мала, то она оставляет без изменения несколько первых цифр величины a и отражается только на некоторой k-ой цифре. По мере увеличения k относительная погрешность уменьшается.

Можно высказать основной принцип всех приближенных вычислений.

1. Всякая неверная цифра есть—ошибка.
2. Всякая лишняя цифра есть—полошибки.

§ 27. Во время моей научной деятельности я встретился один раз с математиком, который сказал мне, что он признает только теоретическую математику и презирает приложения. Чаще мы встречаемся с математиками, которые держатся противоположного мнения. Это суть обычно механики, физики и техники. Обе эти крайности, конечно, неправильны.

Великий Эйлер был другого мнения. Он сделал массу открытий теоретического характера, которые двинули вперед диференциальное и интегральное исчисления и в то же время он был феноменальным числовым вычислителем.

Характерна деятельность гениального немецкого математика Карла Фридриха Гаусса (1777—1855).

В возрасте 24 лет он выступил со знаменитым трактатом по теории чисел „Disquisitiones arithmeticae“. По богатству материала, ряду прекрасных открытий, разнообразию и остроумию доказательств это сочинение до сих пор считается основным при изучении теории чисел. Между прочим, в нем содержится прекрасная теория двучленных уравнений, из которой вытекает, что можно вписать при помощи циркуля и линейки в круг правильный семнадцатиугольник. Тут находится глубокая теория квадратичных форм, в которой, между прочим, Гаусс провидел действия над идеальными числами, которые были открыты полвека спустя.

Несмотря на массу теоретических открытий в разнообразных частях математики, Гаусс, как профессор астрономии, был неутомимый числовой вычислитель, который оставил потомству новый способ вычислять логарифмы сумм и разностей.

Дело в том, что логарифмы упрощают действия, заменяя умножение и деление сложением и вычитанием.

При вычислении сумм и разностей дело до Гаусса происходило несколько громоздко. Приходилось вычислять логарифмы сначала всех слагаемых, далее по этим логарифмам вычисляли самые слагаемые, далее их складывают и, наконец, находят логарифм суммы.

У Гаусса явилась мысль сразу по логарифмам слагаемых получить непосредственно логарифм суммы. Он предложил для этого составить особые таблицы, которые до настоящего времени называются таблицами Гаусса сумм и разностей[1]).

Таблица для сложения отличается от таблицы для вычитания. Положим, что числа A и B известны лишь по своим логарифмам, и требуется найти логарифм их суммы: $\lg(A+B)$.

Пусть будет

$$A > B$$

Тогда имеем:

$$\lg(A+B) = \lg A\left(1+\frac{B}{A}\right) = \lg A + \lg\left(1+\frac{B}{A}\right)$$

---

[1]) J. Zech, Tafeln der Additions- uud Subtractions-Logarithmen, Berlin 1863.

Так как логарифмы чисел A и B заданы, то нам известно число:

$$\lg \alpha = \lg A - \lg B$$

Гауссова таблица так составлена, что по числу $\lg \alpha$ можно получить прямо:

$$\lg\left(1 + \frac{B}{A}\right) = \lg \beta;$$

тогда окончательно:

$$\lg A + \lg \beta = \lg (A + B)$$

Покажем, как составлена Гауссова таблица для вычитания. Мы имеем:

$$\lg (A - B) = \lg A\left(1 - \frac{B}{A}\right) = \lg A - \lg\left(\frac{1}{1 - \frac{B}{A}}\right)$$

Пусть будет

$$\frac{A}{B} = \alpha,$$

тогда

$$\lg \alpha = \lg A - \lg B$$

Для аргументов $\lg \alpha$ вычислена таблица величины

$$\lg \frac{1}{1 - \frac{B}{A}} = \lg \frac{\alpha}{\alpha - 1} = \lg \beta$$

Таблица имеет вид:

$\lg \alpha$	$\lg \beta$
....	....
....	....

Из равенства $\frac{\alpha}{\alpha - 1} = \beta$ следует, что $\alpha = \frac{\beta}{\beta - 1}$, поэтому, если за аргумент $\lg \frac{A}{B}$ принять $\lg \beta$, то соответствующая величина $\lg \frac{1}{1 - \frac{B}{A}}$ найдется в столбце $\lg \alpha$. Кроме того, $\alpha = \beta = 2$, а потому:

$\lg\alpha$	$\lg\beta$
0	∞
. . . . .	. . . . .
. . . . .	. . . . .
0,3010300	0,3010300

§ 28. В технике дело обычно не идет дальше четырех знаков, а то часто достаточно бывает трех и даже двух знаков. Поэтому в технике имеют распространенное применение так называемые логарифмические линейки, дающие два знака и при умении ими пользоваться — даже три знака.

Для четырехзначных таблиц можно порекомендовать:

Глазенап, „Карманная таблица логарифмов“ (существуют два издания — русское и украинское).

Из пятизначных таблиц очень практичны: Е. Пржевальский, „Пятизначные таблицы логарифмов“. В этой книжке, несмотря на ее малый объем, приведено много таблиц, полезных на практике.

Существуют шестизначные и семизначные логарифмы. Семизначные логарифмы были введены в гимназиях и реальных училищах при старом режиме.

Объем таблиц быстро возрастает по мере перехода к большему числу знаков.

Существуют еще восьмизначные логарифмы, изданные во Франции по распоряженю военного министра:

„Service géographique de l'armée. Tables de logarithmes a huit décimales des nombres entiers de 1 à 120.000 et des sinus et tangentes de dix secondes en dix secondes d'arc dans le système de la division centésimale du quadrant publiées par ordre du ministre de la guerre MDCCCXCI“.

Эта книга имеет большой объем, она издана in folio, около 600 страниц. Этот объем помешает ее распространению. Квадрант делится на 100 частей, так что $90^d = 100^c$.

О ПРЕДЕЛЕ ПЕРЕМЕННОЙ

§ 29. Пусть будет задана совокупность вещественных чисел:

$$S(a,\ b,\ c, \ldots),$$

причем безразлично, будет ли в этой совокупности конечное или бесконечное число чисел. Числа a, b, $c, \ldots$ могут быть произвольные.

Если одно из чисел совокупности S, не указывая которое именно, ми обозначим одной буквой x, то эта буква выражает переменную величину. Каждое из чисел $a, b, c, \ldots$ совокупности называется частным значением.

Если написано равенство $x = a$, то говорят, что переменная x приняла частное значение a.

Обычно устанавливается процесс изменения переменной величины, т. е. мы приводим ее численные значения в такой порядок, что знаем, которые значения переменная принимает ранее, которые позднее.

Если все частные значения переменной одинаковы, то переменная называется постоянною. Постоянной величиной можно назвать каждое отдельное заданное число.

§ 30. Назовем через x' какое-нибудь из значений, принимаемое переменной x в некоторый момент процесса изменения, любое же позднейшее значение x мы обозначим через x''.

Определение. Если всякому положительному числу ε (как бы мало оно ни было) можно сопоставить такое значение x' переменной x, что будет иметь место неравенство*)

$$|x'' - a| < \varepsilon \tag{1}$$

при всех позднейших значениях x'', то постоянное число a называется пределом переменной x.

Если предел переменной x есть нуль, то переменная x называется бесконечно малою.

Тогда, подставляя $a = 0$ в неравенство (1), получим неравенство

$$|x| < \varepsilon \tag{2}$$

при всяком малом ε после известного момента в изменении x.

Предел переменной x можно определить, как такое постоянное число a, что разность $x - a$ есть бесконечно малая величина.

Примерами бесконечно малых величин могут быть

$$\frac{1}{n} \quad \text{или} \quad a^x,$$

если n есть бесконечно возрастающее целое число, $a < 1$, а x бесконечно возрастающее по абсолютной величине положительное число.

Переменная, которая в процессе своего изменения может сделаться и остаться больше любого положительного числа, называется бесконечно большою.

---

*) Знак $|b|$ есть знак абсолютного значения числа b.

Например, если мы обозначим через p какое-нибудь простое натуральное число из ряда:

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23, \ldots,$$

то p будет величина бесконечно большая при возрастании p, ибо существуют в ряду сколь угодно большие числа, так как число простых чисел бесконечно большое (Эвклид).

То обстоятельство, что переменная x стремится к пределу a, обозначается одним из знаков

$$\lim x = a, \quad \text{пр.}\ x = a$$

(lim — от латинского слова limes — предел).

Бесконечно малая величина может быть обозначена формулой

$$\lim x = 0$$

Бесконечно большая величина может быть обозначена одним из знаков:

$$\lim x = \infty \quad \text{или} \quad \lim x = -\infty$$

Второй знак показывает, что бесконечно большая величина x отрицательна и беспредельно возрастает по абсолютной величине.

Если переменная x стремится к пределу a, то для всякого положительного ε мы будем писать:

$$|x' - a| < \frac{\varepsilon}{2}, \quad |x'' - a| < \frac{\varepsilon}{2}$$

при достаточно далеких x' і x''.

Тогда

$$|(x' - a) - (x'' - a)| < \varepsilon,$$

или

$$|x' - x''| < \varepsilon$$

Замечательно, что существует теорема обратная.

ТЕОРЕМА КОШИ

§ 31. Если переменная x такова, что всякому положительному малому значению ε можно указать такое значение x' переменной, что при всех дальнейших x'' имеет место неравенство

$$|x' - x''| < \varepsilon, \tag{1}$$

то переменная имеет предел, т. е. существует такое число a, что:

$$\lim x = a$$

Доказательство. Малое положительное число ε будем представлять в виде десятичной дроби и пусть будет

$$\varepsilon = \underbrace{0{,}00\ldots0}_{n \text{ нулей}}\varepsilon_1\,\varepsilon_2,$$

так что его значащие цифры $\varepsilon_1, \varepsilon_2, \ldots$ начинаются после n нулей за запятой.

Тогда у значения x'' на основании неравенства (1) будет такая же целая часть, как у x', и кроме того некоторое число m одинаковых цифр после запятой. Эти цифры сохраняются при всех значениях x'' при дальнейшем процессе x.

Число сохраняющихся цифр увеличивается с увеличением n. Продолжим до бесконечности сохраняющиеся цифры, тогда получим бесконечную десятичную дробь, которая даст некоторое число a. Очевидно, что a будет пределом переменной. В самом деле, в числе $|x' - a|$ будет целая часть нуль и некоторое число нулей после запятой. Так как число этих нулей будет возрастать, то число $x - a$ будет бесконечно малое, и следовательно, $\lim x = a$.

Из этой теоремы, как следствия, вытекают следующие теоремы.

Теорема I. Предел алгебраической суммы конечного числа переменных равен алгебраической сумме пределов слагаемых:

$$\lim (x + y - z) = \lim x + \lim y - \lim z$$

Теорема II. Предел произведения конечного числа переменных равен произведению пределов множителей:

$$\lim (xyz) = \lim x \cdot \lim y \cdot \lim z$$

Теорема III. Предел частного равен частному пределов:

$$\lim \left(\frac{x}{y}\right) = \frac{\lim x}{\lim y}$$

При этом предполагается, что $\lim y$ отличен от нуля.

ПОЛЕ W ЧИСЕЛ ВЕЩЕСТВЕННЫХ

§ 32. Иррациональное число есть предел рациональной переменной.

Рассматривая разность

$$A - A_k = 0,\underbrace{00\ldots0}_{k \text{ нулей}}\, a_{k+1}\, a_{k+2}\ldots,$$

видим, что эта разность будет меньше

$$\frac{1}{10^k} = 0,\underbrace{00\ldots0}_{k-1 \text{ нулей}}1;$$

мы замечаем, что эта разность есть бесконечно малая величина, следовательно,

$$A = \lim A_k, \tag{1}$$

т. е. *иррациональное число есть предел своего приближения по недостатку при увеличении числа* k.

Равенство (1) относится ко всякой бесконечной дроби A даже в том случае, когда она выражает рациональное число.

Необходимо подчеркнуть, что теорема Коши справедлива только в том случае, когда мы будем рассматривать полную систему всех чисел вещественных—как рациональных, так и иррациональных.

Она перестает быть справедливой, если мы ограничимся полем R чисел рациональных, потому что предел a, определяемый бесконечною дробью, может оказаться иррациональным числом, которого нет в поле R, и тогда придется сказать, что в поле R предела не существует.

Существование теоремы Коши в совокупности W всех вещественных чисел, как рациональных, так и иррациональных, есть важное свойство совокупности W, которое выражает свойство *непрерывности*, о которой мы уже упоминали в § 22.

Поле R, как мы уже видели, всюду плотное, но не непрерывное.

§ 33. Свойство, выражаемое формулой (1) § 31, позволяет очень просто убедиться, что совокупность чисел W есть поле. Для этой цели надо показать, что действия над числами иррациональными удовлетворяют тем же формальным законам что и над числами рациональными. В § 4 мы перечислили все формальные законы действий в поле. Рассмотрим сначала действия над положительными числами.

Пусть для двух чисел A и B их приближения будут A_k і B_k. Так как числа A_k і B_k рациональные, то справедливы формулы

$$A_k + B_k = B_k + A_k$$
$$A_k B_k = B_k A_k$$

Переходя к пределу, получим

$$A + B = B + A$$
$$AB = BA$$

Подобным же образом покажем справедливость сочетательного и распределительного законов, ибо из формул:

$$(A_k + B_k) + C_k = A_k + (B_k + C_k)$$
$$(A_k B_k) C_k = A_k (B_k C_k)$$
$$(A_k + B_k) C_k = A_k C_k + B_k C_k,$$

справедливость которых уже доказана для чисел рациональных, получаются, при $k = \infty$, формулы:

$$(A + B) + C = A + (B + C)$$
$$(AB) C = A (BC)$$
$$(A + B) C = AC + BC,$$

справедливые для всяких чисел, определяемых бесконечными дробями, представляющими безразлично как числа иррациональные, так и числа рациональные.

Расширение этих законов для отрицательных иррациональных чисел не представляет затруднения.

Например, формула

$$A + (-B) = (-B) + A$$

следует из

$$A_k + (-B_k) = (-B_k) + A_k$$

[1] Профессор Коркин определял предмет элементарной алгебры, как совокупность двух дисциплин: общей арифметики, как науки обобщения понятия о числе, и формальной алгебры, которая занимается преобразованием выкладок над буквами. Он это делал, очевидно, под влиянием своего учителя, парижского академика Бертрана, который написал два курса: арифметики и алгебры, при-

чем все числовые соображения помещены им в арифметику, а алгебра посвящена формальным преобразованиям над буквами. При этом он в алгебре ничего не говорит о числах иррациональных.

Н. И. Билибин в 80-х годах прошлого столетия издал перевод алгебры Бертрана, но прибавил от себя большие по объему главы о числах иррациональных. Этими прибавленнями он испортил книгу, потому что его соображения о числах иррациональных были полны логических ошибок. Пирожков переиздал перевод алгебры Бертрана без дополнений Билибина.

Можно сказать, что поле R рациональных чисел принадлежит вполне к арифметике. Алгебра кроме поля R берет также более широкое поле W всех вещественных чисел. Алгебра берет, наконец, самое широкое поле I всех чисел как вещественных, так и мнимых. Об этом поле I мы будем говорить далее.

ПОЛЕ КОМПЛЕКСНЫХ ЧИСЕЛ

§ 34. Последнее обобщение понятия о числе, которое вводится в обиход обыкновенной математики, составляют числа мнимые и комплексные.

Мнимые числа возникли под влиянием задачи извлечения корня квадратного из отрицательного числа

$$\sqrt{-a};$$

так как квадраты вещественных чисел всегда положительные, то задача в области вещественных чисел невозможна. Нужны какие-то новые числа:

$$\sqrt{-a}=\sqrt{a}\,\sqrt{-1}=\sqrt{a}\,i,$$

где

$$i=\sqrt{-1},\quad i^2=-1$$

есть мнимый знак.

Числа вида

$$a+bi,$$

где a и b вещественные числа, носят название чисел комплексных.

Посмотрим, нельзя ли над числами комплексными производить все алгебраические действия, считая i как обыкновенное число и имея в виду только основное равенство, определяющее мнимый знак:

$$i^2=-1$$

Это даст нам формулы для нахождения целых степеней знака:

$$i^3 = i^2 \cdot i = -i, \quad i^4 = i^3 \cdot i = -i \cdot i = +1, \quad i^5 = i^4 \cdot i = i$$

і т. д.

Покажем теперь, как выразится равенство двух комплексных чисел:

$$a + bi = c + di$$

Предполагая, что с мнимым знаком можно производить все действия алгебры, получим

$$i = \frac{c-a}{b-d};$$

выходило бы, что мнимый знак был бы вещественным числом, а потому должно быть

$$c - a = 0, \qquad b - d = 0,$$

т. е.

$$c = a, \quad b = d,$$

т. е. у двух равных комплексных чисел должны равняться как вещественные части, так и коэфициенты при мнимом знаке.

Правило сложения и вычитания, очевидно, даются формулами

$$(a + bi) + (c + di) = (a + c) + (b + d)\, i \tag{1}$$

$$(a + bi) - (c + di) = (a - c) + (b - d)\, i \tag{2}$$

Правило умножения получим, если перемножим два комплексных числа как двучлены, предполагая i числом, которое допускает все действия алгебры, т. е.

$$(a + bi)(c + di) = ac + bci + adi + bdi^2;$$

здесь надо заменить $i^2 = -1$.

Получаем правило перемножения комплексных чисел:

$$(a + bi)(c + di) = ac - bd + (bc + bd)\, i \tag{3}$$

Комплексные числа

$$a + bi, \quad a - bi,$$

отличающиеся знаком при i, называются мнимыми сопряженными; их произведение равно п о л о ж и т е л ь н о м у числу:

$$(a + bi)(a - bi) = a^2 - b^2 \cdot i^2 = a^2 + b^2$$

Для получения правила деления пишем:

$$\frac{a+bi}{c+di}=\frac{(a+bi)(c-di)}{c^2+d^2}=\frac{ac+bd}{c^2+d^2}+\frac{bc-ad}{c^2+d^2}i.$$

Существует в совокупности комплексных чисел только одно число, на которое делить нельзя; для этого числа должно быть:

$$c^2+d^2=0$$

Так как c и d вещественные числа, то должно быть:

$$c=0, \quad d=0$$

Это единственное число, на которое делить нельзя, есть обыкновенный нуль:

$$0+0i=0$$

§ 35. Приведенный способ рассуждения считается нестрогим и полагается рассуждать так: знак

$$a+bi$$

представляет число новой природы, в котором (+) пока не есть знак сложения, bi не есть произведение, i считается числом новой природы, о котором мы пока ничего не знаем, a и b суть вещественные числа.

Далее мы устанавливаем правило сложения, как определение сложения новых чисел при помощи равенств (1), а за определение умножения возьмем равенства (3). Тогда, как и можно было ожидать, получим, что (+) можно считать знаком сложения, ib произведением, а $i^2=-1$.

Указанное временное скрытие значения знаков напоминает несколько игру в прятки. Но эта игра в ее полном объеме заключается в книге Edmund Landau, „Grundlagen der Analysis" (1930).

Изложение комплексных чисел начинается на странице 92 этой книги и продолжается до конца книги, т. е. до страницы 133. При этом автор означает комплексное число знаком

$$[\Xi_1, \Xi_2]$$

Надо, конечно, понимать этот знак, как $\Xi_1+\Xi_2 i$, но этого он не говорит. При этом автор приводит мелкие теоремы, вроде того, что $x=x$, от теоремы № 206 до теоремы № 301. И лишь на последней теореме раскрывает карты и пишет:

„Satz 301. Für reelle u_1, u_2 ist

$$u_1+u_2 i=[u_1,\ u_2]$$

Zu jeder komplexen Zahl x gibt es also genau ein Paar reeller Zahlen u_1, u_2 mit

$$x=u_1+u_2 i\text{“}$$

Все его изложение ведется в трудно читаемых формах, причем он вводит свои новые знаки:

÷|÷ один из знаков $+$, $-$

Ʒ вместо $\sum$ или Π

ОСНОВНОЙ ПРИНЦИП АНАЛИТИЧЕСКОЙ ГЕОМЕТРИИ

§ 36. Мы видим, что вещественные числа однозначно сопоставляются точкам прямой без всяких пропусков. На этом свойстве основан принцип так называемой *аналитической геометрии* определять положение точки на прямой при помощи некоторого вещественного числа, называемого *координатою*.

Координата представляет взятое с тем или другим знаком расстояние точки от определенной точки, называемой *началом координат*. Знак $(+)$ соответствует точкам, лежащим по одну сторону начала, а знак $(-)$ — точкам по другую сторону.

ГЕОМЕТРИЧЕСКОЕ ПРЕДСТАВЛЕНИЕ КОМПЛЕКСНЫХ ЧИСЕЛ

§ 37. Возьмем на плоскости прямоугольную систему координат. Всякое комплексное число

$$x+iy$$

можно геометрически представлять точкою M, имеющею координаты x и y.

Вещественным числам x будут соответствовать точки P, лежащие на оси абсцисс, а чисто мнимым числам iy будут соответствовать точки оси ординат.

Абсолютная величина $|x|$ каждой вещественной координаты x точки P на оси OX представляет расстояние OP этой точки P от начала координат.

Хотя понятие о больше и меньше для чисел комплексных не употребляется, но понятие абсолютной величины с вещественных чисел переносится также и на мнимые. Под абсолютной величиной мнимого числа разумеется по-

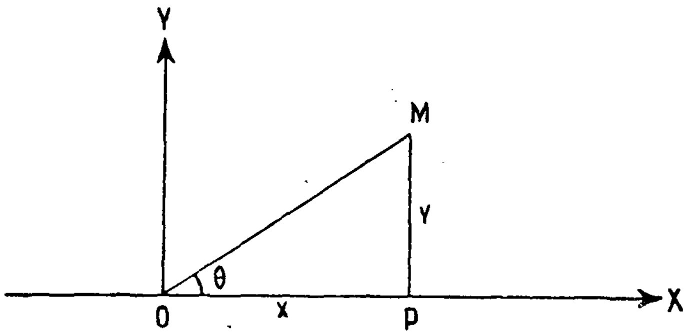

Рис. 7.

ложительное число, выражающее длину OM расстояния точки M до начала координат, т. е.

$$OM = +\sqrt{x^2 + y^2}$$

Для обозначения абсолютной величины употребляется тот же знак, что и для чисел вещественных

$$|x + iy|$$

Мы получаем:

$$|x + iy| = +\sqrt{x^2 + y^2}$$

Абсолютную величину комплексного числа называют часто модулем этого числа.

Угол $\theta = MOP$, который образует модуль OM с осью x-ов, называют аргументом комплексного числа. Мы имеем

$$\theta = \operatorname{arc\,tg} \frac{y}{x}$$

§ 38. Покажем теперь, что совокупность I образует поле. Это следует непосредственно из нашего способа введения чисел комплексных в § 34, где мы полагали, что все наши числа и мнимый знак позволяют производить над собою все алгебраические действия по законам поля. Но, конечно, ригористы (вроде Ландау) доказывают отдельно справедливость для чисел комплексных всех равенств § 4.

Так, например, для доказательства справедливости перестановочности сложения можно написать:

$$(a+bi)+(c+di)=(a+b)+(b+d)\,i$$
$$(c+di)+(a+bi)=(c+a)+(d+b)\,i;$$

но для вещественных чисел $a+c=c+a$, $b+d=d+b$; следовательно,

$$(a+bi)+(c+di)=(c+di)+(a+bi)$$

Подобным же образом мы проверим справедливость всех равенств законов поля для чисел комплексных.

Три поля R, W, I суть основные поля всей математики. Поле W заключается в поле I и есть, как говорят, его делитель. В § 5 мы видели, что R есть простейшее поле, входящее делителем в какое угодно другое поле.

В дальнейшем мы будем рассматривать, так называемые, алгебраические поля, которые все будут делителями поля I.

АЛГЕБРАИЧЕСКАЯ ЗАМКНУТОСТЬ ПОЛЯ I

§ 39. Если мы возьмем уравнение:

$$a_0x^n+a_1x^{n-1}+a_2x^{n-2}+\cdots+a_{n-1}\,x+a_n=0 \tag{1}$$

какой угодно (целой) степени, в котором все коэфициенты $a_0, a_1, a_2, \ldots, a_{n-1}, a_n$ суть произвольные элементы поля I, то все корни его принадлежат к полю I и, значит, для решения уравнения (1) никаких новых чисел, не входящих в I, вводить не нужно.

Это свойство можно назвать алгебраическою замкнутостью поля I. Оно было доказано Карлом Фридрихом Гауссом в его докторской диссертации (1799)*).

Гаусс показал, что всякое уравнение вида (1) имеет по крайней мере один корень. Эту теорему доказывали также предшественники Гаусса, но Гаусс указал недостатки в доказательствах своих предшественников д'Аламбера, Эйлера, Фонсене и Лагранжа. В 1815, 1816, 1849 г. Гаусс опубликовал три новых доказательства**). В дальнейшем я приведу новое доказательство.

---

*) Ges. Werke, 3, 1.

**) Gauss, Ges. Werke, S. 31, 57, 71.

Алгебра в ее широких и глубоких обобщениях и приложениях, особенно к теории чисел, вводит новые числа, о которых будет сказано в дальнейшем. Но приближенная математика в ее приложениях к диференциальным и интегральным уравнениям, в механике, физике и технике до сих пор не вводит новых чисел, а потому поле чисел I является исчерпывающим материалом числовых вычислений, так сказать, обычной математики.

КВАТЕРНИОНЫ

§ 40. Рассмотрим так называемые высшие комплексные числа:

$$a_1e_1+a_2e_2+\cdots+a_ne_n, \tag{1}$$

где $a_1, a_2, \ldots, a_n$ — вещественные числа.

Подобные выражения называются комплексными числами с n единицами $e_1, e_2, \ldots, e_n$. Разобранные нами комплексные числа a_1+a_2i — простейший частный случай чисел (1), а именно $a_1e_1+a_2e_2$, где $e_1=1$, $e_2=i$; поэтому мы их будем называть простейшими.

Два комплексных числа с n единицами $e_1, e_2, \ldots, e_n$ будут считаться тогда равными, когда одинаковы коэфициенты соответственных единиц.

Число (1) тогда и только тогда равно нулю, когда все коэфициенты a_i равны нулю.

Для сложения двух комплексных чисел надо сложить коэфициенты при соответственных единицах, т. е.

$$(a_1e_1+a_2e_2+\cdots+a_ne_n)+(b_1e_1+b_2e_2+\cdots+b_ne_n)=$$
$$=(a_1+b_1)e_1+(a_2+b_2)e_2+\cdots+(a_n+b_n)e_n$$

Сложение ассоциативно и перестановочно и допускает однозначное обращение, т. е. вычитание.

Для определения умножения надо дать для произведения двух единиц e_ie_k его выражение в виде числа (1). В простейших комплексных числах существует одна только формула:

$$i^2=-1$$

Здесь же мы устанавливаем формулы:

$$e_ie_k=\lambda_{ik}^{(1)}e_1+\lambda_{ik}^{(2)}e_2+\cdots+\lambda_{ik}^{(n)}e_n,$$

где $\lambda_{ik}^{(r)}$ суть вещественные числа. Тогда определяют произведение двух чисел:

$$\sum_{i=1}^{n} a_i e_i \quad \text{и} \quad \sum_{k=1}^{n} b_k e_k$$

следующим образом:

$$\sum_{i=1}^{n} a_i e_i \cdot \sum_{k=1}^{n} b_k e_k = \sum_{i,\, k=1}^{n} a_i b_k e_i e_k$$

Это умножение в соединении со сложением обладает распределительным законом. Для того чтобы существовал сочетательный закон, необходимо и достаточно, чтобы $\lambda_{ik}^{(r)}$ удовлетворяли уравнениям

$$\sum_{v=1}^{n} \lambda_{ik}^{(v)} \lambda_{vm}^{(r)} = \sum_{v=1}^{n} \lambda_{km}^{(v)} \lambda_{iv}^{(r)}$$

$$(i,\ k,\ m,\ r = 1,\ 2, \ldots, n)$$

Для того чтобы умножение было коммутативно (перестановочно), необходимо и достаточно, чтобы было

$$e_i e_k = e_k e_i,$$

т. е.

$$\lambda_{ik}^{(r)} = \lambda_{ki}^{(r)}$$

Если мы выберем из нашей системы (1) комплексных чисел n чисел

$$i_k = \alpha_{1k} e_1 + \alpha_{2k} e_2 + \cdots + \alpha_{nk} e_n \qquad (2)$$

$$(k = 1,\ 2, \ldots, n)$$

таким образом, чтобы определитель *), составленный из чисел α_{ik} был отличен от нуля, тогда n уравнений (2) можно решить относительно $e_1, e_2, \ldots, e_n$ и выразить эти числа через i_k, так что наше число (1) примет вид:

$$b_1 i_1 + b_2 i_2 + \ldots + b_n i_n \qquad (3)$$

Говорят, что система комплексных чисел (3) с n единицами $i_1, i_2, \ldots, i_n$ происходит из нашей начальной системы (1) через линейное преобразование (2). И обратно, система (1) происходит из системы (3) через обратное преобразование.

---

*) См. главу Определители, стр. 97.

Существует весьма важная теорема Вейерштрасса (1863):

Теорема. Из всех комплексных систем с двумя и более единицами простейшие числа и происходящие из них при помощи линейного преобразования суть единственные, которые представляют коммутативное поле, причем произведение чисел тогда и только тогда обращается в нуль, когда один из множителей равен нулю.

§ 41. Из других систем комплексных чисел ближе всего к системе I простейших чисел находится замечательная система, введенная в рассмотрение Гамильтоном (Dublin 1853) и названная им системой кватернионов. Формальные законы действий над кватернионами те же, что и у поля, только одно исключение — умножение не коммутативно.

Кватернионы суть числа с четырьмя единицами:

$$1,\ i,\ j,\ k$$

и имеют вид

$$a+bi+cj+dk$$

Равенства, выражающие законы умножения мнимых единиц, такие:

$$i^2=-1,\quad j^2=-1,\quad k^2=-1$$

$$ij=k,\quad ji=-k,\quad jk=i,\quad kj=-i,\quad ki=j,\quad ik=-j \tag{1}$$

Таким образом, при умножении кватернионов надо точно принимать во внимание, в каком порядке кватернионы умножаются, ибо при перестановке множителей произведение меняется:

$$AB\neq BA$$

Мы имеем важную теорему Фробениуса*):

Теорема. Из всех систем комплексных с двумя или более единицами, кроме кватернионов и происходящих из них при помощи линейного преобразования, не существует других систем, которые бы образовали поле без коммутативного закона.

---

*) Crelle Journ., 84, 59, 1878.

§ 42. Рассмотрим некоторые выкладки с кватернионами.

Назовем кватернион $a-bi-cj-dk$, получаемый от изменения знаков у всех мнимых единиц, сопряженным с заданным:

$$a+bi+cj+dk$$

Покажем, что произведеие двух взаимно сопряженных кватерионов—положительное число:

$$(a+bi+cj+dk)(a-bi-cj-dk)=$$
$$=a^2-(bi+cj+dk)(bi+cj+dk)=$$
$$=a^2-[b^2i^2+bcij+bdik+cbji+c^2j^2+cdjk+dbki+dckj+d^2k^2]$$

Но все произведения уничтожаются на основании формул (1) § 41 и, значит,

$$(a+bi+cj+dk)(a-bi-cj-dk)=a^2+b^2+c^2+d^2$$

Корень квадратный из последней формулы, взятый со знаком (+), носит название модуля кватерниона:

$$\mathrm{mod}\,(a+bi+cj+dk)=+\sqrt{a^2+b^2+c^2+d^2}$$

Если

$$A+Bi+Cj+Dk=(a+bi+cj+dk)(a_1+b_1i+c_1j+d_1k),$$

то, меняя знаки мнимых единиц, получим:

$$A-Bi-Cj-Dk=(a_1-b_1i-c_1j-d_1k)(a-bi-cj-dk),$$

ибо непосредственная проверка показывает, что сопряженная величина произведения двух кватернионов равна произведению сопряженных величин множителей, но только эти множители надо переставить.

Мы получаем:

$$A^2+B^2+C^2+D^2=(A+Bi+Cj+Dk)(A-Bi-Cj-Dk)=$$
$$=(a+bi+cj+dk)(a_1+b_1i+c_1j+d_1k)(a_1-b_1i-$$
$$-c_1j-d_1k)(a-bi-cj-dk)=$$
$$=(a_1^2+b_1^2+c_1^2+d_1^2)(a+bi+cj+dk)(a-bi-cj-dk)=$$
$$=(a_1^2+b_1^2+c_1^2+d_1^2)(a^2+b^2+c^2+d^2),$$

и окончательно:

$$\sqrt{A^2+B^2+C^2+D^2}=\sqrt{a^2+b^2+c^2+d^2}\sqrt{a_1^2+b_1^2+c_1^2+d_1^2},$$

т. е. **модуль произведения равен произведению модулей множителей.**

§ 43. Существуют квадратные, так называемые, **ортогональные** матрицы*):

$$\begin{Vmatrix} \alpha_1^{(1)}, & \alpha_2^{(1)}, & \ldots, & \alpha_n^{(1)} \\ \alpha_1^{(2)}, & \alpha_2^{(2)}, & \ldots, & \alpha_n^{(2)} \\ \cdot & \cdot & \cdot & \cdot \\ \alpha_1^{(n)}, & \alpha_2^{(n)}, & \ldots, & \alpha_n^{(n)}, \end{Vmatrix}$$

обладающие свойствами, выраженными равенствами:

$$\begin{aligned} &\alpha_1^{(1)^2} + \alpha_2^{(1)^2} + \ldots + \alpha_n^{(1)^2} = 1 \\ &\alpha_1^{(2)^2} + \alpha_2^{(2)^2} + \ldots + \alpha_n^{(2)^2} = 1, \quad \alpha_1^{(i)}\alpha_1^{(k)} + \alpha_2^{(i)}\alpha_2^{(k)} + \ldots + \alpha_n^{(i)}\alpha_n^{(k)} = 0 \\ &\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot \\ &\alpha_1^{(n)^2} + \alpha_2^{(n)^2} + \ldots + \alpha_n^{(n)^2} = 1 \quad (i, k = 1, 2, \ldots, n) \end{aligned} \tag{1}$$

Одновременно с этими равенствами существуют такие же равенства, относящиеся к вертикалям:

$$\begin{aligned} &\alpha_k^{(1)^2} + \alpha_k^{(2)^2} + \ldots + \alpha_k^{(n)^2} = 1 \quad (k = 1, 2, \ldots, n) \\ &\alpha_k^{(1)}\alpha_c^{(1)} + \alpha_k^{(2)}\alpha_l^{(2)} + \ldots + \alpha_k^{(n)}\alpha_l^{(n)} = 0 \quad (k, l = 1, 2, \ldots, n) \end{aligned} \tag{2}$$

Эйлер указал примечательные рациональные выражения для элементов $\alpha_i^{(k)}$ для случаев $n = 3$ и $n = 4$.

Для случая $n = 3$, его матрица такая:

$$\begin{Vmatrix} D^2 + A^2 - B^2 - C, & 2(AB - CD), & 2(AC + BD) \\ 2(AB + CD), & D^2 - A^2 + B^2 - C^2, & 2(BC - AD) \\ 2(AC - BD), & 2(BC + AD), & D^2 - A^2 - B^2 + C^2 \end{Vmatrix}$$

Для этой матрицы суммы квадратов по горизонталям и вертикалям равны:

$$(D^2 + A^2 + B^2 + C^2)^2$$

Легко сделать, чтобы эти суммы были равны единице, стоит только разделить все числа на $D^2 + A^2 + B^2 + C^2$.

Клейн в своем известном четырехтомном сочинении под названием „**О теории волчка**" приводит матрицу Эйлера и называет величины A, B, C, D **кватернионными.**

---

*) Матрицей называется всякая картина из чисел, расположенных в квадрат или прямоугольник.

Для случая $n=4$ Эйлер дал такую матрицу:

$$\left\| \begin{matrix} A_1 & B_1 & C_1 & D_1 \\ A_2 & B_2 & C_2 & D_2 \\ A_3 & B_3 & C_3 & D_3 \\ A_4 & B_4 & C_4 & D_4, \end{matrix} \right\|,$$

где

$$\begin{array}{ll} A_1 = ap + bq + cr + ds, & A_2 = ar - bs - cp + dq, \\ B_1 = -aq + bp + cs - dr, & B_2 = as + br + cq + dp, \\ C_1 = ar + bs - cp - dq, & C_2 = -ap + bq - cr + ds, \\ D_1 = -as + br - cq + dp, & D_2 = -aq - bp + cs + dr, \\ A_3 = -as - br + cq + dp, & A_4 = aq - bp + cs - dr, \\ B_3 = ar - bs + cp - dq, & B_4 = ap + bq - cr - ds, \\ C_3 = aq + bp + cs + dr, & C_4 = as - br - cq + dp, \\ D_3 = -ap + bq + cr - ds, & D_4 = ar + bs + cp + dq \end{array} \qquad (3)$$

При этом Эйлер пишет: „Solutio haec eo majorem attentionem meretur, quod ad eam nulla certa methodo, sed potius quasi divinando sum perductus; et quoniam ea adeo octo numeros arbitrarios implicat, qui quidem facta reductione ad unitatem, ad septem rediguntur, vix dubitare licet, quin ista solutio sit universalis et omnes prorsus solutiones possibiles in se complectatur. Si quis ergo viam directam ad hanc solutionem manuducentem investigaverit, insignia certe subsidia analysi attulisse erit censendus. Utrum autem similes solutiones pro amplioribus quadratis, quae numeris 25, 36 et majoribus constant, expectare liceat, vix affirmare ausim. Non solum autem hinc algebra communis, sed etiam methodus Diophantea maxima incrementa adeptura videtur“.

В переводе:

„Это решение заслуживает тем большего вниманая, что я пришел к нему не при помощи какого-либо определенного метода, а как бы догадками; а так как оно к тому же содержит 8 произвольных чисел, которые после приведения к единице приводятся к семи, то едва ли можно сомневаться, что решение это универсальное и заключает в себе все возможные решения.

Если кто-нибудь найдет прямой путь к проведению этого решения, то будет считаться, что он оказал анализу выдающуюся помощь. Существуют ли подобные решения для более широких квадратов, которые состоят из 25, 36 и т. д. чисел, я едва ли решусь утверждать. Тут не только обыкновенная алгебра, но и Диофантов метод, кажется, получит огромный вклад“.

Для решения (1) все суммы квадратов по горизонталям и вертикалям равны:

$$(a^2+b^2+c^2+d^2)(p^2+q^2+r^2+s^2)$$

и следовательно, если мы хотим сделать эти суммы квадратов единицами, то должны все числа разделить на

$$\sqrt{(a^2+b^2+c^2+d^2)(p^2+q^2+r^2+s^2)}$$

Мне удалось решить задачу при помощи кватернионов.

§ 44. Рассмотрим такие кватернионы:

$$pi+aj+rk-s$$

$$ai+bj+ck+d$$

$$(ai+bj+ck+d)\,i=di+cj-bk-a$$

$$(ai+bj+ck+d)\,j=-ci+dj+ak-b$$

$$(ai+bj+ck+d)\,k=bi-aj+dk-c$$

Вычисляя произведения, получим:

$$(ai+bj+ck+d)(pi+qj+rk-s)=D_1i-C_1j-B_1k-A_1$$

$$(di+cj-bk-a)(pi+qj+rk-s)=D_3i-C_3j-B_3k-A_3$$

$$(-ci+dj+ak-b)(pi+qj+rk-s)=D_2i-C_2j-B_2k-A_2$$

$$(bi-aj+dk-c)(pi+qj+rk-s)=-D_4i+C_4j+B_4k+A_4$$

Эти формулы показывают:

$$\begin{aligned}A_1^2+B_1^2+C_1^2+D_1^2&=A_2^2+B_2^2+C_2^2+D_2^2=\\=A_3^2+B_3^2+C_3^2+D_3^2&=A_4^2+B_4^2+C_4^2+D_4^2=\\&=(a^2+b^2+c^2+d^2)(p^2+q^2+r^2+s^2)\end{aligned}$$

Нетрудное вычисление показывает, что

$$A_kA_l+B_kB_l+C_kC_l+D_kD_l=0$$
$$(k,\ l=1,\ 2,\ 3,\ 4)$$

В самом деле, докажем, что

$$A_3A_2+B_3B_2+C_3C_2+D_3D_2=0$$

Для этого возьмем два уравнения:

$$(ai+bj+ck+d)\ i\ (pi+qj+rk-s)=D_3i-C_3j-B_3k-A_3$$

$$(ai+bj+ck+d)j\,(pi+qj+rk-s)=D_2i-C_2j-B_2k-A_2$$

Изменим в первом уравнении знаки у мнимых величин i, j, k и умножим полученное уравнение на второе; тогда будем иметь

$$(-D_3i+C_3j+B_3k-A_3)\,(D_2i-C_2j-B_2k-A_2)$$

Надо доказать, что вещественная (скалярная) часть этого произведения будет равна нулю.

В левой части получаем произведение сопряженной величины от

$$(ai+bj+ck+d)\,i\,(pi+qj+rk-s)=$$

$$=(ai+bj+ck+d)\,(-p+qk-rj-si),$$

т. е. произведение величины

$$(-p-qk+rj+si)\,(-ai-bj-ck+d)$$

на

$$(ai+bj+ck+d)j\,(pi+qj+rk-s)$$

Мы получаем:

$$(a^2+b^2+c^2+d^2)\,(-p-qk+rj+si)j\,(pi+qj+rk-s)=$$

$$=(a^2+b^2+c^2+d^2)\,(-pj+qi-r+sk)\,(pi+qj+rk-s)$$

И действительно, вещественная часть этого выражения равна нулю, ибо она равна:

$$pq-pq+rs-rs=0$$

Чтобы убедиться, что сумма квадратов постоянна и по горизонталям, рассмотрим умножение таких кватернионов.

Переставим порядок множителей

$$(pi+qj+rk-s)(ai+bj+ck+d),$$

а затем левый множитель умножим справа на i, j, k; получим:

$$(pi+qj+rk-s)(ai+bj+kc+d)=A_3 i+A_2 j-A_4 k-A_1$$

$$(-si+rj-qk-p)(ai+bj+kc+d)=+D_3 i+D_2 j-D_4 k-D_1$$

$$(-ri-sj+pk-q)(ai+bj+kc+d)=-C_3 i-C_2 j+C_4 k+C_1$$

$$(qi-pj-sk-r)(ai+bj+kc+d)=-B_3 i-B_2 j+B_4 k+B_1$$

Отсюда сразу получаем:

$$\begin{aligned}&A_1^2+A_2^2+A_3^2+A_4^2=B_1^2+B_2^2+B_3^2+B_4^2=\\&=C_1^2+C_2^2+C_3^2+C_4^2=D_1^2+D_2^2+D_3^2+D_4^2=\\&=(a^2+b^2+c^2+d^2)(p^2+q^2+r^2+s^2)\end{aligned}$$

Если взять сумму квадратов по диагоналям, то, полагая, что эта сумма квадратов должна быть

$$(a^2+b^2+c^2+d^2)(p^2+q^2+r^2+s^2),$$

получим:

$$\begin{aligned}&abpq+abrs+acpr+acqs+adps+adqr+\\&+bcqr+bcps+bdqs+bdpr+cdrs+cdpq=0\end{aligned}$$

$$\begin{aligned}&-abpq-abrs+acpr+acqs-adps-adqr-\\&-bcqr-bcps+bdqs+bdpr-cdrs-cdpq=0\end{aligned}$$

Из этих двух соотношений выводим два таких:

$$(ac+bd)(pr+qs)=0$$

$$(ab+cd)(pq+rs)+(ad+bc)(ps+qr)=0$$

или

$$\text{I. } pr+qs=0, \qquad \text{II. } \frac{a}{c}=\frac{-d(pq+rs)-b(ps+qr)}{b(pq+rs)+d(ps+qr)}$$

Эйлер подобрал все числа так, чтобы удовлетворить этим двум равенствам и получить квадрат:

+68	−29	+41	−37
−17	+31	+79	+32
+59	+28	−23	+61
−11	−77	+8	+49

Общая сума черырех квадратов будет 8515. Можно прибавить, что такова же будет сумма квадратов угловых и внутренних, т.-е.

$$68^2+37^2+49^2+11^2=31^2+79^2+23^2+28^2=8515$$

§ 45. Кватернионы являются из всех высших комплексных чисел самыми близкими к полю *I*. Можно сказать, что они образуют некоммутативное поле, т. е. единственное отличие от *I* составляет отсутствие перестановочности умножения.

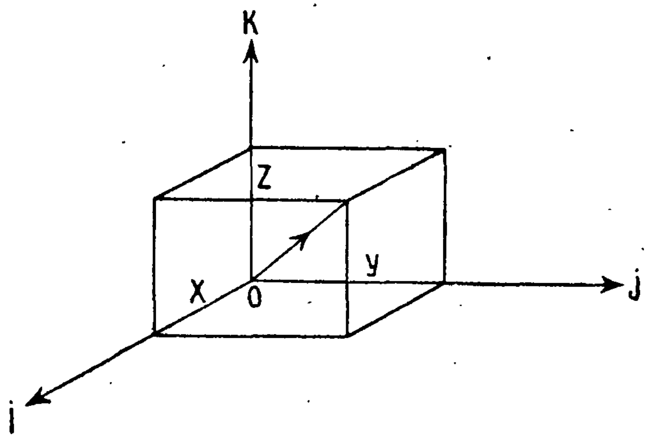

Рис. 8.

Это объясняется происхождением кватернионов из геометрических соображений. Они основаны на теории векторов, причем вектор представляется трехчленом вида:

$$xi+yj+zk, \tag{1}$$

где x, y, z суть проекции вектора на три прямоугольные оси координат в пространстве, а i, j, k—символы, обозначающие направление осей.

Если мы вектор (1) разделим на его длину $\sqrt{x^2+y^2+z^2}$, то получим трехчлен:

$$\cos\lambda i+\cos\mu j+\cos\nu k, \tag{2}$$

где λ, μ, ν углы вектора с осями координат.

Выражение (2) носит название орта кватерниона. Кватернион $xi+yj+zk$ равняется произведению длины вектора $\sqrt{x^2+y^2+z^2}$ на орт.

Рассмотрим произведение двух кватернионов:

$$\alpha = xi + yj + zk, \quad \alpha_1 = x_1 i + y_1 j + z_1 k$$

$$\alpha\alpha_1 = -xx_1 - yy_1 - zz_1 + (yz_1 - zy_1)\,i + (zx_1 - xz_1)\,j + (xy_1 - yx_1)\,k$$

Мы видим, что нельзя органичиваться трехчленным кватернионом, а потому Гамильтон ввел четырехчленные. Вещественная часть кватерниона $-xx_1 - yy_1 - zz_1$ названа скаляром. Под этим названием понимается всякое вещественное число.

Трехчлен же:

$$(yz_1 - zy_1)\,i + (zx_1 - xz_1)\,j + (xy_1 - yx_1)\,k$$

представляет вектор, изображающий линейный момент вокруг начала координат вектора α_1, отложенного от конца вектора α.

В последнее время кватернионы остаются несколько в стороне, ибо главную роль играет теория векторов. Это не совсем правильно, ибо нельзя забывать,что в руках Гамильтона кватернионы привели к открытию конической рефракции в кристаллах, что особенно важно, так как это есть один из характерных фактов, когда физическое явление было предсказано математикой.

О кватернионах помещена целая глава в книге З. Чезаро „Элементарный учебник алгебраического анализа“ *).

МНОЖЕСТВА

§ 46. В § 29 мы рассматривали совокупность

$$S(a,\ b,\ c, \ldots)$$

значений переменной и мы предполагали, что переменная принимает эти значения одно за другим; в последнее время в математике рассматривается новое понятие: когда мы рассматриваем все значения переменной одновременно, то эти значения составляют так называемое множество (Menge, ensemble).

Мы видели уже ряд числовых множеств: поля R, W, I, кватернионы; для геометрии важно рассмотрение точечных множеств (Punktmengen).

Множесто может быть обобщено на случай каких угодно предметов, не обязательно чисел или точек. Необходимо только, чтобы были даны правила, по которым можно узнать отно-

*) Русский перевод — Москва 1936.

сительно всякого определенного предмета, принадлежит он к множеству или нет.

§ 47. Множества разделяются на конечные и бесконечные, или трансфинитные.

Конечные множества имеют целое число n элементов, которые можно перенумеровать, т. е. снабдить его элементы целыми нумерами. Можно указать, который элемент мы будем считать первым, который — вторым и т. д.

В жизни так мы перенумеровываем предметы, например, при составлении каталога книг библиотеки.

Поднимем вопрос о возможности перенумеровать трансфинитное множество. С первого взгляда могло бы показаться, что это всегда возможно, ибо хотя число элементов множества бесконечно велико, но и число чисел целых бесконечно велико. На самом деле это не так. Покажем примеры множеств, которые нельзя перенумеровать.

Совокупность точек на отрезке (0, 1) нельзя перенумеровать. Все эти точки изображаются числами рациональными или иррациональными, которые можно представить десятичными дробями с равною нулю целою частью. Допустим, что мы эти числа перенумеровали:

$$\begin{array}{c|l} 1 & 0,a_1b_1c_1d_1\ldots \\ 2 & 0,a_2b_2c_2d_2\ldots \\ 3 & 0,a_3b_3c_3d_3\ldots \\ \cdot & \cdots\cdots \\ \cdot & \cdots\cdots \end{array}$$

Составим теперь такую десятичную дробь

$$0,\alpha_1\beta_2\gamma_3\ldots, \tag{1}$$

цифры которой составлены так: цифра α_1 взята отличной от a_1, цифра β_2 — отличной от b_2, γ_3 — отличной от c_3,... Дробь (1) дает число, которое заключается между 0 и 1, и следовательно, оно должно встречаться где-нибудь в нашей колонне дробей, но это невозможно, ибо число (1) не может равняться ни одной дроби нашей колонны.

Итак, существуют множества не исчислимые.

Что касается множеств исчислимых, то, во-первых, таково множество натуральных чисел.

Далее множество рациональных положительных чисел, заключающихся между 0 и 1, исчислимо.

Стоит эти рациональные числа разложить в таком порядке:

$$\frac{1}{2};\ \frac{1}{3};\ \frac{2}{3};\ \frac{1}{4};\ \frac{3}{4};\ \frac{1}{5};\ \frac{2}{5};\ \frac{3}{5};\ \frac{4}{5}\ \text{и т. д.},$$

чтобы видеть их исчислимость.

Перечислимое количество исчислимых множеств само исчислимо. Расположим элементы этих исчислимых множеств в таком порядке

$$\begin{tikzcd}
u_{11} & u_{12} \arrow[dl] & u_{13} \arrow[dl] & \dots \arrow[dl] \\
u_{21} & u_{22} \arrow[dl] & u_{23} \arrow[dl] & \dots \\
u_{31} & u_{32} \arrow[dl] & u_{33} & \dots \\
\cdots & \cdots & \cdots & \cdots
\end{tikzcd}$$

Эта фигура показывает способ исчисления.

§ 48. Два множества **э к в и в а л е н т н ы**, если элементы одного однозначно можно сопоставить с элементами другого. Два множества, эквивалентные с третьим, эквавалентны между собой.

Совокупность эквивалентных между собой множеств указывает определенную **м о щ н о с т ь**. За мощность конечных множеств можно принять число их элементов. Таким образом, мощность есть понятие, обобщающее число членов конечного множества на случай множеств трансфинитных. Так как мощности множеств тогут быть различные и так как можно определить действия над ними, то мощности являются бесконечными числами, так называемыми **т р а н с ф и н и т н ы м и**.

Исчислимое множество входит в состав всякого другого множества как часть. В самом деле, начнем над элементами бесконечного множества производить нумерование, т. е. ставить нумер 1, 2, 3,... над произвольно взятыми элементами множества. Мы нумерование произведем до конца, так как в данном множестве существует бесконечное число элементов. Если перенумерованные элементы исчерпывают множество, тогда оно исчислимое, но может случиться, что множество будет неисчислимым.

Итак, мощность исчислимого самая малая из возможных мощностей. Георг Кантор — творец всей теории множеств — обозначает ее через

$$\aleph_0 \text{ (алеф с нулем)}$$

Обозначим мощности двух множеств M и N буквами $\mathfrak{m}$, $\mathfrak{n}$. Если множества M и N эквивалентны, то

$$\mathfrak{m} = \mathfrak{n}$$

Если же M и N не эквивалентны, то либо $\mathfrak{m} > \mathfrak{n}$, либо $\mathfrak{m} < \mathfrak{n}$.

§ 49. Действия над мощностями определяются по аналогии с множествами конечными.

Предполагая, что два конечных множества M и N не имеют общих элементов, можно составить так называемое соединительное множество (Vereinigungsmenge), в состав которого будуть входить все элементы обоих множеств. Ясно, что число элементов соединительного множества будет равно сумме чисел элементов обоих множеств.

Перенося наши рассуждения на трансфинитные множества, мы определяем мощность соединительного множества, как сумму мощностей заданных, т. е.

$$\mathfrak{m} + \mathfrak{n}$$

Это действие обладает свойствами сочетательными и коммутативными.

Для определения умножения мощностей начнем опять с конечных множеств. Введем понятие о связывающем множестве (Verbindungsmenge).

Возьмем из множеств M и N элементы по одному из каждого множества m и n. Множество всех комбинаций пар (m, n) мы назовем связывающим множеством. Очевидно, что число комбинаций (m, n) будет равно произведению числа чисел m на число чисел n.

Перенося наши рассуждения на трансфинитные множества, мы определяем мощность связывающего множества как произведение мощностей заданных, т. е.

$$\mathfrak{m} \cdot \mathfrak{n}$$

Это умножение сочетательное, коммутативное и распределительное в отношении сложения.

§ 50. Трансфинитное множество может иметь ту же мощность, что и его часть. В этом можно убедиться на таком примере: множество четных чисел:

$$2,\quad 2\cdot 2,\quad 2\cdot 3,\quad \ldots,\quad 2\cdot n, \ldots$$

эквивалентно с множеством всех натуральных чисел:

$$1,\ 2,\ 3,\ \ldots,\ n, \ldots,$$

если за закон сопоставления выберем $2\cdot n$ соответственно n.

Ригористы теории множеств выбирают за определение бесконечного множества его свойство быть эквивалентным с частью, чего нет при конечных множествах.

§ 51. В отличие от обыкновенной алгебры мы имеем:

$$\aleph_0 + \aleph_0 = \aleph_0, \quad \aleph_0 \cdot \aleph_0 = \aleph_0, \tag{1}$$

ибо соединительное множество двух исчислимых — само исчислимо:

$$(a_1,\ a_2,\ a_3, \ldots) + (b_1,\ b_2,\ b_3, \ldots) = (a_1,\ b_1,\ a_2,\ b_2,\ a_3,\ b_3, \ldots)$$

Точно также связывающее множество двух перисчислимых само исчислимо, ибо мы имеем картину:

$$\begin{array}{ccccccc}
a_1b_1 & & a_1b_2 & & a_1b_3 & \ldots \\
 & \swarrow & & \swarrow & & \\
a_2b_1 & & a_2b_2 & & a_2b_3 & \ldots \\
 & \swarrow & & \swarrow & & \\
a_3b_1 & & a_3b_2 & & a_3b_3 & \ldots
\end{array}$$

Неудивительно, что равенства (1) имеют место для трансфинитных чисел.

Покажем пример конкретной алгебры, у которой существуют свойства (1).

Конечно, такая алгебра имеет место не с числами, а с некоторыми другими предметами.

Рассмотрим множество, безразлично конечное или трансфинитное, каких-нибудь определенных предметов. Пусть буквы $a, b, c, \ldots,$ над которыми мы производим действия, суть части нашего множества.

Всякий элемент мы будем считать индивидуально отличным от всех остальных. В каждую букву будет входить каждый элемент только один раз.

Будем под суммой двух букв разуметь соединительное множество этих букв, а под произведением — совокупность общих элементов этих букв. Тогда, очевидно,

$$a + a = a, \quad a \cdot a = a,$$

ибо при сложении и умножении каждый элемент не может входить два раза.

Кантор назвал множество „wohlgeordnet" (вполне упорядоченное), если каждая его часть имеет первый элемент, при известном порядке расположения его элементов.

Он был убежден, что всякое множество эквивалентно некоторому — вполне упорядоченному.

Он называл мощности вполне упорядоченных множеств алефами $\aleph$ и относительно их он нашел ряд важных свойств.

Он показал, что алефы в порядке их возрастания могут быть расположены в ряд:

$$\aleph_0, \aleph_1, \aleph_2, \ldots, \aleph_n,$$

который продолжается до бесконечности.

Предположение Кантора об эквивалентности множеста множеству вполне упорядоченному было доказано Е. Цермело *). Это доказательство вызвало большую полемику, его находили неудовлетворительным следующие математики: Борель, Бер, Лебег, Шенфлис, Пуанкаре. Цермело им подробно отвечал.

Далее необходимо указать на предположение Кантора, что $\aleph_1$ есть мощность континуума, т. е. мощность всех точек прямой.

ЛИТЕРАТУРА

Александров П. С., Колмогоров А. Н., „Введение в теорию функций действительного переменного". — Валле-Пуссен Ш. Ж., „Курс анализа бесконечно малых." — Греллинг В. И., „Теория множеств." — Гоусдорф, „Учение о множествах".

ПОНЯТИЕ О ФУНКЦИИ

§ 52. Рассмотрим два эквивалентных множества $\mathfrak{A}$ и $\mathfrak{B}$. Элементы множества $\mathfrak{A}$ могут быть частными значениями некоторой переменной x, а соответствующие элементы $\mathfrak{B}$ — частными значениями переменной y. Если выбор частных значений x

*) Math. Ann., 65, стр. 111, 1907.

зависит от нашего произвольного выбора, то переменная x называется независимой, соответствующие значения переменной y уже указываются по соответствующим значениям x и тогда переменная y называется зависимою переменною или функциею, что обозначается так:

$$y=f(x)$$

и читается: y есть функция f от x. Какие действия надо произвести над частными значениями x, чтобы осуществить функцию f, — зависит от закона сопоставления элементов множеств $\mathfrak{A}$ и $\mathfrak{B}$.

Ясно, что можно было бы принять y за независимую переменную, тогда x будет ее функция. Эта функция называется обратной относительно f и обозначается знаком:

$$x=\underset{-1}{f}(y)$$

Если сопоставление элементов множеств $\mathfrak{A}$ и $\mathfrak{B}$ взаимно однозначно (biunivoque), то обе функции f и f_1 называются однозначными.

Если среди элементов множеств $\mathfrak{A}$ и $\mathfrak{B}$ находятся одинаковые, то мы приходим к функциям многозначным.

§ 53. Наиболее важным является случай, когда функциональная зависимость обозначается формулами. Целой функцией от нескольких переменных независимых называется такое выражение, которое получается, если над переменными независимыми произвести в конечном числе действия сложения, вычитания, умножения и, как частный случай умножения, возвышения в целую положительную степень, но не деления.

Ясно, что целой функцией будет всякий полином:

$$\sum Ax^{\lambda}y^{\mu}z^{\nu}\ldots t^{\tau},$$

где A—произвольные коэфициенты, x, y, z, ..., t—независимые переменные, показатели λ, μ, ν, ..., τ—некоторые произвольные целые числа или нули. Сумма $\sum$ распространяется на конечное число членов.

Сумма $\lambda+\mu+\nu+\ldots+\tau$ называется степенью члена. Наибольшая из степеней отдельных членов представляет степень функции.

Если степени всех отдельных членов одинаковы, то целая функция называется формой, напр.,

$$x^3+x^2y+xyz$$

Формы 2-ой и 3-ей степени называются соответственно квадратичными и кубичными, формы от двух и трех независимых переменных называются бинарными и тройничными.

Так, например,

$$ax^2+2bxy+cy^2$$

есть бинарная квадратичная форма, а

$$x^3+y^3+z^3+3xyz$$

есть тройничная кубичная.

Алгебраическим уравнением называется всякое уравнение вида:

$$U=0,$$

где U есть целая функция от ряда переменных $x, y, z, \ldots, u, v, \ldots$

Если выражение функции задано прямо через независимые переменные, то такая функция называется явною. Если же для получения выражения функции через независимые переменные нужно решить одно или несколько уравнений, то в таком случае функция называется неявной. Так, например, если функция v от двух переменных x и y задана уравнением:

$$v^2-2xv-y^2=0,$$

то v будет, очевидно, неявной функцией. Эту неявную функцию мы обратим в явную, если решим уравнение относительно v. Получим:

$$v=x\pm\sqrt{x^2+y^2}$$

Если функция может удовлетворять алгебраическому уравнению, связывающему ее с переменными независимыми, то она называется алгебраическою. В обратном случае она называется трансцендентною, т. е. другими словами функция называется трансцендентною, если нельзя подобрать никакого алгебраического уравнения, которому она удовлетворяет.

Рациональною называется такая алгебраическая функция, которая удовлетворяет уравнению первой степени. Если функция не удовлетворяет никакому уравнению первой степени, то функция называется иррациональною.

Рациональная функция v должна удовлетворять уравнению

$$Qv - P = 0,$$

где Q и P целые функции независимых переменных. Мы получим:

$$v = \frac{P}{Q};$$

если Q сводится к постоянному числу, то рациональная функция есть целая.

Если уравнение, которому удовлетворяет иррациональная функция, будет второй, третьей и четвертой степени, то мы можем его решить и найти явное выражение этой функции.

Когда уравнение выше четвертой степени, то задача приведения неявной функции в явную делается в общем случае невозможною и может решаться только в известных частных случаях.

§ 54. Вейерштрасс определяет функцию комплексного переменного рядом:

$$a_0 + a_1 z + a_2 z^2 + a_3 z^3 + \ldots, \tag{1}$$

где a_0, a_1, $a_2, \ldots$ — произвольные коэфициенты из поля I, а $z = x + iy$.

До Вейерштрасса также определял функцию Лагранж (1813), но Лагранж органичивался вещественными значениями, и его соображения были недостаточно строги.

Прежде чем определить функцию $f(z)$ рядом (1), надо доказать, что этот ряд сходящийся, т. е. что сумма n первых его членов:

$$a_0 + a_1 z + a_2 z^2 + \ldots + a_n z^n$$

имеет определенный предел при возрастании n до бесконечности.

Точка зрения Вейерштрасса вошла во всеобщее употребление. Образовалась серьезная теория функций комплексного переменного, которую вследствие ее известности называют просто теорией функций.

В последнее время разрабатывается параллельно теория функций вещественного переменного. Здесь мы имеем большой труд Каратеодори. Теория функций вещественного переменного основывается на изучении свойств поля W. В ней большую роль играет теория множеств.

§ 55. Так как мы начали говорить о теории функций комплексного переменного, то мы должны теперь выяснить, что значит извлечь корень целой степени n из комплексного числа

$$\sqrt[n]{a+bi}$$

и какое значение имеет логарифм от комплексного числа. Функция:

$$v=\sqrt[n]{a+bi}$$

есть иррациональная алгебраическая, как корень алгебраического уравнения:

$$v^n=a+bi$$

Это уравнение называется двучленным.

Перемножим два комплексных числа в их тригонометрической форме:

$$\rho_1(\cos\theta_1+i\sin\theta_1)\cdot\rho_2(\cos\theta_2+i\sin\theta_2)=$$
$$=\rho_1\rho_2\left\{[\cos\theta_1\cos\theta_2-\sin\theta_1\sin\theta_2]+i[\cos\theta_1\sin\theta_2+\cos\theta_2\sin\theta_1]\right\}=$$
$$=\rho_1\rho_2\left\{\cos(\theta_1+\theta_2)+i\sin(\theta_1+\theta_2)\right\}$$

Мы приходим к теореме:

Модуль произведения двух комплексных чисел равен произведению их модулей, а аргумент произведения равен сумме аргументов множителей.

Применяя эту теорему к случаю нескольких одинаковых множителей, получим:

$$[\rho(\cos\theta+i\sin\theta)]^n=\rho^n(\cos n\theta+i\sin n\theta) \tag{1}$$

Отсюда получаем весьма важную формулу Моавра:

$$\cos n\theta+i\sin n\theta=(\cos\theta+i\sin\theta)$$

Покажем, что для каждого числа $a+bi$ соответствует n и только n различных значений радикала $\sqrt[n]{a+bi}$. Обозначим через α и δ модуль и аргумент заданного комплексного числа $a+bi$, а через ρ и θ модуль и один из аргументов искомого радикала:

$$a+bi=\alpha(\cos\delta+i\sin\delta)$$

$$v=\rho(\cos\theta+i\sin\theta)$$

Тогда уравнение

$$v^n=a+bi \tag{2}$$

приводится к такому:

$$\rho^n(\cos n\theta+i\sin n\theta)=\alpha(\cos\delta+i\sin\delta),$$

откуда:

$$\rho^n=\alpha$$

$$n\theta=\delta+2k\pi,$$

где k произвольное целое число

Получаем:

$$\rho=\sqrt[n]{\alpha}, \qquad \theta=\frac{\delta+2k\pi}{n}$$

Здесь $\sqrt[n]{\alpha}$ есть арифметическая величина корня степени n из положительного числа α, т. е. также некоторое положительное число. И мы находим окончательно выражение:

$$\sqrt[n]{a+bi}=v=\sqrt[n]{\alpha}\left\{\cos\frac{\delta+2k\pi}{n}+i\sin\frac{\delta+2k\pi}{n}\right\}$$

Из бесчисленного числа значений различными будут только числа при k, равном:

$$0,\ 1,\ 2,\ 3,\ \ldots,\ n-1$$

Эти значения и будут корнями двучленного уравнения (2).

§ 56. Для выяснения вопроса о значении логарифма от мнимого числа, рассмотрим важное для всей математики иррациональное число:

$$e=2{,}718281828459045\ldots$$

Это число есть предел выражения

$$u_n=\left(1+\frac{1}{n}\right)^n, \tag{1}$$

когда целое число n возрастает до бесконечности. Покажем прежде всего, что выражение (1) возрастает при возрастании n.

Покажем, что разность $u_{n+1}-u_n$ есть положительное число. В самом деле:

$$u_{n+1}-u_n=\left(1+\frac{1}{n+1}\right)^{n+1}-\left(1+\frac{1}{n}\right)^n=$$

$$=\left(1+\frac{1}{n+1}\right)^{n+1}-\left(1+\frac{1}{n}\right)^n\left(1+\frac{1}{n}-\frac{1}{n}\right)= \qquad (2)$$

$$=B^{n+1}-A^{n+1}+\frac{1}{n}\left(1+\frac{1}{n}\right)^n,$$

где

$$B=1+\frac{1}{n+1}, \qquad A=1+\frac{1}{n};$$

так как $A>B$, то можем применить неравенство, известное из элементарной алгебры*):

$$A^{n+1}-B^{n+1}<(A-B)(n+1)A^n$$

Для нашего случая получаем:

$$A-B=\frac{1}{n}-\frac{1}{n+1}=\frac{1}{n(n+1)}$$

$$A^{n+1}-B^{n+1}<\frac{1}{n(n+1)}(n+1)\left(1+\frac{1}{n}\right)^n<$$

$$<\frac{1}{n}\left(1+\frac{1}{n}\right)^n$$

Итак, во второй части равенства (2) первые два члена $B^{n+1}-A^{n+1}$ дают отрицательное число, меньшее по абсолютной величине, чем третий положительный член

$$\frac{1}{n}\left(1+\frac{1}{n}\right)^n,$$

значит:

$$u_{n+1}-u_n>0,$$

что и требовалось доказать.

---

*) Доказательство неравенства такое:

$$A^{n+1}-B^{n+1}=(A-B)(A^n+A^{n-1}B+A^{n-2}B^2+\ldots);$$

заменяя во второй части B бо́льшим числом A, получим неравенство.

Раскладывая по формуле бинома Ньютона, получим:

$$\left(1+\frac{1}{n}\right)^n=1+n\frac{1}{n}+\frac{n(n-1)}{1\cdot 2}\frac{1}{n^2}+\frac{n(n-1)(n-2)}{1\cdot 2\cdot 3}\frac{1}{n^3}\ldots$$

$$=1+1+\frac{1-\frac{1}{n}}{1\cdot 2}+\frac{\left(1-\frac{1}{n}\right)\left(1-\frac{2}{n}\right)}{1\cdot 2\cdot 3}+\ldots<$$

$$<1+1+\frac{1}{1\cdot 2}+\frac{1}{1\cdot 2\cdot 3}+\ldots<$$

$$<1+1+\frac{1}{2}+\frac{1}{2^2}+\frac{1}{2^3}+\ldots<$$

$$<1+\frac{1}{1-\frac{1}{2}}, \text{ или } 3$$

Итак, выражение u_n возрастает, но остается меньше чем 3, значит, оно приближается к пределу, не превосходящему числа 3.

Я считаю, что следует доказать теорему:

Если переменная u_n, возрастающая с возрастанием значка n, остается меньше определенного числа A, то она стремится к некоторому пределу.

Допустим, что переменная не имеет предела; тогда не должно удовлетворяться свойство теоремы Коши, а именно, что всякому ε можно сопоставить такое n, что при всяком p будет:

$$u_{n+p}-u_n<\varepsilon$$

Если мы хотим это отрицать, другими словами, если не всякому ε можно сопоставить число n, то должно существовать по крайней мере одно число ε_1, которому нельзя сопоставить требуемое n. Что же значит, что числу ε_1 нельзя сопоставить число n такое, чтобы независимо от числа p имело место неравенство:

$$u_{n+p}-u_n<\varepsilon_1$$

Это значит, очевидно, что какое бы число n мы ни выбрали, будет по крайней мере при одном целом числе p_1 противоречие этому неравенству, т. е., другими словами, всякому числу n можно будет сопоставить по крайней мере одно целое число p_1, при котором

$$u_{n+p_1}-u_n\geqslant\varepsilon_1$$

Подобным же образом для числа $n+p_1$ можно найти новое число p_2, чтобы было

$$u_{n+p_1+p_2} - u_{n+p_1} \geqslant \varepsilon_1$$

и т. д.; мы получим неравенство:

$$u_{n+p_1+p_2+\ldots+p_k} - u_{n+p_1+p_2+\ldots+p_{k-1}} \geqslant \varepsilon_1;$$

отсюда, складывая, получим:

$$u_{n+p_1+p_2+\ldots+p_k} \geqslant u_n + k\varepsilon_1$$

Мы видим, что при достаточно большом k наша переменная может сделаться сколь угодно большой, что противоречит предположению, что она всегда остается меньше A.

Очевидно, что предел будет больше всякого значения u_n и что этот предел не может превосходить A.

Итак, мы доказали существование числа e.

Вычислим величину

$$e^{x+yi}$$

Сначала вычислим e^x, где x—вещественное число. Покажем, что

$$e^x = \lim_{n=\infty}\left(1+\frac{x}{n}\right)^n \tag{3}$$

Положим, $\dfrac{x}{n}=\dfrac{1}{\alpha}$, где α будет беспредельно возрастать, проходя через дробные значения. Тогда:

$$\left(1+\frac{x}{n}\right)^n = \left(1+\frac{1}{\alpha}\right)^{\alpha x} = \left[\left(1+\frac{1}{\alpha}\right)^{\alpha}\right]^x$$

Нетрудно убедиться, что при возрастании α через дробные значения, как положительные, так и отрицательные,

$$\lim\left(1+\frac{1}{\alpha}\right)^{\alpha} = e$$

и, значит,

$$\lim\left(1+\frac{x}{n}\right)^n = e^x$$

Эта формула дает возможность нам определить функцию e^x для того случая, когда x число комплексное, а потому мы будем определять $e^{\alpha+\beta i}$ при помощи равенства:

$$e^{\alpha+\beta i}=\lim_{n=\infty}\left(1+\frac{\alpha+\beta i}{n}\right)^n$$

Сделаем предварительно весьма важное замечание. Если $n\varepsilon=\omega$, где ω какое-нибудь вещественное число, то

$$\lim_{n=\infty}(1+\varepsilon)^n=\lim\left(1+\frac{\omega}{n}\right)^n=e^\omega,$$

и можно показать, что тот же предел e^ω получится, если $n\varepsilon$ не равняется точно ω, а только стремится к пределу ω. Мы можем взять два каких-нибудь вещественных числа a и b так, что

$$b>n\varepsilon>a$$

$$\left(1+\frac{b}{n}\right)^n>(1+\varepsilon)^n>\left(1+\frac{a}{n}\right)^n,$$

откуда

$$e^b>\lim(1+\varepsilon)^n>e^a$$

Если εn стремится к пределу ω, то можно подобрать числа b и a сколь угодно близкие к ω, удовлетворяющие неравенствам:

$$b>\omega>a,$$

а тогда, следовательно, e^a и e^b будут отличаться от e^ω сколь угодно мало, и

$$\lim_{n=\infty}(1+\varepsilon)^n=e^\omega \tag{4}$$

Обращаемся к вычислению $\lim\left(1+\frac{\alpha+\beta i}{n}\right)^n$.

Обозначим через ρ и θ модуль и аргумент числа $1+\frac{\alpha+\beta}{n}$, и мы получим:

$$\rho\cos\theta=1+\frac{\alpha}{n},\quad \rho\sin\theta=\frac{\beta}{n}$$

Применяя формулу Моавра, получим:

$$\left(1+\frac{\alpha+\beta i}{n}\right)^n=\rho^n(\cos n\theta+i\sin n\theta)$$

Чтобы найти искомый предел, надо найти пределы, к которым приближаются числа ρ^n и $n\theta$; тогда $\lim \rho^n$ будет модулем искомого предела, а $\lim n\theta$ — его аргументом:

$$\rho = \sqrt{\left(1+\frac{\alpha}{n}\right)^2 + \frac{\beta^2}{n^2}};$$

отсюда

$$\rho^n = \left\{\left(1+\frac{\alpha}{n}\right)^2 + \frac{\beta^2}{n^2}\right\}^{\frac{n}{2}};$$

полагая $n = 2m$, получим:

$$\rho^n = \left\{1 + \frac{\alpha}{m} + \frac{\alpha^2+\beta^2}{4m^2}\right\}^m$$

Применяя формулу (4), получим:

$$\varepsilon = \frac{\alpha}{m} + \frac{\alpha^2+\beta^2}{4m^2}$$

В данном случае

$$m\varepsilon = \alpha + \frac{\alpha^2+\beta^2}{4m};$$

отсюда

$$\lim_{m=\infty} m\,\varepsilon = \alpha$$

Итак, мы видим, что

$$\lim \rho^n = e^\alpha$$

Остается теперь найти предел аргумента $n\theta$. Мы имеем:

$$\operatorname{tg}\theta = \frac{\frac{\beta}{n}}{1+\frac{\alpha}{n}},$$

отсюда

$$n\theta = \frac{\beta}{1+\frac{\alpha}{n}}\,\frac{\theta}{\operatorname{tg}\theta},$$

так что

$$\lim n\theta = \beta,$$

ибо малая дуга почти равна своему тангенсу.

Мы получаем знаменитую формулу Эйлера:

$$e^{\alpha+\beta i}=e^{\alpha}(\cos\beta+i\sin\beta) \tag{5}$$

Мы имеем отсюда формулу для логарифма при основании e от комплексного числа:

$$\lg e^{\alpha}(\cos\beta+i\sin\beta)=\alpha+\beta i$$

Комплексное число не меняется, если к β присоединим еще $2k\pi$, где k произвольное целое число.

Следовательно логарифм произвольного комплексного числа:

$$\lg\rho(\cos\beta+i\sin\beta)=\lg\rho+(\beta+2k\pi)\,i, \tag{6}$$

где $\lg\rho$ есть вещественный логарифм от положительного числа ρ.

Логарифмы при основании e называются **натуральными**, и имеют постоянное применение в анализе.

Мнимые логарифмы при других основаниях не рассматриваются, так как они приводят к разным затруднениям.

РЕШЕНИЕ АЛГЕБРАИЧЕСКИХ УРАВНЕНИЙ

§ 57. Начнем с двучленного уравнения третьей степени

$$x^3-1=0, \tag{1}$$

или

$$(x-1)(x^2+x+1)=0$$

Корни уравнения $x^2+x+1=0$ суть:

$$\alpha=\frac{-1+i\sqrt{3}}{2},\quad \beta=\frac{-1-i\sqrt{3}}{2}$$

Тогда три корня уравнения (1) суть:

$$1,\ \alpha,\ \beta$$

Между этими корнями существуют соотношения:

$$1+\alpha+\beta=0,\quad 1+\alpha^2+\beta^2=0,\quad \alpha\beta=1,\quad \alpha=\beta^2,\quad \beta=\alpha^2$$

§ 58. Перейдем теперь к общему уравнению третьей степени:

$$z^3+az^2+bz+c=0$$

Подстановка

$$z=x-\frac{a}{3}$$

приводит это уравнение к такому:

$$x^3+px+q=0 \tag{1}$$

Положим

$$x = u + v,$$

откуда

$$u^3 + v^3 + q + (3uv + p)(u + v) = 0 \tag{2}$$

Так как вместо одной неизвестной мы ввели две, u и v, то можно ввести какое-нибудь новое соотношение.

Положим

$$3uv + p = 0; \tag{3}$$

тогда уравнение (2) обращается в такое:

$$u^3 + v^3 = -q$$

и кроме того

$$u^3 v^3 = -\frac{p^3}{27}$$

Величины u^3 и v^3, как определенные по их сумме и произведению, суть корни уравнения:

$$y^2 + qy - \frac{p^3}{27} = 0 \tag{4}$$

Получаем:

$$u^3 = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}, \quad v^3 = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}},$$

откуда

$$u = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}, \quad v = \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

Так как всякому корню кубическому можно дать 3 значения, то получается 9 корней уравнения (1); но не надо забывать, что надо удовлетворить соотношению (3), и мы получим только три комбинации:

$$\begin{aligned} x_1 &= u + v \\ x_2 &= \alpha u + \beta v \\ x_3 &= \beta u + \alpha v; \end{aligned} \tag{5}$$

здесь u и v произвольно выбранные значения кубических радикалов, удовлетворяющие условию (3).

Формулы (5) получили название формул Кардана.

Ограничимся случаем вещественных p и q.

I.
$$\frac{q^2}{4}+\frac{p^3}{27}>0$$

Тогда u и v можно выбрать вещественными:

$$x_1=u+v$$
$$x_2=-\frac{1}{2}(u+v)+i\sqrt{3}\,\frac{u-v}{2}$$
$$x_3=-\frac{1}{2}(u+v)-i\sqrt{3}\,\frac{u-v}{2}$$

Получается один вещественный корень и два мнимых сопряженных.

II.
$$\frac{q^2}{4}+\frac{p^3}{27}=0, \quad u=v$$
$$x_1=2u, \quad x_2=v, \quad x_3=u$$

Все три корня вещественные, из них два одинаковых.

III.
$$\frac{q^2}{4}+\frac{p^3}{27}<0$$

Тогда u и v — величины мнимые сопряженные:

$$u=\lambda+i\mu, \quad v=\lambda-i\mu;$$
$$x_1=2\lambda, \quad x_2=-\lambda+\mu\sqrt{3}, \quad x_3=-\lambda-\mu\sqrt{3}$$

Все корни вещественные.

Мы видим, что уравнение третьей степени (1) приводится к уравнению второй степени (2), которое называется резольвентой (разрешающей уравнение).

Формулы Кардана позволяют вычислять корни и при мнимых p и q.

§ 59. Обращаемся к уравнению четвертой степени:

$$z^4+Az^3+Bz^2+Cz+D=0;$$

подстановкой

$$z=x-\frac{A}{4}$$

уничтожим коэфициент при x^3, и мы можем рассматривать уравнение:

$$x^4+ax^2+bx+c=0 \tag{1}$$

Представим полином 4-й степени в виде произведения двух квадратных:

$$x^4+ax^2+bx+c=(x^2+\alpha x+\beta)(x^2-\alpha x+\gamma),$$

т. е.

$$-\alpha^2+\beta+\gamma=a, \quad \alpha(\gamma-\beta)=b, \quad \beta\gamma=c \tag{2}$$

Решим эти три уравнения относительно трех букв α, β, γ. Для этой цели исключим две буквы γ и β. Выразим β и γ из двух первых уравнений (2):

$$\beta+\gamma=a+\alpha^2, \quad \gamma-\beta=\frac{b}{\alpha};$$

отсюда:

$$\beta=\frac{a+\alpha^2}{2}-\frac{b}{2\alpha}, \quad \gamma=\frac{a+\alpha^2}{2}+\frac{b}{2\alpha} \tag{3}$$

Заданное уравнение (1) получает вид:

$$\left(x^2+\alpha x+\frac{a+\alpha^2}{2}-\frac{b}{2\alpha}\right)\left(x^2-\alpha x+\frac{a+\alpha^2}{2}+\frac{b}{2\alpha}\right)=0$$

Мы привели задачу к решению двух квадратных уравнений. Остается только найти число α. Подставляя выражения (3) в третье уравнение (2), получим:

$$4\beta\gamma=4c=(a+\alpha)^2-\frac{b^2}{\alpha^2}$$

Это уравнение, по освобождении от дробей, получает вид:

$$\alpha^6+2a\alpha^4+(a^2-4c)\alpha^2-b^2=0$$

Полагая $\alpha^2=y$, мы придем к кубическому уравнению:

$$y^3+2ay^2+(a^2-4c)y-b^2=0 \tag{4}$$

Мы привели решение уравнения (1) к решению кубической резольвенты (4). Достаточно знать один корень этой резольвенты, а тогда, вычисляя $\alpha=\sqrt{y}$, решим вполне заданное уравнение.

§ 80. Покажем, как применить формулы Кардана к случаю комплексных коэфициентов заданного уравнения:

$$x^3+(2+i)\,x+1+i=0$$

Здесь:

$$p=2+i, \quad q=1+i$$

$$\frac{p^3}{27}=\frac{8+3\cdot 4i-3\cdot 2-i}{27}=\frac{2}{27}+\frac{11}{27}i$$

$$\frac{p^3}{27}+\frac{q^2}{4}=\frac{2}{27}+\frac{11}{27}i+\frac{i}{2}=\frac{4}{54}+\frac{49}{54}i=$$

$$=\frac{\sqrt{2417}}{54}(\cos 85^\circ 20'+i\sin 85^\circ 20'), \quad 4^2+49^2=2417$$

$$\sqrt{\ldots}=\frac{\sqrt{2417}}{\sqrt{54}}(\cos 42^\circ 40'+i\sin 42^\circ 40')$$

Будем обозначать знаком

$$\{9{,}97963\}$$

число, логарифм которого есть 9,97963.

$$\sqrt{\ldots}=\{9{,}97963\}\,(\cos 42^\circ 40'+i\sin 42^\circ 40')$$

$$=\{9{,}84610\}+i\,\{9{,}81069\}=0{,}70161+i\,0{,}64669$$

$$-\frac{q}{2}+\sqrt{\cdots}=-\frac{1}{2}-\frac{1}{2}i+0{,}70161+i\,0{,}64669=$$

$$=0{,}20161+i\,0{,}14669$$

$$-\frac{q}{2}-\sqrt{\cdots}=-\frac{1}{2}-\frac{1}{2}i-0{,}70161-i\,0{,}64669=$$

$$=-1{,}20161-i\,1{,}14669$$

$$\sqrt[3]{-\frac{q}{2}+\sqrt{\cdots}}=\sqrt[3]{0{,}2161+i\,0{,}14669}=$$

$$=\sqrt[3]{\{9{,}39677\}}\left(\cos\frac{36^\circ 2'\,20''}{3}+i\sin\frac{36^\circ 2'\,20''}{3}\right)=$$

$$=\{9{,}79892\}\,(\cos 12^\circ 0'\,47''+i\sin 12^\circ 0'\,47'')$$

$$\sqrt[3]{-\frac{q}{2}-\sqrt{\cdots}}=-\sqrt[3]{+1{,}20161+i\,1{,}14669}=$$

$$=-\sqrt[3]{\{0{,}22034\}}\left(\cos\frac{43^\circ 39' 30''}{3}+i\sin\frac{43^\circ 39' 30''}{3}\right)=$$

$$=-\{0{,}07345\}(\cos 14^\circ 33' 10''+i\sin 14^\circ 33' 10'')$$

Проверим теперь произведение uv:

$$uv=-\{9{,}87236\}(\cos 26^\circ 33' 57''+i\sin 26^\circ 33' 57'')=$$

$$=-\frac{\sqrt{5}}{3}\left(\frac{2}{\sqrt{5}}+\frac{1}{\sqrt{5}}\,i\right)=-\frac{p}{3}$$

Итак, вычисленные величины можно принять:

$$x_1=u+v=\{9{,}79892\}\{\cos 12^\circ 0' 47''+i\sin 12^\circ 0' 47''\}-$$

$$-0{,}07345\{\cos 14^\circ 33' 10''+i\sin 14^\circ 33' 10''\}=$$

$$=-0{,}5307-i\,0{,}16657$$

$$x_2=\alpha u+\beta v=\{9{,}79892\}\{\cos 132^\circ 0' 47''+i\sin 132^\circ 0' 47''\}-$$

$$-\{0{,}07345\}\{\cos 254^\circ 33' 10''+i\sin 254^\circ 33' 10''\}=$$

$$=-0{,}10582+i\,1{,}60912$$

$$x_3=\beta u+\alpha v=\{9{,}79892\}\{\cos 252^\circ 0' 47''+i\sin 252^\circ 0' 47''\}-$$

$$-\{0{,}07345\}\{\cos 134^\circ 33' 10''+i\sin 134^\circ 33' 10''\}=$$

$$=0{,}63649-i\,1{,}44265$$

Подобным же образом можно по формулам § 59 вычислять корни уравнения четвертой степени в случае мнимых коэфициентов.

§ 61. В 1770 году Лагранж опубликовал мемуар под заглавием „Réflexions sur la resolution algébrique des équations“. В этой замечательной работе Лагранж подверг обсуждению предложенные до его времени методы решения уравнений третьей и четвертой степени для того, чтобы догадаться, как надо поступать с уравнениями высшей степени.

Лагранж показал, что если прилагать метод составления резольвенты к общему уравнению выше четвертой степени, то резольвента выходит степени более высокой, чем заданное уравнение.

Он высказал мнение, что, вероятно, общие уравнения степени выше четвертой не могут иметь корней, алгебраически выражающихся в функциях от коэфициентов.

Абель показал (1826), что это действительно так.

Еще раньше доказал невозможность алгебраического решения общего уравнения выше четвертой степени Руфини (1799).

Лагранж показал, что резольвента для уравнения пятой степени имеет степень шестую. Мальфати вскоре после мемуара Лагранжа вычислил коэфициенты резольвенты в целых функциях от коэфициентов заданного уравнения; он полагал в заданном уравнении коэфициент при четвертой степени равным нулю.

Кели вывел резольвенту для общего уравнения, когда не равен нулю коэфициент при четвертой степени. Вывод резольвенты Кели можно найти в книге: Д. Граве „Элементы высшей алгебры", 1914.

ГРУППЫ

§ 62. Теория групп настолько же старая по ее внутреннему содержанию, как сама математическая мысль. Она получила окончательную формулировку лишь в последнее время.

В основе ее лежит понятие о так называемой группе однородных предметов, понятие, давшее возможность сблизить самые разнородные части математики.

Формулируем понятие о группе в его современном, самом общем виде. Рассмотрим совокупность $\mathfrak{M}$ некоторых однородных предметов. Эти предметы могут быть самой разнообразной природы: числа, формулы, аналитические операции, геометрические фигуры, механические движения и т. д. Число предметов совокупности $\mathfrak{M}$ может быть как конечное, так и бесконечное.

Установим понятие об операции *сопоставления* или *композиции* предметов совокупности $\mathfrak{M}$.

Предположим, что указаны правила, по которым каждым двум предметам A и B совокупности $\mathfrak{M}$ сопоставляется некоторый элемент C той же совокупности. Такое сопоставление мы назовем *символическим умножением* и будем обозначать:

$$A \cdot B = C$$

Композицию мы будем предполагать, вообще говоря, действием не перестановочным, т. е. будем считать два результата композиции $A.B$ и $B.A$, вообще говоря, различными.

ОПРЕДЕЛЕНИЕ ГРУППЫ

§ 63. Группой называется всякая совокупность G предметов $\mathfrak{M}$, обладающая следующими четырьмя свойствами:

I. Композиция всяких двух предметов совокупности G дает предмет той же совокупности.

II. Композиция предметов совокупности G обладает сочетательным (ассоциативным) законом:

$$A \cdot (B \cdot C) = (A \cdot B) \cdot C$$

III. Существуют в совокупности G предметы I такие, что для всякого предмета A из совокупности G имеет место равенство:

$$A \cdot I = A$$

Предмет I носит название правой единицы группы.

IV. Для некоторой определенной из единиц I и для всякого предмета совокупности G существует в совокупности G другой предмет X, удовлетворяющий равенству:

$$A \cdot X = I$$

Предмет X носит название правого обратного относительно A.

Предметы, входящие в состав группы, носят название ее элементов. Если число элементов группы конечное, то группа называется конечною, в обратном случае — бесконечною.

Число элементов конечной группы называется ее порядком.

Сделаем из наших четырех постулатов прежде всего необходимые выводы.

Покажем, что существует только одна единица в группе.

Допустим, что существуют две единицы I и I_1. На основании постулата IV можем единице I_1 сопоставить элемент X такой, чтобы было:

$$I_1 \cdot X = I \tag{1}$$

Умножаем в смысле композиции это равенство слева на I

$$I_1 \cdot (I_1 \cdot X) = I_1 \cdot I$$
$$(I_1 \cdot I_1) \cdot X = I_1 \cdot I;$$

но I и I_1 — единицы, следовательно,

$$I_1 \cdot I_1 = I_1, \quad I_1 \cdot I = I_1;$$

мы получаем:

$$I_1 \cdot X = I_1$$

Сравнивая с (1), мы видим, что

$$I_1 = I$$

Покажем, что единственная правая единица I есть в то же время и левая.

Положим, что

$$I \cdot A = B \tag{2}$$

Докажем, что $B = A$.

Умножим (2) справа на элемент Y, обратный A:

$$I \cdot A \cdot Y = B \cdot Y,$$

где

$$A \cdot Y = I$$
$$I \cdot I = B \cdot Y = I \tag{3}$$

Сравнивая с (3), получим:

$$A \cdot Y = B \cdot Y$$

Умножая справа на элемент обратный Y, получим:

$$A = B$$

Покажем, наконец, что правый обратный элемент есть в то же время и левый обратный, т.-е. из равенства

$$A \cdot X = I \tag{4}$$

следует:

$$X \cdot A = I \tag{5}$$

В самом деле, умножим равенство (4) слева на X:

$$X \cdot A \cdot X = X$$

и, наконец, умножая справа на элемент правый обратный X, получим равенство (5).

Если композиция всяких двух элементов перестановочна, т. е.

$$A \cdot B = B \cdot A,$$

то группа носит название абелевой, или коммутативной.

§ 64. Покажем примеры групп. Во всяком числовом поле все поле есть группа относительно сложения (в обыкновенном смысле). Ее единица групповая есть обыкновенный нуль, а всякому элементу A соответствует обратный $-A$. Эта группа носит название аддитивной.

Если мы откинем из поля 0, то останется группа относительно умножения (в обыкновенном смысле). Ее групповая единица есть обыкновенная арифметическая единица 1, а всякому элементу A будет соответствовать обратный $\frac{1}{A}$.

Эта группа называется мультипликативной.

ПОДСТАНОВКИ

§ 65. Рассмотрим n предметов:

$$a_1, a_2, a_3, \ldots, a_n$$

Меняя расположение предметов, мы можем получить

$$N = 1 \cdot 2 \cdot 3 \ldots n = n!$$

перемещений этих предметов, которые обозначим:

$$S_1, S_2, S_3, \ldots, S_N$$

Подстановкой мы будем называть действие перехода от одного перемещения S_k к другому S_l. Это действие состоит в изменении значка каждого предмета.

Если мы будем обозначать подстановку знаком

$$\begin{pmatrix} S_l \\ S_k \end{pmatrix},$$

то мы будем иметь полную систему подстановок n предметов:

$$\begin{pmatrix} S_1 \\ S_1 \end{pmatrix} = 1, \begin{pmatrix} S_2 \\ S_1 \end{pmatrix}, \begin{pmatrix} S_3 \\ S_1 \end{pmatrix}, \ldots, \begin{pmatrix} S_N \\ S_1 \end{pmatrix}$$

Если под композицией подстановок S и T мы будем разуметь результат производства подстановок одной вслед за другою, сначала подстановку S, а потом T, то окончательная подстановка, которая получится, и будет ST:

$$ST = U$$

Итак, общая совокупность всех N подстановок обладает свойством группы.

Внутри группы всех подстановок существуют меньшие группы, так называемые делители, или подгруппы.

Родоначальником теории групп подстановок был Лагранж. В мемуаре 1770 года он рассматривает группы подстановок корней x_1, $x_2, \ldots, x_n$ уравнения n-ой степени в связи с рациональными функциями от этих корней:

$$\varphi(x_1, x_2, \ldots, x_n)$$

Лагранж ограничивался буквенными уравнениями, в которых коэфициентам не придается никаких численных значений и, значит, корни которых суть независимые переменные.

Исследования Лагранжа вдохновили Галуа к открытию глубокой теории, которая обнимает как буквенные, так и численные уравнения, в которых коэфициентам заданы численные значения.

Далее мы посвятим особую главу теории Галуа, а пока ограничимся буквенными уравнениями.

§ 66. Всякой рациональной функции от n независимых переменных соответствует некоторая группа подстановок этих переменных, не изменяющих вида этой функции.

Это совершенно очевидно, ибо если две подстановки S и T не изменяют вида φ, то, очевидно, и подстановка ST не будет менять вида φ.

Существует обратное свойство, что всякой группе подстановок соответствует своя функция.

Возьмем выражение:

$$y = \alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_3 + \ldots,$$

где $\alpha_1, \alpha_2, \alpha_3, \cdots$ — различные между собой коэфициенты.

Применим к переменным $x_1, x_2, x_3, \ldots$ подстановки заданной группы:

$$S_1, S_2, S_3, \ldots, S_k \tag{1}$$

Пусть значения y, которые получаются при подстановках, суть:

$$y_1, y_2, \ldots, y_k \tag{2}$$

Тогда функция:

$$(\xi - y_1)(\xi - y_2)\ldots(\xi - y_k), \tag{3}$$

очевидно, не будет меняться при подстановках (1), а будет меняться от всякой новой подстановки. Функция (3) соответствует группе подстановок.

Я буду рассматривать свойства групп подстановок, следуя Лагранжу, в связи с рациональными функциями.

§ 67. Предполагая далее рассмотреть теорию Галуа, ограничимся пока уравнениями буквенными и, следуя Лагранжу, свяжем теорию групп подстановок с рассмотрением рациональных функций от корней:

$$\varphi(x_1, x_2, \ldots, x_n)$$

Мы получим ряд свойств групп подстановок, так сказать, наглядно; эти свойства будут относиться к общего вида группам, не подстановкам.

Если рациональная функция φ не меняется от подстановок группы G, а меняется от всех других, то говорят, что она п р и н а д л е ж и т к группе G.

Так, например, существуют функции:

$$x_1 + x_2 + \ldots + x_n, \quad x_1 x_2 \ldots x_n,$$

которые не меняют своего вида при всех $n!$ подстановках. Они называются с и м м е т р и ч е с к и м и. Отсюда полная группа подстановок называется также с и м м е т р и ч е с к о ю.

С другой стороны, можно составить функцию, которая не меняется только при одной тождественной подстановке и меняется при всех остальных. Одну такую функцию мы видели:

$$\alpha_1 x_1 + \alpha_2 x_2 + \ldots$$

Эта функция принадлежит к группе, состоящей только из одной единичной подстановки. Ее обыкновенно называют функцией Галуа.

§ 68. Пусть функция φ принадлежит к группе:

$$G = 1, S_1, S_2, \ldots, S_{r-1}$$

порядка r, где $r < n!$

Кроме значения $\varphi = \varphi_1$ (происходящего от подстановок группы G), от подстановок, не принадлежащих к группе G, получаются другие значения функции. Пусть всех значений функции будет q:

$$\varphi = \varphi_1, \varphi_2, \varphi_3, \ldots, \varphi_q$$

Пусть одна из подстановок, которые переводят φ_1 в φ_i, будет T_{i-1}, тогда мы получим все подстановки, которые дают значение φ_i, умножая все подстановки группы G на T_{i-1}.

Итак, все подстановки симметрической группы распадаются на q систем:

$$\begin{array}{lllll} G\,.\,1 = 1, & S_1, & S_2, & \ldots, & S_{r-1} \\ GT_1 = T_1, & S_1T_1, & S_2T_1, & \ldots, & S_{r-1}T_1 \\ GT_2 = T_2, & S_1T_2, & S_2T_2, & \ldots, & S_{r-1}T_2 \\ GT_{q-1} = T_{q-1}, & S_1T_{q-1}, & S_2T_{q-1}, & \ldots, & S_{r-1}T_{1-1}; \end{array} \qquad (1)$$

значит, число всех подстановок будет:

$$r \cdot q = n! \qquad (2)$$

Итак, произведение порядка группы G и числа q различных значений функции равняется порядку всей симметрической группы.

Это дает разложение симметрической группы на так называемые сопряженные системы. Из этих систем только первая G. 1 есть группа, а остальные же—не группы, потому что в них нет единицы.

Можно было бы разложить иначе симметрическую группу на сопряженные системы. Будем рассматривать подстановки, которые переводят φ_i в φ_1; за такие подстановки можно принять обратные подстановки T_{i-1}; обозначим эти подстановки U_{i-1}; мы получим тогда системы:

$$\begin{array}{l} 1 . G = 1,\ S_1,\ S_2, \ldots,\ S_{r-1} \\ U_1 G = U_1,\ U_1 S_1,\ U_1 S_2, \ldots,\ U_1 S_{r-1} \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ U_{q-1} G = U_{q-1},\ U_{q-1} S_1,\ U_{q-1} S_2, \ldots,\ U_{q-1} S_{r-1} \end{array} \tag{3}$$

Разложение данной группы P по сопряженным системам относительно подгруппы Q совершается таким же способом при произвольных конечных группах (не подстановках). Получается общая теорема, что если порядок группы P есть m а порядок подгруппы Q есть q, то

$$qr = m,$$

так что порядок подгруппы есть делитель порядка группы. Число r носит название и н д е к с а подгруппы. При подстановках индекс, как мы видели, имеет конкретное значение.

Возьмем произвольный элемент A конечной группы и составим бесконечный ряд степеней:

$$A,\ A^2,\ A^3, \ldots,\ A^n, \ldots \tag{4}$$

Так как все степени суть элементы группы, а число таких элементов конечное, следовательно, среди степеней ряда (4) должны быть одинаковые; пусть

$$A^l = A^{l+q},$$

откуда, умножая на элемент обратный A^l, получим:

$$1 = A^q \tag{5}$$

Пусть будет q наименьшее из чисел, при которых имеет место равенство (5); тогда степени:

$$A^0 = 1,\ A,\ A^2, \ldots, A^{q-1} \tag{6}$$

все различны и образуют, очевидно, группу, порядок которой есть q. Возвышая обе части равенства (5) в степень r, получим:

$$A^m = 1 \tag{7}$$

Мы получаем важное свойство, что возвышение произвольного элемента группы в степень показателя, равного порядку группы, дает единичную подстановку.

Применим формулу (7) к одному вопросу теории чисел.

Рассмотрим так называемые положительные вычеты по модулю k, где k натуральное число. Будем называть вычетом числа x такое натуральное число a, что

$$x = lk + a,$$

причем $a < k$, а l — известным образом выбранное положительное или отрицательное целое число.

Следуя обозначению Гаусса, будем писать:

$$x \equiv a \pmod{k} \tag{8}$$

Этот знак называется сравнением и выражает делимость разности $x - a$ на k. Словами сравнение (8) можно выразить так: „x сравнимо с a по модулю k".

Система вычетов:

$$a_1, a_2, \ldots, a_q$$

по модулю k взаимно простых с k образует группу относительно умножения, ибо всегда

$$a_i a_j \equiv a_s \pmod{k}$$

Порядок q этой группы обозначается через $\varphi(k)$.

Эта функция φ выражает число чисел меньших k и взаимно простых с k. Эйлер показал, как вычислить для всякого k функцию $\varphi(k)$.

Применяя формулу (7), получим известную формулу Эйлера:

$$a^{\varphi(k)} \equiv 1 \pmod{k},$$

где a число взаимно простое с k.

Если $k = p$, где p простое число, то

$$a^{p-1} \equiv 1 \pmod{p},$$

где a не делится на p. Последняя формула выражает так называемую малую теорему Фермата, в отличие от большой, о которой будет сказано во втором томе.

Если $p = 5$, то

$$1^4 = 1 \equiv 1 \pmod{5},\ 2^4 = 16 \equiv 1 \pmod{5},\ 3^4 = 81 \equiv 1 \pmod{5},$$

$$4^4 = 256 \equiv 1 \pmod{5}$$

ИНВАРИАНТНАЯ ПОДГРУППА

§ 69. Введем в рассмотрение так называемое преобразование подгруппы при помощи подстановки T. Опять возьмем наглядный пример рациональной функции.

Пусть подстановка T переводит функцию φ в другую φ_1; очевидно, что T не принадлежит к групе G функции φ.

Найдем, к какой группе будет принадлежать функция φ_1. Эта функция сводится к функции φ при помощи подстановки обратной T, которую мы можем назвать T^{-1}; далее применяем к функции φ все подстановки группы G и, наконец, применим подстановку T, которая вернет функцию φ_1.

Итак, все подстановки, не изменяющие функцию φ_1, суть:

$$1 = T^{-1} \cdot 1 \cdot T,\ T^{-1} S_1 T,\ T^{-1} S_2 T\ , \ldots,\ T^{-1} S_q T, \tag{1}$$

что можно сокращенно обозначить:

$$T^{-1} G T$$

Подстановки (1) суть подстановки, принадлежащие к группе H функции φ_1, которая происходит из функции φ через преобразование переменных при помощи подстановки T.

Поэтому называют преобразованием подстановки S при помощи подстановки T такую новую:

$$U = T^{-1} S T \tag{2}$$

Название „преобразование S при помощи T" оставляют за подстановкой U вида (2) и в общей теории групп.

Подстановки системы (1) образуют группу, ибо, если

$$B_i = T^{-1} S_i T, \quad B_j = T^{-1} S_j T,$$

то

$$B_i B_j = T^{-1} S_i T T^{-1} S_j T = T^{-1} S_i S_j T$$

и если по законам действий в группе G:

$$S_i S_j = S_l, \tag{3}$$

то будет:

$$B_i B_j = B_l \tag{4}$$

Итак, система подстановок B_i есть группа.

Мы видим, что законы композиции в группах G и H одинаковы. Это выражает так называемый изоморфизм двух групп. Так как в теории групп природа элементов группы не играет никакой роли, а все дело состоит в законе композиции, то две изоморфные группы считаются за одну.

Если мы имеем коммутативную групу, то

$$B_i = T^{-1} S_i T = T^{-1} T S_i = S_i,$$

т. е. подстановка не меняется от преобразования.

Итак, обе группы тождественны по изоморфизму:

$$G = H$$

Всякая подгруппа коммутативной (абелевой) группы инвариантная.

Часто бывает другое обстоятельство, что группы H и G совпадают в целом, причем элементы H пробегают элементы G в другом порядке, т. е.

$$T^{-1} S_i T = S_j \tag{5}$$

Мы можем назвать в случае (5), если T пробегает всю симметрическую группу, групу G инвариантной подгруппой.

Если G подгруппа группы G_1, то мы назовем ее инвариантною, если будет:

$$G = T^{-1} G T,$$

когда T пробегает все элементы группы G_1.

§ 70. До сих пор мы рассматривали такие свойства групп подстановок, которые непосредственно переносятся на группы общего характера. Теперь мы перейдем к изучению некоторых важных обстоятельств, которые относятся исключительно к подстановкам.

Введем в рассмотрение понятия о цикле и о транспозиции.

Разделим круг на несколько равных частей и в точках деления укажем переменные независимые:

$$x_1, \ x_2, \ x_3, \ldots,$$

причем так, что увеличение значка должно соответствовать движению по кругу в сторону движения часовой стрелки.

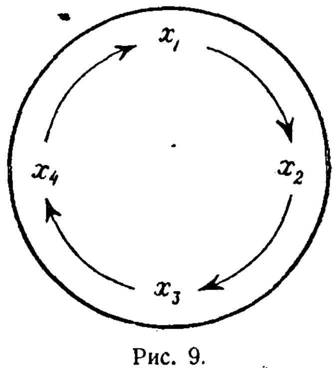

Рис. 9.

Мы будем называть круговой подстановкой или циклом подстановку, в которой x_1 переходит в x_2, x_2

в x_3, x_3 в x_4 и, наконец, x_4 в x_1, причем цикл замыкается. Круговую подстановку записывают знаком:

$$(x_1,\ x_2,\ x_3,\ x_4)$$

Каждая буква цикла переходит в следующую справа и последняя буква переходит в первую.

Всякую подстановку можно переписать в виде произведения циклов.

Пусть S будет некоторая подстановка. Берем одну из букв, перемещаемых этой подстановкой, например a. Пусть эта буква заменяется некоторою другою b. Пусть затем буква b заменяется на c и т. д. Продолжая следить за рядом последовательных букв a, b, $c, \ldots$, необходимо дойдем, наконец, до такой буквы f, которая заменяется первой буквой a. Получим, таким образом, цикл:

$$C_1 = (a,\ b,\ c, \ldots, f)$$

Если этим циклом исчерпываются все буквы, перемещаемые подстановкой S, то сама S есть не что иное, как цикл. Если же цикл C_1 не исчерпывает перемещаемых букв, то берем какую-нибудь из остальных букв, и, оперируя попрежнему, составляем новую группу букв, образующих новый цикл C_2.

Продолжая далее выделение циклов, исчерпаем все буквы, так что будет:

$$S = C_1 C_2 C_3 \ldots$$

Полезно вводить в рассмотрение циклы из одной буквы

$$(a),$$

причем знак (a) указывает, что буква a не меняется.

Например, подстановка

$$S = \begin{pmatrix} f\,b\,a\,e\,d\,g\,c \\ a\,b\,c\,d\,e\,f\,g \end{pmatrix}$$

дает такое разложение на циклы:

$$S = (a\,f\,g\,c)(d\,e)(b)$$

§ 71. Цикл, состоящий из двух букв

$$(a\,b)$$

носит название т р а н с п о з и ц и и. Тут буква a заменяется на b, а b на a.

Всякую подстановку можно представить в виде произведения транспозиций.

Мы видели, что всякая подстановка может быть разложена на произведение циклов.

Покажем, что цикл можно заменить произведением транспозиций. Например,

$$(a\,b\,c\ldots f) = (a\,b)(a\,c)\ldots(a\,f);$$

число транспозиций на единицу меньше порядка цикла. Цикл, перемещающий нечетное число букв, равносилен четному числу транспозиций. Разложение подстановки на произведение транспозиций может быть сделано различными способбми.

В самом деле:

$$1 = (a\,b)(b\,a);$$

такую единицу, состоящую из двух транспозиций, можно ввести в произведение где угодно между множителями.

§ 72. Все подстановки разделяются на четные и нечетные.

Четные подстановки состоят из произведения четного числа транспозиций, а нечетные—из нечетного.

Совокупность четных подстановок составляет группу (которую мы назовем через $\mathfrak{A}$), потому что в произведении четных подстановок будет опять четная подстановка.

Найдем функцию φ, имеющую группу $\mathfrak{A}$. Эта функция есть:

$$\begin{aligned} V = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)\ldots(x_1 - x_n) \\ (x_2 - x_3)(x_2 - x_4)\ldots(x_2 - x_n) \\ (x_3 - x_4)\ldots(x_3 - x_n) \\ \ldots\ldots\ldots\ldots \\ (x_{n-1} - x_n) \end{aligned} \qquad (1)$$

Нетрудно усмотреть, что транспозиция (x_1, x_2) изменяет знак V, подобным образом транспозиция всяких двух букв (x_i, x_k) меняет также знак V, ибо всегда изменением названия букв можно x_i и x_k заменить на x_1 и x_2.

Итак, от четных подстановок функция V не меняется, а от нечетных она обращается в $-V$.

Поэтому функция V называется знакопеременной. Она принадлежит к группе $\mathfrak{A}$, которая также называется знакопеременной.

Укажем ряд свойств знакопеременной группы.

I. Знакопеременная группа заключает все тройные циклы.

Все подстановки $\mathfrak{A}$ могут быть представлены в виде произведения тройных циклов. Справедливость этого следует из того, что всякая пара транспозиций дает в произведении или один или два тройных цикла:

$$\begin{aligned}(a\,b)\,(a\,c) &= (a\,b\,c)\\(a\,b)\,(c\,d) &= (a\,c\,d)\,(a\,c\,b)\end{aligned} \tag{2}$$

II. Знакопеременная группа есть $n-2$ раз транзитивная.

Группа называется $n-2$ раз транзитивной, если произвольные $n-2$ буквы:

$$a_1 a_2 \ldots a_{n-2}$$

могут быть заменены на другие произвольно указанные:

$$b_1 b_2 \ldots b_{n-2}$$

Итак, подстановка, дающая указанную замену, может быть такая:

$$\begin{pmatrix} b_1 b_2 \ldots b_{n-2} b_{n-1} b_n \\ a_1 a_2 \ldots a_{n-2} a_{n-1} a_n \end{pmatrix},$$

где a_{n-1}, a_n, b_{n-1}, b_n—остальные перемещаемые буквы. Пишем в нашей подстановке эти остальные буквы в произвольном порядке. Если подстановка оказывается нечетною, то достаточно переставить буквы b_{n-1}, b_n, т. е. умножить подстановку на транспозицию, и мы получим подстановку из группы $\mathfrak{A}$.

III. Порядок группы $\mathfrak{A}$ есть $\frac{1}{2}n!$

В самом деле, назовем порядок $\mathfrak{A}$ через k, а число подстановок нечетных—через k_1, тогда

$$k + k_1 = n!$$

но через умножение всех подстановок на транспозицию подстановки системы четных подстановок перейдут в нечетные, и обратно, значит:

$$k = k_1 \quad \text{и} \quad k = \frac{1}{2} n!$$

IV. Группа $\mathfrak{A}$ есть инвариантная подгруппа всей симметрической.

Возьмем произвольную подстановку T симметрической группы, тогда

$$T^{-1}\mathfrak{A}T = \mathfrak{A},$$

потому что, если

$$T = (a\,b)(b\,c)\ldots(u\,r),$$

то, очевидно,

$$T^{-1} = (u\,r)\ldots(b\,c)(a\,b),$$

т. е. число транспозиций в T и T^{-1} одинаково, и тогда от умножения подстановки на T справа и на T^{-1} слева прибавляется четное число транспозиций и, следовательно, четность подстановки не меняется.

Группа называется простою, если она не имеет отличной от единицы инвариантной подгруппы, в обратном случае она называется составною. Симметрическая группа есть всегда составная, ибо она всегда имеет инвариантную подгруппу $\mathfrak{A}$.

Покажем, что знакопеременная группа $\mathfrak{A}$ при $n > 4$ простая. На этом свойстве основывается доказательство того, что общие уравнения выше четвертой степени не решаются в радикалах.

Пусть Q будет инвариантная подгруппа группы $\mathfrak{A}$ из n элементов $1, 2, 3, \ldots, n$.

При $n > 4$ группа Q не может заключать среди своих подстановок единичного тройного цикла.

Допустим обратное, пусть в группе Q заключается подстановка (123), но в группе $\mathfrak{A}$ должна заключаться подстановка $\begin{pmatrix} a\,b\,c\,d\,e\ldots \\ 1\,2\,3\,4\,5\ldots \end{pmatrix}$. Преобразовывая цикл (123) при помощи подстановки T, мы должны заменить в цикле элементы 1, 2, 3 на a, b, c, и в группу Q должен входить цикл $(a\,b\,c)$, но при $n > 4$ три элемента a, b, c могут быть произвольно выбраны. Значит, в группу Q входят все тройные циклы, а следовательно, она совпадает со всей группой $\mathfrak{A}$ и не может быть ее подгруппой.

Пусть в Q входит какая-нибудь подстановка S, а T пусть будет произвольно взятая подстановка из всей группы $\mathfrak{A}$. В группу Q должны входить обе подстановки S и $T^{-1}ST$, как в инвариантную подгруппу $\mathfrak{A}$, а следовательно, и подстановка

$$U = S^{-1}T^{-1}ST$$

Мы докажем, что Q не может быть инвариантной подгруппой, показав, что можно во всех случаях подобрать S и T так, чтобы U был одиночный тройной цикл.

Рассмотрим все возможные случаи.

I случай. В подстановку S входит цикл из более чем трех элементов:

$$S = (1\,2\,3\,4 \ldots m)(\ldots)(\ldots)\ldots$$

Возьмем подстановку $T = (1\,2\,3)$, тогда:

$$S^{-1}T^{-1}S = S^{-1}(1\,3\,2)S = (2\,4\,3),$$

и

$$U = (2\,4\,3)\,(1\,2\,3) = (1\,2\,4)$$

II случай. Пусть в подстановку S входят только тройные и двойные циклы. Если в подстановку входит только один тройной цикл и кроме того двойные циклы, то квадрат такой подстановки обратится в одиночный тройной цикл.

Остается рассмотреть случай, когда в подстановку S входит более одного тройного цикла:

$$S = (1\,2\,3)\,(4\,5\,6)\,(\ldots)\,(\ldots)\ldots$$

Возьмем подстановку $T = (1\,3\,4)$, тогда:

$$S^{-1}T^{-1}S = S^{-1}(1\,4\,3)S = (2\,5\,1), \quad U = (2\,5\,1)\,(1\,3\,4) = (1\,2\,5\,3\,4),$$

и мы приходим к разобранному уже случаю I.

III случай. В подстановку S входят только двойные циклы. Случай одного двойного цикла нечего рассматривать, ибо тогда подстановка S нечетная и не входит в группы $\mathfrak{A}$ и Q.

Случай двух циклов можно не рассматривать, ибо тогда на основании (2) § 72 дело тогда сводится к одному или двум тройным циклам, т. е. к случаю II.

Остается случай более двух двойных циклов:

$$S = (1\,2)\,(3\,4)\,(5\,6)\ldots$$

Возьмем $T = (1\,3\,5)$, тогда:

$$S^{-1}T^{-1}S = S^{-1}(1\,5\,3)S = (2\,6\,4),$$

и

$$U = (2\,6\,4)(1\,3\,5),$$

и мы приходим к случаю II.

Итак, во всех случаях при $n > 4$ мы приходим к противоречию. Значит группа $\mathfrak{A}$ простая.

§ 73. Группы разделяются на непрерывные и дискретные. Непрерывные группы суть бесконечные, среди элементов которых находятся бесконечно близкие.

К числу таких групп принадлежат, например, указанные нами уже аддитивная и мультипликативная группы поля I.

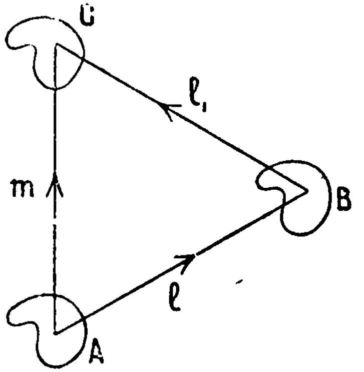

Рис. 10.

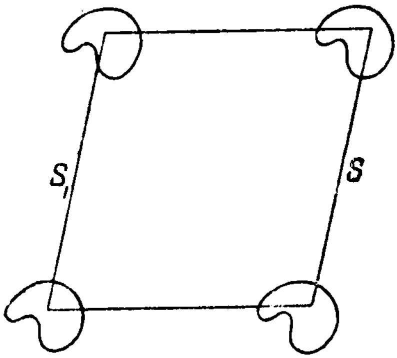

Рис. 11.

Дискретными называются группы, когда условия бесконечной близости между элементами не существуют.

Всякая конечная группа, очевидно, дискретная.

Во второй половине XIX столетия происходила конкуренция двух сильных математиков Клейна и Софуса Ли. Клейн разрабатывал дискретные группы, а Софус Ли—непрерывные и применял их к преобразованию диференциальных уравнений.

В заключение нашего изложения но теории групп мы рассмотрим пример непрерывных групп нечисловых.

Рассмотрим все возможные перемещения в пространстве твердого тела. Они образуют группу относительно композиции, которая состоит в последовательном выполнении перемещений одного за другим.

Рассмотрим движение твердого тела в пространстве, причем будем принимать во внимание только два положения тела:

начальное A и конечное B. Соединим мысленно эти положения жестким стержнем l, предполагая его укрепленным также жестко как к A, так и к B.

Мы получаем мысленно жесткое тело, состоящее из A, l и B, и будем его мысленно перемещать как угодно в пространстве. Как бы тело AlB ни было передвинуто в пространстве, будем его считать одним перемещением от A к B.

Композицию перемещений мы представим себе так: мы приставляем перемещение $A_1l_1B_1$ к перемещению AlB таким образом, чтобы тело A_1 было вполне отождествлено с B, а тогда положение B_1, которое мы будем называть C, даст окончательное перемещение AmC, происходящее от композиции двух перемещений AlB и $A_1l_1B_1$.

Под трансляцией мы будем называть такое перемещение AlB, когда всякая прямая тела будет в двух положениях A и B давать две параллельные прямые.

Пусть S будет одна из трансляций и возьмем произвольное перемещение T, тогда перемещение S_1, полученное из S от преобразования перемещением T, т. е.

$$S_1 = T^{-1}ST,$$

будет, очевидно, также трансляцией.

ОПРЕДЕЛИТЕЛИ

§ 74. Мы будем заниматься решением систем уравнений первой степени, так называемых линейных.

Решая систему двух уравнений:

$$a_1x + b_1y = k_1$$

$$a_2x + b_2y = k_2$$

относительно x и y, мы получим:

$$x = \frac{k_1b_2 - b_1k_2}{a_1b_2 - b_1a_2}, \quad y = \frac{a_1k_2 - k_1a_2}{a_1b_2 - b_1a_2}$$

Имеем систему трех уравнений:

$$a_1x + b_1y + c_1z = k_1$$

$$a_2x + b_2y + c_2z = k_2$$

$$a_3x + b_3y + c_3z = k_3,$$

Решая, получим:

$$x = \frac{k_1b_2c_3 - k_1b_3c_2 - b_1k_2c_3 + b_1k_3c_2 - c_1k_2b_3 - c_1k_3b_2}{a_1b_2c_3 - a_1b_3c_2 - b_1a_2c_3 + b_1a_3c_2 + c_1a_2b_3 - c_1a_3b_2}$$

$$y = \frac{a_1k_2c_3 - a_1k_3c_2 - k_1a_2c_3 + k_1a_3c_2 + c_1a_2k_3 - c_1a_3k_2}{a_1b_2c_3 - a_1b_3c_2 - b_1a_2c_3 + b_1a_3c_2 + c_1a_2b_3 - c_1a_3b_2}$$

$$z = \frac{a_1b_2k_3 - a_1b_3k_2 - b_1a_2k_3 + b_1a_3k_2 + k_1a_2b_3 - k_1a_3b_2}{a_1b_2c_3 - a_1b_3c_2 - b_1a_2c_3 + b_1a_3c_2 + c_1a_2b_3 - c_1a_3b_2}$$

Обращаемся теперь к общему случаю n уравнений с n неизвестными:

$$\begin{aligned} a_1x_1 + b_1x_2 + c_1x_3 + \cdots + e_1x_n &= k_1 \\ a_2x_1 + b_2x_2 + c_2x_3 + \cdots + e_2x_n &= k_2 \\ \cdots\cdots\cdots\cdots & \cdots\cdots \\ a_nx_1 + b_nx_2 + c_nx_3 + \cdots + e_nx_n &= k_n \end{aligned} \tag{1}$$

Решением мы, как увидим дальше, получим формулы вида:

$$x_1 = \frac{\Delta_1}{\Delta}, \quad x_2 = \frac{\Delta_2}{\Delta}, \quad \ldots, \quad x_n = \frac{\Delta_n}{\Delta}, \tag{2}$$

причем вторые части $k_1, k_2, \ldots, k_n$ входят в $\Delta_1, \Delta_2, \ldots, \Delta_n$, а общий знаменатель заключает только коэфициенты перед неизвестными.

Общий знаменатель Δ будет функцией от коэфициентов, которую мы обозначим:

$$\begin{vmatrix} a_1 & b_1 & c_1 & \ldots & e_1 \\ a_2 & b_2 & c_2 & \ldots & e_2 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ a_n & b_n & c_n & \ldots & e_n \end{vmatrix} = \Delta \tag{3}$$

Мы эту функцию определим так, что она равна сумме членов:

$$\pm a_{i_1}b_{i_2}c_{i_3}\ldots e_{i_n},$$

где $i_1, i_2, i_3, \ldots, i_n$ всевозможные перемещения индексов $1, 2, 3, \ldots, n$, совершаемые при помощи подстановок симметрической группы. Мы будем ставить перед буквенным выражением знак $(+)$, если подстановка

$$\begin{pmatrix} i_1 & i_2 & i_3 & \ldots & i_n \\ 1 & 2 & 3 & \ldots & n \end{pmatrix}$$

четная, и знак $(-)$ — при нечетной подстановке.

Итак, мы будем считать:

$$\Delta = \sum (\pm a_{i_1} b_{i_2} c_{i_3} \ldots e_{i_n})$$

Это выражение мы будем называть о п р е д е л и т е л е м (Determinant).

Рассмотрим основные свойства определителей.

О п р е д е л и т е л ь м е н я е т с в о й з н а к п р и п е р е м е щ е н и и д в у х г о р и з о н т а л е й:

$$a_k \; b_k \; c_k \ldots e_k$$

$$a_l \; b_l \; c_l \ldots e_l,$$

потому что такое перемещение соответствует транспозиции

$$(k \;\; l),$$

а от применения транспозиции подстановки четные переходят в нечетные, и обратно, следовательно, члены, имеющие знак (+), получают знак (—), и обратно.

Итак, перестановка двух горизонталей обращает Δ в $-\Delta$.

О п р е д е л и т е л ь р а в е н н у л ю, к о г д а д в е г о р и з о н т а л и о д и н а к о в ы.

С одной стороны, от перестановки одинаковых горизонталей определитель должен был бы менять знак, но так как он не меняется, то:

$$\Delta = -\Delta$$

$$2\Delta = 0$$

$$\Delta = 0$$

О п р е д е л и т е л ь н е м е н я е т с я, к о г д а к ч л е н а м о д н о й г о р и з о н т а л и п р и б а в л я ю т с я с о о т в е т с т в е н н ы е ч л е н ы д р у г о й г о р и з о н т а л и, у м н о ж е н н ы е н а п о с т о я н н ы й м н о ж и т е л ь.

Т. е. если в определителе вместо i-ой горизонтали:

$$a_i \; b_i \; c_i \ldots e_i \tag{4}$$

напишем такую горизонталь:

$$a_i + ma_j, \; b_i + mb_j, \; c_i + mc_j, \; \ldots, \; e_i + me_j \tag{5}$$

Но так как все буквы определителя входят в первой степени, то новый определитель будет состоять из суммы двух определителей. В одном из них i-ая горизонталь будет прежняя (4), а в другом — она обратится в

$$ma_j,\ mb_j,\ mc_j\ \ldots\ me_j;$$

число m можно вывести общим множителем за определитель, и у нас остается определитель, в котором строка (4) заменяется такой:

$$a_j\ b_j\ c_j\ \ldots\ e_j, \tag{6}$$

так что в определителе оказывается две равных горизонтали.

§ 75. Мы обозначали буквами $a, b, c, \ldots$ колонны, а цифрами 1, 2, 3, ... горизонтали. Изменим тепер способ обозначения, причем будем буквами $\alpha, \beta, \gamma, \ldots$ обозначать горизонтали, а цифрами 1, 2, 3, ... — колонны. Мы очень легко придем к заключению, что те свойства определителей, которые мы дали для горизонталей, можно будет перенести на колонны, а именно, перемещение двух колонн изменяет знак определителя; определитель равен нулю, если две колонны одинаковы и т. д. Это показывает, что в определителе можно горизонтали опрокидывать и писать в виде колонн:

$$\begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} = \begin{vmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{vmatrix}$$

Чтобы яснее выразить мою мысль, рассмотрим пример определителя 3-го порядка:

$$\begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} = \begin{vmatrix} \alpha_1 & \alpha_2 & \alpha_3 \\ \beta_1 & \beta_2 & \beta_3 \\ \gamma_1 & \gamma_2 & \gamma_3 \end{vmatrix},$$

так что:

$$a_1 = \alpha_1,\ b_1 = \alpha_2,\ c_1 = \alpha_3,\ a_2 = \beta_1,\ b_2 = \beta_2,\ c_2 = \beta_3,$$

$$a_3 = \gamma_1,\ b_3 = \gamma_2,\ c_3 = \gamma_3$$

Возьмем какой-нибудь член определителя:

$$+ a_3 b_1 c_2 \tag{1}$$

и перепишем его в новых обозначениях:

$$+ \gamma_1 \alpha_2 \beta_3$$

или в естественном порядке букв:

$$+\alpha_2\beta_3\gamma_1 \tag{2}$$

Подстановка члена (1) есть $\begin{pmatrix}3\,1\,2\\1\,2\,3\end{pmatrix}$, а подстановка члена (2) есть $\begin{pmatrix}2\,3\,1\\1\,2\,3\end{pmatrix}$.

Эти подстановки взаимно обратны, ибо

$$\begin{pmatrix}3\,1\,2\\1\,2\,3\end{pmatrix}\begin{pmatrix}2\,3\,1\\1\,2\,3\end{pmatrix}=\begin{pmatrix}1\,2\,3\\1\,2\,3\end{pmatrix}=1$$

Но обратные подстановки состоят из одинакового числа транспозиций только в обратном порядке. Обе обратные подстановки принадлежат к одинаковой четности, и значит, знак члена сохраняется.

Например, в нашем случае:

$$\begin{pmatrix}3\,1\,2\\1\,2\,3\end{pmatrix}=(1\,3)(1\,2),\quad \begin{pmatrix}2\,3\,1\\1\,2\,3\end{pmatrix}=(1\,2)\,(1\,3)$$

Перейдем к общему случаю:

$$\begin{vmatrix}a_1 & b_1 & c_1 & \dots\\ a_2 & b_2 & c_2 & \dots\\ a_3 & b_3 & c_3 & \dots\\ \dots & \dots & \dots & \dots\end{vmatrix}=\begin{vmatrix}\alpha_1 & \alpha_2 & \alpha_3 & \dots\\ \beta_1 & \beta_2 & \beta_3 & \dots\\ \gamma_1 & \gamma_2 & \gamma_3 & \dots\\ \dots & \dots & \dots & \dots\end{vmatrix}$$

Рассмотрим какой-нибудь член определителя:

$$\pm a_{i_1}b_{i_2}c_{i_3}\dots \tag{3}$$

Выразим его в новых обозначениях

$$\pm\alpha_{j_1}\beta_{j_2}\gamma_{j_3}\dots \tag{4}$$

Подстановка члена (3) есть $\begin{pmatrix}i_1\ i_2\ i_3\dots\\1\ \ 2\ \ 3\dots\end{pmatrix}$ Перепишем эту подстановку так, чтобы верхний ряд $i_1\ i_2\dots$ обратить в $1\ 2\ 3\dots$, тогда в нижнем ряду будут некоторые числа $j_1\ j_2\ j_3$, так что:

$$\begin{pmatrix}i_1\ i_2\ i_3\dots\\1\ \ 2\ \ 3\dots\end{pmatrix}=\begin{pmatrix}1\ \ 2\ \ 3\dots\\j_1\ j_2\ j_3\dots\end{pmatrix}$$

Очевидно, что $j_1, j_2, j_3, \ldots$, будут значки в произведении (3), но подстановка (4) будет $\begin{pmatrix} j_1 & j_2 & j_3 & \ldots \\ 1 & 2 & 3 & \ldots \end{pmatrix}$, она будет обратной *) для данной $\begin{pmatrix} 1 & 2 & 3 & \ldots \\ j_1 & j_2 & j_3 & \ldots \end{pmatrix}$.

РАЗЛОЖЕНИЕ ОПРЕДЕЛИТЕЛЯ ПО ЭЛЕМЕНТАМ ГОРИЗОНТАЛИ (КОЛОННЫ)

§ 76. Рассмотрим главную букву определителя a_1, находящуюся сверху диагонали $a_1 b_2 c_3 \ldots e_n$.

Возьмем a_1 за скобку во всех членах, где эта буква входит. Тогда в состав определителя войдет сумма:

$$a_1 M_1 \qquad (1)$$

Члены выражения (1) будут:

$$\pm a_1 b_{i_2} c_{i_3} \ldots e_{i_n}$$

Подстановка, соответствующая этому члену, будет:

$$\begin{pmatrix} 1 & i_2 & i_3 & \ldots & i_n \\ 1 & 2 & 3 & \ldots & n \end{pmatrix} = (1) \begin{pmatrix} i_2 & i_3 & \ldots & i_n \\ 2 & 3 & \ldots & n \end{pmatrix}$$

Мы видим, что подстановки:

$$\begin{pmatrix} 1 & i_2 & i_3 & \ldots \\ 1 & 2 & 3 & \ldots \end{pmatrix} \text{ и } \begin{pmatrix} i_2 & i_3 & \ldots \\ 2 & 3 & \ldots \end{pmatrix}$$

будут иметь одинаковую четность, значит, сумма:

$$\sum (\pm b_{i_2} b_{i_3} \ldots b_{i_n})$$

будет также определитель, который мы можем обозначить:

$$\begin{vmatrix} b_2 & c_2 & \ldots & e_2 \\ b_3 & c_3 & \ldots & e_3 \\ \cdot & \cdot & \cdot & \cdot \\ b_n & c_n & \ldots & e_n \end{vmatrix}$$

Этот определитель имеет на единицу меньшее число горизонталей и колонн; он называется **м и н о р о м**. Он происходит от

---

*) Мы согласно со сказанным в § 65 под подстановкой разумеем переход от нижнего перемещения к верхнему.

откидывания первой горизонтали и первой колонны, т. е. как раз тех, на пересечении которых находятся элемент a_1.

Итак, в состав определителя Δ входят члены:

$$a_1 \begin{vmatrix} b_2 & c_2 & \dots & e_2 \\ \dots & \dots & \dots & \dots \\ b_n & c_n & \dots & e_n \end{vmatrix};$$

таким образом, выражение M_1 в (1) есть минор.

Найдем теперь члены Δ, в состав которых входит a_l; для этого передвинем l-ую горизонталь на верхнее место, чтобы сделать главным элементом a_l. Мы получим от такого передвижения последовательно на одно место множитель:

$$(-1)^{l-1}$$

для определителя. Итак, если мы обозначим через

$$a_l M_l$$

совокупность членов, которые заключают a_l, мы будем иметь:

$$M_l = (-1)^{l-1} \begin{vmatrix} b_1 & c_1 & \dots & e_1 \\ b_2 & c_2 & \dots & e_2 \\ \dots & \dots & \dots & \dots \\ b_{l-1} & c_{l-1} & \dots & e_{l-1} \\ b_{l+1} & c_{l+1} & \dots & e_{l+1} \\ \dots & \dots & \dots & \dots \\ b_n & c_n & \dots & e_n \end{vmatrix},$$

где у нас получается минор определителя после выкидывания первой колонны и l-ой горизонтали.

Итак, мы будем иметь:

$$\Delta = a_1 M_1 + a_2 M_2 + \dots + a_n M_n \qquad (2$$

$$\begin{aligned} b_1 M_1 + b_2 M_2 + \dots + b_n M_n &= 0 \\ c_1 M_1 + c_2 M_2 + \dots + c_n M_n &= 0 \\ \dots\dots\dots\dots\dots\dots & \\ e_1 M_1 + e_2 M_2 + \dots + e_n M_n &= 0 \end{aligned} \qquad (3)$$

Уравнения (3) получаются из выражения (2) через замену элементов a_1, a_2, ... первой колонны элементами других колонн

$b_1, b_2, \ldots, c_1, c_2, \ldots, e_1, e_2, \ldots$; тогда получается определитель, имеющий две одинаковые колонны, что дает нуль.

Теперь мы можем показать решение линейных уравнений (1) § 74. Умножим эти уравнения по порядку на $M_1, M_2, \ldots, M_n$, получим:

$$\Delta x = k_1 M_1 + k_2 M_2 + \ldots + k_n M_n,$$

т. е.

$$\Delta x = \Delta_1, \tag{4}$$

где $\Delta_1 = k_1 M_1 + k_2 M_2 + \ldots + k_n M_n$, т. е. получается определитель, где первая колонна, соответствующая неизвестному x, заменяется колонной вторых частей уравнения.

Если мы желаем найти неизвестное u, соответствующее l-ой колонне, то можно рассуждать так: перенесем l-ую колонну на первое место, тогда коэфициент r займет главное место. Рассуждая подобно раньше сказанному, мы разложим определитель Δ по элементам:

$$r_1, r_2, r_3, \ldots, r_n$$

l-ой колонны, которая теперь есть первая слева. Мы получим

$$\Delta = r_1 R_1 + r_2 R_2 + \ldots + r_n R_n,$$

и неизвестную u мы найдем так:

$$\Delta u = k_1 R_1 + k_2 R_2 + \ldots + k_n R_n,$$

или

$$\Delta u = \Delta_l,$$

где Δ_l получается из определителя Δ заменой l-ой колонны колонной вторых частей $k_1, k_2, \ldots, k_n$.

Итак, мы решили систему (1) § 74:

$$\Delta x = \Delta_1, \quad \Delta y = \Delta_2, \quad \ldots, \quad \Delta t = \Delta_n \tag{5}$$

§ 77. Рассмотрим теперь систему так называемых однородных уравнений, когда вторые части все равны нулю:

$$\left.\begin{aligned} a_1 x + b_1 y + c_1 z + \ldots + e_1 t &= 0 \\ a_2 x + b_2 y + c_2 z + \ldots + e_2 t &= 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_n x + b_n y + c_n z + \ldots + e_n t &= 0 \end{aligned}\right\} \tag{1}$$

На основании равенств (5) предыдущего параграфа мы получим:

$$\Delta x = 0, \quad \Delta y = 0, \quad \ldots, \quad \Delta t = 0$$

Тогда происходит одно из двух.

1. Определитель Δ отличен от нуля, и тогда все неизвестные равны нулю:

$$x = 0, \quad y = 0, \quad z = 0, \quad \ldots, \quad t = 0$$

2. Или же определитель равен нулю, если существуют отличные от нуля неизвестные:

$$\Delta = 0$$

Рассмотрим еще случай $n-1$ однородного линейного уравнения от n неизвестных:

$$ax + by + cz = 0$$
$$a_1x + b_1y + c_1z = 0;$$

тогда неизвестные определяют пропорцию:

$$\frac{x}{\begin{vmatrix} b & c \\ b_1 & c_1 \end{vmatrix}} = \frac{y}{\begin{vmatrix} c & a \\ c_1 & a_1 \end{vmatrix}} = \frac{z}{\begin{vmatrix} a & b \\ a_1 & b_1 \end{vmatrix}},$$

в чем нетрудно убедиться подстановкой вместо x, y, z им пропорциональных определителей.

ИСЧИСЛЕНИЕ МАТРИЦ

§ 78. Совокупность n^2 произвольных чисел, расположенных по следующей квадратной системе:

$$\begin{Vmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \cdot & \cdot & \cdot & \cdot \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{Vmatrix} = \| a_{ik} \|,$$

образуют так называемую квадратичную матрицу порядка n. В определителях мы рассматривали подобную схему, но там мы по элементам a_{ik} находили число, которое называли определителем, здесь же мы рассматриваем самоё картину расположенных в квадрат чисел и считаем эту картину как за объект математического рассуждения, не совмещая с этой картиной никакого обыкновенного числа. Чтобы отличить матрицу от определителя, мы будем с двух сторон писать двойную черту, тогда как для обозначения определителя мы будем писать по одной черте.

Кели*) первый обратил внимание на то, что можно матрицу рассматривать как одно комплексное число. Можно установить правила для сложения и умножения, откуда появится новая алгебра действий над матрицами,

Будем рассматривать всю совокупность I комплексных чисел обыкновенной алгебры; кроме этих чисел будем рассматривать всевозможные матрицы порядка n, элементами которых являются числа I. Эти матрицы вместе с числами i образуют совокупность $\mathfrak{M}$, в состав которой входит совокупность I как часть. Для совокупности $\mathfrak{M}$ числа I называются **скалярными**, а матрицы — величинами **комплексными**.

Будем обозначать матрицы прописными готическими буквами:

$$\mathfrak{A},\ \mathfrak{B},\ \mathfrak{C},\ldots$$

Определение равенства матриц

Две матрицы:

$$\mathfrak{A} = \| a_{ik} \|, \quad \mathfrak{B} = \| b_{ik} \|$$

называются равными, если они тождественны, т. е. если каждый из n^2 элементов матрицы $\mathfrak{A}$ равен соответственному элементу матрицы $\mathfrak{B}$, т. е.

$$\mathfrak{A} = \mathfrak{B},$$

если

$$a_{ik} = b_{ik}$$

$$(i, k = 1, 2, \ldots, n)$$

Определение нуля

Матрица называется **нулем** тогда и только тогда, когда все ее элементы равны нулю.

---

*) Coll. math. papers, 2, c. 475.

Определение сложения матриц

По соответственным элементам a_{ik} і b_{ik} двух матриц $\mathfrak{A}$ і $\mathfrak{B}$ составляется элемент:

$$s_{ik} = a_{ik} + b_{ik}$$

новой матрицы $\mathfrak{S}$. Эту матрицу называют суммой $\mathfrak{A}$ и $\mathfrak{B}$ и пишут:

$$\mathfrak{S} = \mathfrak{A} + \mathfrak{B}$$

Разность $\mathfrak{A} - \mathfrak{B}$ будет, очевидно, такая:

$$\| a_{ik} - b_{ik} \|$$

Мы видим, что матрицы представляют относительно сложения абелеву группу, ибо из определения сложения следует как перестановочный закон:

$$\mathfrak{A} + \mathfrak{B} = \mathfrak{B} + \mathfrak{A},$$

так и сочетательный:

$$\mathfrak{A} + (\mathfrak{B} + \mathfrak{C}) = (\mathfrak{A} + \mathfrak{B}) + \mathfrak{C}$$

Об умножении матриц

§ 79. Обращаемся теперь к определению понятия об умножении матриц, но предварительно скажем несколько слов о так называемых линейных преобразованиях. Для большей наглядности ограничимся случаем матриц третьего порядка:

$$\begin{aligned} x_1 &= a_{11}x_1' + a_{12}x_2' + a_{13}x_3' \\ x_2 &= a_{21}x_1' + a_{22}x_2' + a_{23}x_3' \\ x_3 &= a_{31}x_1' + a_{32}x_2' + a_{33}x_3' \end{aligned} \tag{1}$$

Это преобразование переводит переменные x_1, x_2, x_3 в новые x_1', x_2', x_3'. Это обстоятельство можно записать символически так:

$$x = \mathfrak{A}(x'),$$

где $\mathfrak{A}$ есть матрица $\| a_{ik} \|$ из коэфициентов.

Возьмем другое преобразование, переводящее переменные x_1', x_2', x_3' в новые x_1'', x_2'', x_3'':

$$\begin{aligned} x_1' &= b_{11}x_1'' + b_{12}x_2'' + b_{13}x_3'' \\ x_2' &= b_{21}x_1'' + b_{22}x_2'' + b_{23}x_3'' \\ x_3' &= b_{31}x_1'' + b_{32}x_2'' + b_{33}x_3'' \end{aligned} \tag{2}$$

Эти уравнения можно символически обозначить:

$$x' = \mathfrak{B}(x''),$$

где

$$\mathfrak{B} = \| b_{ik} \|$$

Подставим x_1', x_2', x_3' из (2) в уравнения (1), тогда получим линейное преобразование, дающее перевод от первоначальных: переменных x_1, x_2, x_3 к окончательным x_1'', x_2'', x_3' в таком виде

$$\begin{aligned} x_1 &= c_{11}x_1'' + c_{12}x_2'' + c_{13}x_3'' \\ x_2 &= c_{21}x_1'' + c_{22}x_2'' + c_{23}x_3'' \\ x_3 &= c_{31}x_1'' + c_{32}x_2' + c_{33}x_3'', \end{aligned} \tag{3}$$

что мы обозначим:

$$x = \mathfrak{C}(x''),$$

где

$$\mathfrak{C} = \| c_{ik} \|$$

Мы можем написать символически:

$$x = \mathfrak{A}\mathfrak{B}(x''),$$

так что:

$$\mathfrak{C} = \mathfrak{A}\mathfrak{B}$$

Проделав на самом деле преобразование (2) в уравнениях (1), получим:

$$\begin{aligned} c_{11} &= a_{11}b_{11} + a_{12}b_{21} + a_{13}b_{31} \\ c_{12} &= a_{11}b_{12} + a_{12}b_{22} + a_{13}b_{32} \\ c_{13} &= a_{11}b_{13} + a_{12}b_{23} + a_{13}b_{33}, \\ c_{21} &= a_{21}b_{11} + a_{22}b_{21} + a_{23}b_{31} \\ c_{22} &= a_{21}b_{12} + a_{22}b_{22} + a_{23}b_{32} \\ c_{23} &= a_{21}b_{13} + a_{22}b_{23} + a_{23}b_{33}, \\ c_{31} &= a_{31}b_{11} + a_{32}b_{21} + a_{33}b_{31} \\ c_{32} &= a_{31}b_{12} + a_{32}b_{22} + a_{33}b_{32} \\ c_{33} &= a_{31}b_{13} + a_{32}b_{23} + a_{33}b_{33} \end{aligned} \tag{4}$$

Так как по нашим обозначениям элемента матрицы

$$a_{ik}$$

левый индекс обозначает номер горизонтали, а правый k—номер колонны, то легко увидеть закон составления c_{ik}: умножается элемент i-ой горизонтали первого множителя $\mathfrak{A}$ на соответственный элемент k-ой колонны второго множителя $\mathfrak{B}$, а именно:

$$c_{ik} = a_{i1}b_{1k} + a_{i2}b_{2k} + a_{i3}b_{3k}$$

Такой же закон сохраняется и для общего случая перемножения матриц n-го порядка.

Умножение матриц есть действие, вообще говоря, не перестановочное.

Хотя умножение матриц обладает свойствами сочетательным и распределительным:

$$\mathfrak{A}(\mathfrak{B}\mathfrak{C}) = (\mathfrak{A}\mathfrak{B})\mathfrak{C}$$

$$\mathfrak{A}(\mathfrak{B}+\mathfrak{C}) = \mathfrak{A}\mathfrak{B}+\mathfrak{A}\mathfrak{C},$$

но совокупность $\mathfrak{M}$ не есть коммутативное поле. Отличием является не перестановочность умножения. Еще более важное отличие представляет то обстоятельство, что произведение нескольких матриц может равняться нулю, тогда как ни один из множителей не равен нулю.

Например,

$$\begin{Vmatrix} a_{11} & a_{12} & 0 \\ a_{21} & a_{22} & 0 \\ a_{31} & a_{32} & 0 \end{Vmatrix} \cdot \begin{Vmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ b_{31} & b_{32} & b_{33} \end{Vmatrix} = \begin{Vmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{Vmatrix} = 0$$

§ 80. Будем называть модулем матрицы соответственный ей определитель.

Покажем, что произведение двух определителей матриц $\mathfrak{A}$ и $\mathfrak{B}$ равно определителю матрицы $\mathfrak{C} = \mathfrak{A}\cdot\mathfrak{B}$, что можно записать так:

$$|\mathfrak{C}| = |\mathfrak{A}|\cdot|\mathfrak{B}|$$

Ограничимся разбором случая определителей 3-го порядка; соображения будут одинаковыми и для общего случая определителей порядка n:

$$\begin{vmatrix} a_{11}b_{11}+a_{12}b_{21}+\ldots, & a_{11}b_{12}+a_{12}b_{22}+\ldots, & a_{11}b_{13}+a_{12}b_{23}+\ldots \\ a_{21}b_{11}+a_{22}b_{21}+\ldots, & a_{21}b_{12}+a_{22}b_{22}+\ldots, & a_{21}b_{13}+a_{22}b_{23}+\ldots \\ a_{31}b_{11}+a_{32}b_{21}+\ldots, & a_{31}b_{12}+a_{32}b_{22}+\ldots, & a_{31}b_{13}+a_{32}b_{23}+\ldots \end{vmatrix}$$

Очевидно, что этот определитель будет суммою всевозможных таких:

$$\begin{vmatrix} a_{11}b_{11} & a_{11}b_{12} & a_{12}b_{23} \\ a_{11}b_{11} & a_{21}b_{12} & a_{22}b_{23} \\ a_{11}b_{11} & a_{31}b_{12} & a_{32}b_{23} \end{vmatrix} = b_{11}b_{12}b_{23} \begin{vmatrix} a_{11} & a_{11} & a_{12} \\ a_{21} & a_{21} & a_{22} \\ a_{31} & a_{31} & a_{32} \end{vmatrix}$$

Это выражение равно нулю, так как две колонны равны нулю.

Итак, надо брать только такие комбинации, где первые значки при b различные.

В сумме определителей будет, например, такая комбинация:

$$\begin{vmatrix} a_{12}b_{21} & a_{11}b_{12} & a_{13}b_{33} \\ a_{22}a_{21} & a_{21}b_{12} & a_{23}b_{33} \\ a_{32}b_{21} & a_{31}b_{12} & a_{33}b_{33} \end{vmatrix} = b_{21}b_{12}b_{33} \begin{vmatrix} a_{12} & a_{11} & a_{13} \\ a_{22} & a_{21} & a_{23} \\ a_{32} & a_{31} & a_{33} \end{vmatrix} =$$

$$= -b_{21}b_{12}b_{33} \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = -b_{21}\, b_{12}b_{33}\, |\mathfrak{A}|$$

Итак, наш определитель $|\mathfrak{C}|$ будет равняться сумме:

$$|\mathfrak{C}| = \sum(\pm\, b_{i_1 1}\, b_{i_2 2}\, b_{i_3 3})|\mathfrak{A}| = |\mathfrak{A}| \sum(\pm\, b_{i_1 1}\, b_{i_2 2}\, b_{i_3 3}),$$

где знак зависит от четности перемещений $i_1\, i_2\, i_3$. Значит:

$$|\mathfrak{C}| = |\mathfrak{A}| \cdot |\mathfrak{B}|$$

§ 81. При выводе правила умножения матриц мы умножали элементы горизонтали первого множителя на элементы колонны второго. Мы могли бы установить правило умножения четырьмя различными способами, а именно: умножить горизонтали первого множителя на горизонтали второго, умножить горизонтали на колонны, колонны—на горизонтали, и наконец, колонны—на колонны. В матрицах будут получаться разные результаты. Но определитель не будет изменять своей величины, ибо колонны можно опрокидывать, а горизонтали также обратить в колонны.

Рассмотрим теперь умножение двух матриц не квадратных, по правилу умножения горизонталей на горизонтали. Рассмотрим сначала, когда число колонн меньше числа горизонталей:

$$\begin{Vmatrix} a_1 & a_2 \\ b_1 & b_2 \\ c_1 & c_2 \end{Vmatrix} \cdot \begin{Vmatrix} \alpha_1 & \alpha_2 \\ \beta_1 & \beta_2 \\ \gamma_1 & \gamma_2 \end{Vmatrix};$$

Умножая, как сказано, получим:

$$\begin{Vmatrix} a_1\alpha_1+a_2\alpha_2 & a_1\beta_1+a_2\beta_2 & a_1\gamma_1+a_2\gamma_2 \\ b_1\alpha_1+b_2\alpha_2 & b_1\beta_1+b_2\beta_2 & b_1\gamma_1+b_2\gamma_2 \\ c_1\alpha_1+c_2\alpha_2 & c_1\beta_1+c_2\beta_2 & c_1\gamma_1+c_2\gamma_2 \end{Vmatrix}$$

Определитель подобной матрицы всегда равен нулю. В самом деле, этот определитель может быть переписан так:

$$\begin{vmatrix} a_1\alpha_1+a_2\alpha_2+00 & a_1\beta_1+a_2\beta_2+00 & a_1\gamma_1+a_2\gamma_2+00 \\ b_1\alpha_1+b_2\alpha_2+00 & b_1\beta_1+b_2\beta_2+00 & b_1\gamma_1+b_2\gamma_2+00 \\ c_1\alpha_1+c_2\alpha_2+00 & c_1\beta_1+c_2\beta_2+00 & c_1\gamma_1+c_2\gamma_2+00 \end{vmatrix};$$

он равен произведению двух определителей:

$$\begin{vmatrix} a_1 & a_2 & 0 \\ b_1 & b_2 & 0 \\ c_1 & c_2 & 0 \end{vmatrix} \cdot \begin{vmatrix} \alpha_1 & \alpha_2 & 0 \\ \beta_1 & \beta_2 & 0 \\ \gamma_1 & \gamma_2 & 0 \end{vmatrix}.$$

из которых каждый равен нулю.

Если мы будем перемножать по горизонталям две матрицы с числом горизонталей, меньшим числа колонн:

$$\begin{Vmatrix} a & b & c \\ a_1 & b_1 & c_1 \end{Vmatrix} \quad \text{и} \quad \begin{Vmatrix} \alpha & \beta & \gamma \\ \alpha_1 & \beta_1 & \gamma_1 \end{Vmatrix},$$

то результат умножения будет:

$$\begin{Vmatrix} a\alpha+b\beta+c\gamma & a_1\alpha+b_1\beta+c_1\gamma \\ a\alpha_1+b\beta_1+c\gamma_1 & a_1\alpha_1+b_1\beta_1+c_1\gamma_1 \end{Vmatrix}$$

Эта матрица имеет определитель, который на основании соображений, подобных изложенным в § 80, может быть представлен в виде суммы произведений определителей:

$$\begin{vmatrix} a & b \\ a_1 & b_1 \end{vmatrix} \cdot \begin{vmatrix} \alpha & \beta \\ \alpha_1 & \beta \end{vmatrix} + \begin{vmatrix} a & c \\ a_1 & c_1 \end{vmatrix} \cdot \begin{vmatrix} \alpha & \gamma \\ \alpha_1 & \gamma_1 \end{vmatrix} + \begin{vmatrix} b & c \\ b_1 & c_1 \end{vmatrix} \cdot \begin{vmatrix} \beta & \gamma \\ \beta_1 & \gamma_1 \end{vmatrix}$$

О ПРОИЗВОДНЫХ

§ 82. Рассмотрим задачу о проведении касательной к кривой, определяемой функцией $f(x)$. Уравнение этой кривой будет:

$$y=f(x)$$

Возьмем на кривой точку M, соответствующую значению x независимой переменной. Координаты этой точки будут x и y. Координаты бесконечно близкой точки M_1 на кривой будут:

$$x+\Delta x, \quad y+\Delta y,$$

где Δx и Δy суть приращения x и y.

Возьмем на секущей, проведенной через точки M и M_1, какую-нибудь произвольную точку N с координатами ξ, η. Тогда будем иметь пропорцию:

$$\frac{\xi - x}{\Delta x} = \frac{\eta - y}{\Delta y} \tag{1}$$

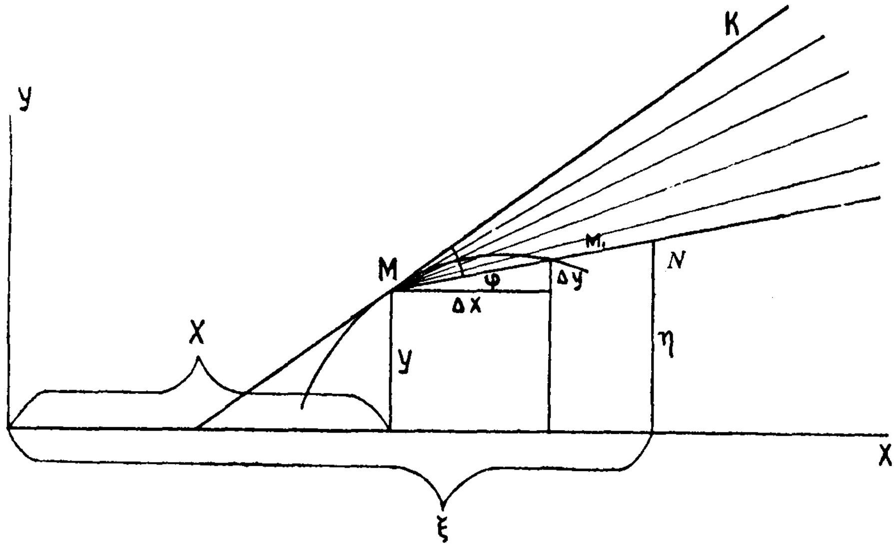

Рис. 12.

При переменных ξ и η мы получаем уравнение первой степени для секущей.

Это уравнение можно написать так:

$$\eta - y = \frac{\Delta y}{\Delta x}(\xi - x)$$

Если мы будем приближать Δx к нулю, то секущая, поворачиваясь около точки x, y, будет стремиться совпасть с к а с а т е л ь н о ю MK к кривой, с точкой касания в M.

Если при приближении Δx к нулю предел $\frac{\Delta y}{\Delta x}$ существует, то он называется производною от функции $f(x)$. Так как этот предел зависит от значения x независимой переменной, то он будет функцией от x, и его обозначают так:

$$f'(x)$$

Существование производной сопровождается существованием касательной. Мы будем иметь:

$$\Delta y = f(x + \Delta x) - f(x), \quad f'(x) = \lim \frac{f(x + \Delta x) - f(x)}{\Delta x}$$

Приложим правило вычисления производной к функции

$$f(x) = x^n,$$

где n целое положительное число.

Мы имеем по формуле Ньютона:

$$(x + \Delta x)^n = x^n + nx^{n-1}\Delta x + \frac{n(n-1)}{1 \cdot 2} x^{n-2} \Delta x^2 + \cdots,$$

тогда:

$$\frac{(x + \Delta x)^n - x^n}{\Delta x} = nx^{n-1} + \Delta x \frac{n(n-1)}{1 \cdot 2} x^{n-2} + \cdots$$

Приближая Δx к нулю, получим:

$$f'(x) = (x^n)' = nx^{n-1}$$

Если мы от первой производной возьмем еще раз производную, то получим вторую производную, которую будем обозначать:

$$f''(x)$$

Продолжая далее брать производные, мы дойдем до производной порядка k:

$$f^{(k)}(x)$$

Ряд производных от функции $f(x) = x^n$ будет:

$$f'(x) = nx^{n-1}$$

$$f''(x) = n(n-1)x^{n-2}$$

$$f'''(x) = n(n-1)(n-2)x^{n-3}$$

. . . .

Постоянный множитель может быть выведен из под знака производной. Если

$$F(x) = cf(x),$$

то

$$\frac{F(x+\Delta x) - F(x)}{\Delta x} = \frac{cf(x+\Delta x) - cf(x)}{\Delta x} = c\frac{f(x+\Delta x) - f(x)}{\Delta x},$$

так что

$$F'(x) = cf'(x)$$

Наконец, очевидно, что производная суммы конечного числа слагаемых равняется сумме производных слагаемых.

Производная постоянного числа равна нулю:

$$\frac{c-c}{\Delta x} = 0$$

§ 83. Дадим понятие о подкасательной.

Очевидно, что производная есть тангенс угла φ, который касательная образует с осью x. Мы получаем:

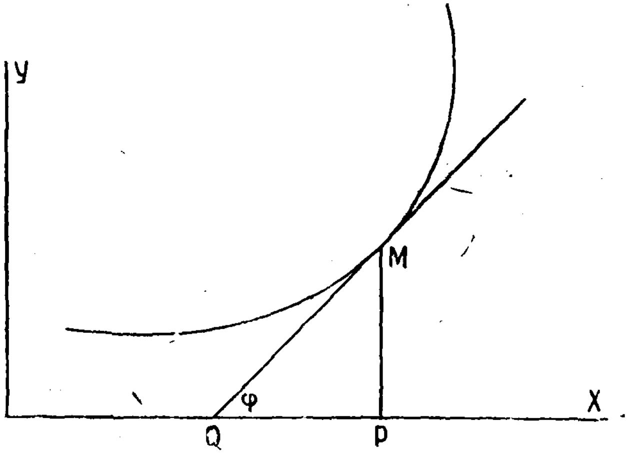

Рис. 13.

$$f'(x) = \frac{MP}{QP}$$

$MP = f(x)$, а QP есть так называемая подкасательная. Мы будем иметь:

$$QP = \frac{f(x)}{f'(x)}$$

ТЕОРЕМА ТЕЙЛОРА

§ 84. Мы имеем:

$$(x+h)^n = x^n + nx^{n-1}h + \frac{n(n-1)}{1\cdot 2}x^{n-2}h^2 + \\ + \frac{n(n-1)(n-3)}{1\cdot 2\cdot 3}x^{n-3}h^3 + \cdots + h^n$$

Если обозначим x^n через $f(x)$, то мы получаем:

$$f(x+h) = f(x) + hf'(x) + \frac{h^2}{1\cdot 2}f''(x) + \\ + \frac{h^3}{1\cdot 2\cdot 3}f'''(x) + \cdots + \frac{h^n}{1\cdot 2\cdots n}f^{(n)}(x) \qquad (1)$$

Это и есть знаменитая формула Тейлора приложения к функции x^n. Она прилагается без всякого изменения вида ко всякой целой функции:

$$f(x) = p_0x^n + p_1x^{n-1} + p_2x^{n-2} + \cdots + p_n \qquad (2)$$

Чтобы в этом убедиться, надо приложить формулу Тейлора к ряду функций:

$$x^n,\ x^{n-1},\ x^{n-2},\ \ldots,\ x,\ 1,$$

затем умножить эти формулы на постоянные:

$$p_0,\ p_1,\ p_2,\ \ldots,\ p_n$$

и сложить, тогда мы заметим, что формула (1) применяется к полиному (2) степени n.

Для другой функции (не полинома) ряд последовательных производных не обрывается, а может быть продолжен до бесконечности. Тогда можно поступать двояко, или оборвать ряд Тейлора на некотором члене

$$\frac{h^n}{1\cdot 2\cdots n}f^n(x)$$

и считать этот ряд за приближение к функции $f(x)$, или же продолжать ряд Тейлора до бесконечности, и тогда возникает серьезный вопрос о сходимости этого ряда, т. е. о том, приближается ли к какому-нибудь пределу ряд, оборванный на степени h^n с увеличением показателя n.

ИСКЛЮЧЕНИЕ

§ 85. В общем анализе, например, при изучении уравнений с частными производными, на каждом шагу говорится об исключении переменных. При этом принимается за принцип, что исключение из $k+l$ уравнений k величин должно оставлять l уравнений относительно всех остальных величин.

Это утверждение делается огулом, причем не выясняется, что надо под этим исключением понимать.

Лишь в алгебраическом анализе вопрос исключения выясняется со всей полнотой.

§ 86. Положим, что требуется исключить одну букву x из двух уравнений первой степени:

$$\begin{aligned} Px - Q &= 0 \\ P_1x - Q_1 &= 0, \end{aligned} \tag{1}$$

где P, Q, P_1, Q_1 могут быть функциями от новых переменных.

В элементарной алгебре давались два принципа исключения одной буквы из двух уравнений. Один способ состоял в сравнении решений обоих уравнений. Другой способ состоял в подстановке решения одного уравнения в другое.

По первому способу, решая оба уравнения, получаем:

$$x = \frac{Q}{P}, \quad x = \frac{Q_1}{P_1}$$

Сравниваем полученные решения

$$\frac{Q}{P} = \frac{Q_1}{P_1},$$

откуда получаем:

$$QP_1 - PQ_1 = 0 \tag{2}$$

По второму способу подставляем решение первого уравнения:

$$x = \frac{Q}{P}$$

во второе, и получаем:

$$P_1 \frac{Q}{P} - Q_1 = 0.$$

Мы приходим к тому же результату исключения (2).

Можно сразу применить соображения параграфа § 77 и получить:

$$\begin{vmatrix} P & Q \\ P_1 & Q_1 \end{vmatrix} = 0$$

§ 87. Обращаемся теперь к общему случаю исключения буквы x из двух алгебраических уравнений степени n и m:

$$p_0 x^n + p_1 x^{n-1} + p_2 x^{n-2} + \ldots + p_n = 0 \qquad (1)$$

$$q_0 x^m + q_1 x^{m-1} + q_2^{m-2} + \ldots + q_m = 0 \qquad (2)$$

Умножая первое уравнение последовательно на

$$x^{m-1},\ x^{m-2},\ \ldots,\ x,\ 1,$$

а второе уравнение — на

$$x^{n-1},\ x^{n-2},\ \ldots,\ x,\ 1,$$

получим $m+n$ уравнений линейных однородных относительно $m+n$ неизвестных:

$$x^{m+n-1},\ x^{m+n-2},\ \ldots,\ x,\ 1$$

Так как одно из неизвестных есть 1, т. е. не равно нулю, следовательно, должен равняться нулю определитель, составленный из коэфициентов:

$$R = \begin{vmatrix} p_0 & p_1 & \ldots & p_n & & & \\ & p_0 & p_1 & \ldots p_n & & & \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ & & & p_0 & p_1 & \ldots & p_n \\ q_0 & q_1 & \ldots & q_m & & & \\ & q_0 & q_1 & \ldots & q_m & & \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ & & & q_0 & q_1 & \ldots & q_m \end{vmatrix}$$

Мы получаем:

$$R = 0; \qquad (3)$$

R есть так называемый р е з у л ь т а н т двух уравнений (1) и (2) относительно буквы x. Он выражается рационально через коэфициенты p_i и q_j этих уравнений.

Равенство (3) есть результат исключения буквы x из двух уравнений (1) и (2).

§ 88. Кронекер указал общий способ, как определять, что такое исключение букв из каких угодно уравнений.

Пусть рассматривается система уравнений от букв:

$$x_1,\ x_2,\ \ldots\ldots,\ x_k,\ y_1,\ y_2,\ldots,\ y_l$$

и пусть каким-либо способом мы получили l уравнений от букв $y_1,\ y_2,\ y_3,\ldots,y_l$. Как убедиться, что эти уравнения представляют настоящий результат исключения букв $x_1, x_2, \ldots, x_k$ из первоначальных уравнений?

Кронекер формулирует задачу исключения так.

Он вводит термин содержание (Inhalt), причем под содержанием он понимает совокупность всех числовых значений $x_1,\ x_2,\ldots,\ x_n$, которые удовлетворяют системе. Так, содержанием системы:

$$Ax+By+Cz+D=0$$

$$A_1x+B_1y+C_1z+D_1=0$$

будут координаты всех точек прямой, которая определяется этими уравнениями.

Таким образом, понятие о содержании в плоской и пространственной геометриях сливается с понятием про ту фигуру, которая определяется нашими уравнениями.

Поясним идеи Кронекера на примере.

Возьмем две линейчатые поверхности второго порядка:

$$s_1(x, y, z)=0, \quad s_2(x, y, z)=0, \tag{1}$$

имеющие общую линейную составляющую, тогда они пересекаются по этой линейной составляющей и еще по косой линии третьего порядка. Координаты точки этой кривой линии третьего порядка в параметрическом виде представляются так:

$$x=\frac{a_1t^3+b_1t^2+c_1t+d_1}{at^3+bt^2+ct+d}$$

$$y=\frac{a_2t^3+b_2t^2+c_2t+d_2}{at^3+bt^2+ct+d} \tag{2}$$

$$z=\frac{a_3t^3+b_3t^2+c_3t+d_3}{at^3+bt^2+ct+d}$$

Вывод уравнений (2) из уравнений (1) можно найти в книге: Ґраве, Аналітична геометрія, 1933 (стр. 224 — 225).

Если мы поставим себе вопрос, можно ли систему из 2-х уравнений (1) считать за результат исключения t из системы трех уравнений (2), то ответ будет отрицательный. Система (2) относительно букв x, y, z дает линию третьего порядка, система же (1), кроме линии третьего порядка, заключает еще общую прямолинейную составляющую.

ЗАВИСИМОСТЬ МЕЖДУ КОЭФИЦИЕНТАМИ И КОРНЯМИ

§ 89. Возьмем уравнение общего вида:

$$f(x) = x^n + p_1 x^{n-1} + p_2 x^{n-2} + \ldots + p_n = 0 \qquad (1)$$

Рассмотрим разность $f(x) - f(a)$, где a произвольное число. Эта разность будет:

$$x^n - a^n + p_1 (x^{n-1} - a^{n-1}) + \ldots + p_{n-1}(x - a) = 0$$

Все разности $x^k - a^k$ делятся на $x - a$ и, следовательно,

$$f(x) - f(a) = (x - a) f_1(x),$$

где $f_1(x)$ полином $n - 1$ степени.

Если a — корень уравнения (1), то

$$f(a) = 0,$$

и мы получим:

$$f(x) = (x - a)\, f_1(x)$$

На основании теоремы Гаусса, что всякий полином имеет по крайней мере один корень, замечаем, что, если мы обозначим его через x_1, то можно в полиноме $f(x)$ выделить разность $x - x_1$:

$$f(x) = (x - x_1) f_1(x)$$

Но и полином $f_1(x)$ должен иметь некоторый корень x_2. Продолжая далее выделение разностей $x - x_1$, $x - x_2$, $x - x_3, \ldots$, получим окончательно:

$$f(x) = (x - x_1)(x - x_2)(x - x_3) \ldots (x - x_n), \qquad (2)$$

где $x_1, x_2, \ldots, x_n$ суть все корни функции $f(x)$.

Сравнивая (1) и (2), получим:

$$\begin{aligned} p_1 &= -x_1 - x_2 - \ldots - x_n = -\sum x \\ p_2 &= \sum x_i x_k \\ p_3 &= -\sum x_i x_k x_l \\ &\ldots\ldots\ldots\ldots \\ p_n &= (-1)^n x_1 x_2 \ldots x_n, \end{aligned} \qquad (3)$$

где в правых частях написаны суммы всевозможных комбинаций корней по одному, по два, по три и так далее.

Итак, коэфициенты p_i суть симметрические функции от корней. Очевидно, что всякая рациональная функция от коэфициентов

$$R(p_1, p_2, \ldots, p_n)$$

будет симметрическою от корней $x_1, x_2, \ldots, x_n$. Покажем обратное, что всякая рациональная функция от корней, имеющая симметрическую группу, может быть представлена в виде рациональной функции от коэфициентов.

§ 90. Предварительно мы рассмотрим, следуя Ньютону, симметрические функции:

$$s_k = x_1^k + x_2^k + \ldots + x_k^n, \qquad (1)$$

которые представляют суммы одинаковых степеней корней.

Рассмотрим производную от функции:

$$f(x) = (x - x_1)(x - x_2) \ldots (x - x_n)$$

Имеем:

$$\frac{f(x+\Delta x) - f(x)}{\Delta x} =$$

$$= \frac{(x+\Delta x - x_1)(x+\Delta x - x_2)\ldots(x+\Delta x - x_n) - (x-x_1)(x-x_2)\ldots(x-x_n)}{\Delta x} =$$

$$= \frac{\Delta x}{\Delta x}\left\{\frac{f(x)}{x-x_1} + \frac{f(x)}{x-x_2} + \ldots + \frac{f(x)}{x-x_n}\right\} + \Delta x \cdot \Phi$$

Приближая к нулю Δx, получим:

$$f'(x) = \frac{f(x)}{x-x_1} + \frac{f(x)}{x-x_2} + \ldots + \frac{f(x)}{x-x_i} + \ldots + \frac{f(x)}{x-x_n}$$

Подставим в это равенство $x = x_i$, получим:

$$f'(x_i) = \left\{ \frac{f(x)}{x - x_i} \right\}_{x = x_i}$$

Отсюда:

$$f'(x_1) = (x_1 - x_2)(x_1 - x_3) \ldots (x_1 - x_n)$$

$$f'(x_2) = (x_2 - x_1)(x_2 - x_3) \ldots (x_2 - x_n)$$

$$f'(x_3) = (x_3 - x_1)(x_3 - x_2)(x_3 - x_4) \ldots (x_3 - x_n)$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$f'(x_n) = (x_n - x_1)(x_n - x_2) \ldots (x_n - x_{n-1})$$

Вычислим

$$\frac{f(x)}{x - x_i} \tag{2}$$

$$\begin{array}{l|l}
x^n + p_1 x^{n-1} + p_2 x^{n-2} + p_3 x^{n-3} + \ldots & x - x_i \\ \cline{2-2}
\mp x^n \pm x_i x^{n-1} & x^{n-1} + (p_1 + x_i) x^{n-2} + (x_i^2 + p_1 x_i + p_2) x^{n-3} + \ldots \\ \cline{1-1}
\quad x^{n-1}(p_1 + x_i) + p_2 x^{n-2} & \\
\quad \pm x^{n-1}(p_1 + x_i) \pm (p_1 x_i + x_i^2) x^{n-2} & \\ \cline{1-1}
\qquad x^{n-2}(x_i^2 + x_i p_1 + p_2) + p_3 x^{n-3} & \\
\qquad \cdots\cdots\cdots\cdots &
\end{array}$$

Деление закончится без остатка, так как x_i есть корень уравнения. Частное имеет вид:

$$\omega_0(x_i) x^{n-1} + \omega_1(x_i) x^{n-2} + \omega_2(x_i) x^{n-3} + \omega_3(x_i) x^{n-4} + \ldots + \omega_{n-1}(x_i),$$

где:

$$\omega_0(x_i) = 1$$

$$\omega_1(x_i) = x_i + p_1$$

$$\omega_2(x_i) = x_i^2 + p_1 x_i + p_2$$

$$\omega_3(x_i) = x_i^3 + p_1 x_i^2 + p_2 x_i + p_3$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$\omega_{n-1}(x_i) = x_i^{n-1} + p_1 x_i^{n-2} + p_2 x_i^{n-3} + \ldots + p_{n-1}$$

Взяв суммы (2) по всем i, получим коэфициенты производной:

$$f'(x) = nx^{n-1} + (n-1)p_1 x^{n-2} + (n-2)p_2 x^{n-3} + \ldots + p_{n-1}$$

Сравнивая коэфициенты $\sum \frac{f(x)}{x - x_i}$ и $f'(x)$, получим равенства:

$$\begin{aligned} &\sum \omega_1(x_i) = (n-1)p_1 \\ &\sum \omega_2(x_i) = (n-2)p_2 \\ &\ldots\ldots\ldots\ldots \\ &\sum \omega_{n-1}(x_i) = p_{n-1} \end{aligned} \qquad (3)$$

Но

$$\begin{aligned} &\sum \omega_1(x_i) = s_1 + np_1 \\ &\sum \omega_2(x_i) = s_2 + s_1 p_1 + np_2 \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ &\sum \omega_{n-1}(x_i) = s_{n-1} + s_{n-2}p_1 + s_{n-3}p_2 + \ldots + np_{n-1}, \end{aligned}$$

а потому раскрывая равенства (3), получим:

$$\begin{aligned} &s_1 + p_1 = 0 \\ &s_2 + p_1 s_1 + 2p_2 = 0 \\ &s_3 + p_1 s_2 + p_2 s_1 + 3p_3 = 0 \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ &s_{n-1} + p_1 s_{n-2} + p_2 s_{n-3} + \ldots + (n-1)p_{n-1} = 0 \end{aligned} \qquad (4)$$

К этой системе надо присоединить еще уравнение:

$$\sum (x_i^n + p_1 x_i^{n-1} + p_2 x_i^{n-2} + \ldots + p_n) = 0,$$

ибо все x_i суть корни нашего уравнения (1) § 89. Мы получаем:

$$s_n + p_1 s_{n-1} + p_2 s_{n-2} + \ldots + np_n = 0 \qquad (5)$$

Получаем систему (4) и (5) n уравнений. Эти уравнения можно решить относительно n неизвестных s_k и выразить их рационально через коэфициенты.

Получаем:

$$\begin{aligned} &s_1 = -p_1 \\ &s_2 = p_1^2 - 2p_2 \\ &s_3 = -p_1^3 + 3p_1 p_2 - 3p_3 \\ &s_4 = p_1^4 - 4p_1^2 p_2 + 4p_1 p_3 + 2p_2^2 - 4p_4 \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned}$$

Важно обратить внимание на то, что все s_k выражаются целыми функциями от коэфициентов $p_1, p_2, \ldots, p_n$ с целыми коэфициентами.

Обратно, при помощи уравнений (4) можно выразить p_1, $p_2, \ldots, p_n$ через s_k. Однако коэфициенты этих формул будут уже дробные:

$$p_1 = -s_1$$

$$2p_2 = s_1^2 - s_2$$

$$6p_3 = -s_1^3 + 3s_1 s_2 - 2s_2$$

$$\cdots\cdots\cdots\cdots\cdots$$

Умножая уравнение (1) § 89 на x, получим:

$$x^{n+1} + p_1 x \ + p_2 x^{n-1} + \ldots + p_n x = 0$$

Суммируя по всем корням

$$\sum (x_i^{n+1} + p_1 x_i^n + \ldots + p_n x_i) = 0,$$

получим:

$$s_{n+1} + p_1 s_n + p_2 s_{n-1} + \ldots + p_n s_1 = 0,$$

что даст s_{n+1} через известные уже $s_1, s_2, \ldots, s_n$.

Умножая уравнения (1) § 89 на x^2 и суммируя, получим выражение s_{n+2} и т. д. Постепенно мы дойдем до вычисления s_k с каким угодно большим значком k. Можно получить s_k с отрицательным значком, если умножить уравнение (1) § 89 на x^{-1}, $x^{-2}, \ldots$ и суммируя.

§ 91. Тепер можем показать, что всякая рациональная симметрическая функция от корней $x_1, x_2, \ldots, x_n$ выражается рациональной функцией от s_k, а значит, и рациональной функцией от p_i.

Рациональная функция есть (§ 53) частное двух целых функций. Остается показать, как выразить через s целую симметрическую функцию. Целая функция от переменных независимых может быть написана так:

$$\sum A x_1^{\lambda_1} x_2^{\lambda_2} \ldots x_n^{\lambda_n},$$

где $\lambda_1, \lambda_2, \ldots, \lambda_n$ — целые числа или нули.

В симметрической функции, кроме члена

$$A x_1^{\lambda_1} x_2^{\lambda_2} \ldots x_n^{\lambda_n},$$

должны находиться все члены

$$A\sum x_1^{\lambda_1}x_2^{\lambda_2}\ldots x_n^{\lambda_n}, \tag{1}$$

где показатели $\lambda_1, \lambda_2, \ldots, \lambda_n$ не меняются при переходе от одного члена к другому, сумма же распространяется на всевозможные перемещения корней. Покажем, как выразить через s суммы подобные (1), а именно:

$$\sum x_1^{\lambda_1}x_2^{\lambda_2}\ldots x_m^{\lambda_m},$$

где $m \leqslant n$ и все показатели различные.

Начнем вычисление со случаев $m=1$, $m=2$, $m=3$ и т. д.

$$m=1. \qquad \sum x_i^{\lambda_1} = s_{\lambda_1}$$

$$m=2. \qquad \sum x_i^{\lambda_1}x_k^{\lambda_2} = \sum_i x_i^{\lambda_1}\left[\sum_k x_k^{\lambda_2} - x_i^{\lambda_2}\right]$$

Так как сумма распространяется на все комбинации различных i и k, то случай $i=k$ исключается. Поэтому при постоянном i суммирование по k должно распространяться на все значки $1, 2, 3, \ldots, n$ за исключением i:

$$\sum x_i^{\lambda_1}x_k^{\lambda_2} = \sum_i x_i^{\lambda_1}\sum_k x_k^{\lambda_2} - \sum x_i^{\lambda_1+\lambda_2} = s_{\lambda_1}s_{\lambda_2} - s_{\lambda_1+\lambda_2}$$

$$m=3. \qquad \sum x_i^{\lambda_1}x_k^{\lambda_2}x_l^{\lambda_3} = \sum x_i^{\lambda_1}x_k^{\lambda_2}\left[\sum_l x_l^{\lambda_3} - x_i^{\lambda_3} - x_k^{\lambda_3}\right] =$$

$$= \sum x_i^{\lambda_1}x_k^{\lambda_2}\sum_l x_l^{\lambda_3} - \sum x_i^{\lambda_1+\lambda_3}x_k^{\lambda_2} - \sum x_i^{\lambda_1}x_k^{\lambda_2+\lambda_3}$$

Итак, мы приходим к суммам случая $m=2$.

Получаем окончательно:

$$\begin{gathered}\sum x_i^{\lambda_1}x_k^{\lambda_2}x_l^{\lambda_3} = \\ = s_{\lambda_3}(s_{\lambda_1}s_{\lambda_2} - s_{\lambda_1+\lambda_2}) - (s_{\lambda_1+\lambda_3}s_{\lambda_2} - s_{\lambda_1+\lambda_2+\lambda_3}) - \\ - (s_{\lambda_2+\lambda_3}s_{\lambda_1} - s_{\lambda_1+\lambda_2+\lambda_3}) = s_{\lambda_1}s_{\lambda_2}s_{\lambda_3} - s_{\lambda_1}s_{\lambda_2+\lambda_3} - s_{\lambda_2}s_{\lambda_1+\lambda_3} - \\ - s_{\lambda_3}s_{\lambda_1+\lambda_2} + 2s_{\lambda_1+\lambda_2+\lambda_3}\end{gathered} \tag{2}$$

Далее мы можем рассматривать случаи $m=4$, $m=5, \ldots$ и приходим последовательно к общему случаю.

Сделаем еще важное замечание, когда в функции (1) среди показателей $\lambda_1, \lambda_2, \ldots, \lambda_m$ существует k одинаковых, тогда от подстановок $x_1, x_2, \ldots, x_k$ получается один и тот же член. Значит, надо общий результат разделить на $1\cdot2\cdot3\ldots k$.

Например, по формуле (2) при $\lambda_1 = \lambda_2$ получим:

$$\sum x_i^{\lambda_1} x_k^{\lambda_1} x_l^{\lambda_3} =$$
$$= \frac{1}{1 \cdot 2} \{ s_{\lambda_1}^2 s_{\lambda_3} - 2 s_{\lambda_1} s_{\lambda_1+\lambda_3} - s_{\lambda_3} s_{2\lambda_1} + 2 s_{2\lambda_1+\lambda_3} \} ;$$

при $\lambda_1 = \lambda_2 = \lambda_3$ получаем:

$$\sum (x_i x_k x_l)^{\lambda_1} = \frac{1}{1 \cdot 2 \cdot 3} \{ s_{\lambda_1}^3 - 3 s_{\lambda_1} s_{2\lambda_1} + 2 s_{3\lambda_1} \}$$

ТЕОРЕМА ЛАГРАНЖА

§ 92. Симметрические функции от корней выражаются через коэфициенты p. Они суть функции рациональные от p:

$$\omega(p_1, p_2, \ldots, p_n) \tag{1}$$

При буквенных уравнениях p суть независимые переменные, при численных уравнениях они уже числа.

Мы при решении уравнений будем считать симметрические функции заданными величинами.

Рассмотрим поле $\Omega(p)$ всех функций (1), коэфициенты которых суть числа из поля I (§ 38).

Мы будем говорить, что функция лежит в поле $\Omega(p)$, если все ее коэфициенты лежат в поле $\Omega(p)$.

Теорема Лагранжа. Если функция ψ не меняется от всех подстановок группы G, к которой принадлежит функция φ, то функция ψ выражается через φ рационально с коэфициентами из поля $\Omega(p)$.

Пусть сопряженные значения функции φ будут:

$$\varphi, \varphi_1, \varphi_2, \ldots, \varphi_{k-1} \tag{2}$$

и положим, что этим значениям соответствуют сопряженные системы подстановок:

$$G, GT_1, GT_2, \ldots, GT_{k-1} \tag{3}$$

Применяя к функции ψ подстановки системы (3), получим ряд функций:

$$\psi, \psi_1, \psi_2, \ldots, \psi_{k-1} \tag{4}$$

Если мы составим сумму:

$$\frac{\psi}{x-\varphi} + \frac{\psi_1}{x-\varphi_1} + \ldots + \frac{\psi_{k-1}}{x-\varphi_{k-1}}, \tag{5}$$

то это будет функция, в которой мы будем считать x за произвольный параметр, и которая не меняется от любой подстановки симметрической группы, ибо, применяя любую подстановку T_0 к ряду систем (3), получим простую перестановку этих систем, значения же ряда (2) функций φ будут перемещаться как значения ряда (4) функций ψ.

Итак, сумма (5) будет рациональная функция от x вида:

$$\frac{H(x)}{F(x)}=\frac{\Phi_1 x^{k-1}+\Phi_2 x^{k-2}+\ldots+\Phi_k}{(x-\varphi_1)(x-\varphi_2)\ldots(x-\varphi_k)},$$

где $\Phi_1, \Phi_2, \ldots, \Phi_k$ суть симметрические функции. Коэфициенты же при различных степенях x в функции $F(x)$ будут также симметрические функции.

Мы получаем формулу Лагранжа:

$$\frac{H(x)}{F(x)}=\frac{\psi}{x-\varphi}+\frac{\psi_1}{x-\varphi_1}+\ldots+\frac{\psi_{k-1}}{x-\varphi_{k-1}}$$

Найдем коэфициент ψ. Умножим обе части равенства на $x-\varphi$ и подставим $x=\varphi$:

$$\frac{H(x)}{\frac{F(x)}{x-\varphi}}=\psi+(x-\varphi)\left\{\frac{\psi_1}{x-\varphi_1}+\ldots\right\}$$

Получаем:

$$\frac{H(\varphi)}{F'(\varphi)}=\psi, \tag{6}$$

что и требовалось доказать.

Если функция ψ не только не меняется от подстановок группы G функции φ, но принадлежит точно к этой группе, т. е. меняется при подстановках, не принадлежащих к группе G, тогда каждая из функций φ и ψ выражается рационально через другую.

§ 93. Чтобы составить себе ясное представление об изложенной в предыдущем параграфе теореме Лагранжа, рассмотрим частный пример.

Возьмем общее уравнение третьей степени:

$$x^3+p_1 x^2+p_2 x+p_3=0 \tag{1}$$

и пусть его корни будут x_1, x_2, x_3.

Рассмотрим две функции $\varphi = x_1 x_2$, $\psi = x_1 + x_2$. Они принадлежат к одной и той же группе, не меняющей буквы x_3.

Их сопряженные величины будут:

$$\varphi = x_1 x_2 \qquad \varphi_1 = x_1 x_3 \qquad \varphi_2 = x_2 x_3$$

$$\psi = x_1 + x_2 \quad \psi_1 = x_1 + x_3 \quad \psi_2 = x_2 + x_3$$

Выразим ψ через φ; тогда для этой цели рассмотрим сумму:

$$\frac{x_1 + x_2}{x - x_1 x_2} + \frac{x_1 + x_3}{x - x_1 x_3} + \frac{x_2 + x_3}{x - x_2 x_3} =$$

$$= \frac{(x_1+x_2)(x-x_1x_3)(x-x_2x_3)+(x_1+x_3)(x-x_1x_2)(x-x_2x_3)+(x_2+x_3)(x-x_1x_2)(x-x_1x_3)}{(x - x_1 x_2)(x - x_1 x_3)(x - x_2 x_3)}$$

$$= \frac{-2p_1 x^2 + (p_1 p_2 + 3p_3)x - 2p_2 p_3}{x^3 - p_2 x^2 + p_2 p_3 x^2 - p_3^2}$$

На основании формулы (6) § 92, получим:

$$\psi = \frac{-2p_1\varphi^2 + (p_1 p_2 - 3p_3)\varphi - 2p_2 p_3}{3\varphi^2 - 2p_2\varphi + p_1 p_3}$$

Если мы хотим обратно выразить φ через ψ, то надо рассмотреть сумму:

$$\frac{x_1 x_2}{x - x_1 - x_2} + \frac{x_1 x_3}{x - x_1 - x_3} + \frac{x_2 x_3}{x - x_2 - x_3} =$$

$$= \frac{x^2 p_2 + x(3p_3 + p_1 p_2) - 3p_1 p_3}{x^3 + 2p_1 x^2 + (2p_1^2 + 2p_2)x + p_1 p_2 + p_3}$$

Значит,

$$\varphi = \frac{p_2\psi^2 + (3p_3 + p_1 p_2)\psi - 3p_1 p_3}{3\psi^2 + 4p_1\psi + 2p_1^2 + 2p_2}$$

О РЕЗУЛЬТАНТЕ

§ 94. Равенство нулю результанта, как мы видели, является необходимым и достаточным условием для того, чтобы уравнения:

$$f(x) = x^n + p_1 x^{n-1} + p_2 x^{n-2} + \dots \tag{1}$$

$$\varphi(x) = x^m + q_1 x^{m-1} + q_2 x^{m-2} + \dots \tag{2}$$

имели по крайней мере один общий корень.

Назовем через $\alpha_1, \alpha_2, \ldots, \alpha_n$ корни (1), а через $\beta_1, \beta_2, \ldots, \beta_m$ — корни (2). Мы можем выразить результант в одной из форм:

$$\varphi(\alpha_1)\varphi(\alpha_2)\ldots\varphi(\alpha_n) \tag{3}$$

$$f(\beta_1)f(\beta_2)\ldots f(\beta_m) \tag{4}$$

Но принимая во внимание, что

$$f(x) = (x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n)$$

$$\varphi(x) = (x-\beta_1)(x-\beta_2)\ldots(x-\beta_m),$$

то результант независимо от знака выразится произведением

$$R = \pm\prod(\alpha_i - \beta_k)$$

Покажем на примере вычисление результанта.

$$x^2 + p_1x + p_2 = 0 \tag{5}$$

$$x^2 + q_1x + q_2 = 0 \tag{6}$$

Пусть корни (5) будут α_1, α_2; тогда

$$R = (\alpha_1^2 + \alpha_1 q_1 + q_2)(\alpha_2^2 + \alpha_2 q_1 + q_2) =$$

$$= \alpha_1^2\alpha_2^2 + q_1(\alpha_1^2\alpha_2 + \alpha_2^2\alpha_1) + q_1^2\alpha_1\alpha_2 + q_1q_2(\alpha_1+\alpha_2) + q_2^2;$$

но

$$\alpha_1\alpha_2 = p_2, \quad \alpha_1 + \alpha_2 = -p_1,$$

и мы получим:

$$R = (q_2 - p_2)^2 - (q_1 - p_1)(p_1q_2 - q_1p_2)$$

ТЕОРЕМА БЕЗУ

§ 95. Рассмотрим две функции от ряда букв x, y, $z, \ldots$ Расположим их по степеням x:

$$f(x) = p_0x^n + p_1x^{n-1} + p_2x^{n-2} + \ldots \tag{1}$$

$$\varphi(x) = q_0x^m + q_1x^{m-1} + q_2x^{m-2} + \ldots \tag{2}$$

Предположим, что коэфициенты p и q заданные функции, которые, таким образом, выражаются через новые переменные $y, z, \ldots$, что целые функции (1) и (2) суть функции самого общего вида степеней n и m относительно всех букв $x, y, z, \ldots$ Значит, в каждой из этих функций должны входить всевозможные члены, буквенные выражения которых x^λ, y^μ, z^ν могут принимать всевозможные значения не отрицательных показателей, сумма которых не выше степени всей функции. Тогда очевидно, что коэфициенты p_i и q_k должны быть целыми функциями общего вида степеней, равных значкам i и k.

Рассмотрим теперь некоторый член результанта R. Так как этот результант есть целая функция от коэфициентов обеих функций, то, значит, каждый его член должен иметь вид:

$$Ap_0^{\lambda_0} p_1^{\lambda_1} p_2^{\lambda_2} \dots p_n^{\lambda_n} q_0^{\mu_0} q_1^{\mu_1} \dots q_m^{\mu_m}, \tag{3}$$

где λ_i и μ_i целые числа, а A есть некоторый числовой коэфициент. Так как степень p_i относительно корней $\alpha_1, \alpha_2, \dots$ есть i, а степень q_j от корней $\beta_1, \beta_2, \dots, \beta_m$ есть j, то степень члена (3) относительно всех корней α и β будет:

$$1 \cdot \lambda_1 + 2\lambda_2 + 3\lambda_3 + \dots + n\lambda_n + 1 . \mu_1 + 2\mu_2 + \dots + m\mu_m;$$

но, с другой стороны,

$$R = \prod (\alpha_i - \beta_k)$$

есть однородная функция степени mn относительно всех корней α и β; значит,

$$1 \cdot \lambda + 2\lambda_2 + \dots + n\lambda_n + 1 \cdot \mu_1 + 2\mu_2 + \dots + m\mu_m = mn \tag{4}$$

Найдем теперь степень члена (3) если выражать все коэфициенты p_i, q_k через названные переменные $y, z, \dots$ Так как степень коэфициентов p_i и q_k равняется значку, то для степени члена (3) получаем то же выражение:

$$1 \cdot \lambda_1 + 2\lambda_2 + \dots + n\lambda_n + 1 \cdot \mu_1 + 2\mu_2 + \dots + m\mu_m$$

Но по формуле (4) мы получаем, что степень результанта R относительно $y, z, \dots$ будет mn, что дает теорему Безу:

Степень результанта, происходящего от исключения переменной из двух уравнений общего вида, равна произведению степеней этих двух уравнений.

В приложении к плоской геометрии мы получаем, что когда мы рассматриваем два уравнения степеней m и n от двух координат x и y, то исключение одной из координат дает уравнение относительно другой координаты степени mn.

Если мы целую функцию $\varphi(x, y)$ степени n от двух координат приравняем нулю, то уравнение

$$\varphi(x, y) = 0$$

даст так называемую кривую n-го порядка.

Таким образом, две общие кривые порядков m и n имеют mn точек пересечения.

Две прямые пересекаются в одной точке, ибо они определяются уравнениями первой степени $(1 \cdot 1 = 1)$.

Всякая прямая пересекает линию n-го порядка в n точках $(1 \cdot n = n)$.

Две кривые второго порядка пересекаются в четырех точках.

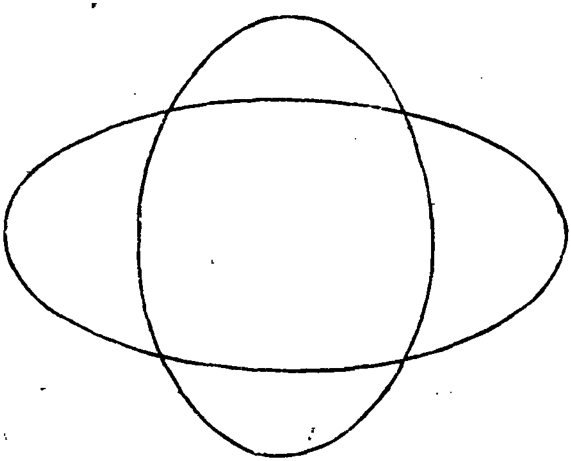

Рис. 14.

Может случиться при особом выборе числовых коэфициентов, что степень результанта будет меньше mn. Это происходит тогда, когда некоторые из точек пересечения двух кривых уходят на бесконечность.

Например, два круга, будучи кривыми 2-го порядка, пересекаются только в двух точках. Все круги проходят через постоянные две мнимые точки на бесконечности, называемые **циклическими** точками.

Вопрос об указании точной степени результанта в том случае, когда эта степень меньше mn, был решен профессором Дерптского университета Миндингом.

Можно видеть это решение в Алгебре Серре (том I, § 278).

Возникает весьма важный вопрос. Если степень результанта не может быть выше mn, то, быть может, понижение степени, о котором писал Миндинг, происходит всегда. Что это не так, можно убедиться на простом примере:

$$f(x,y) = x - y^n = 0, \quad \varphi(x,y) = x^m - y + 1 = 0$$

$$R = y^{mn} - y + 1$$

Безу дал самую общую теорему относительно исключения $k-1$ переменной из k уравнений, заключающих k переменных. Степень результанта исключения букв из уравнений общего вида, коэфициенты которых суть переменные независимые, равен произведению степеней этих уравнений.

ДИСКРИМИНАНТ

§ 96. Рассмотрим теперь результант функции и ее производной, который носит название дискриминанта.

Этот дискриминант D будет

$$\pm f'(x_1)f'(x_2)f'(x_3)\ldots f'(x_n)$$

На основании формул § 89 мы получаем:

$$\begin{aligned}(-1)^{\frac{n(n-1)}{2}} f'(x_1)f'(x_2)\ldots f'(x_n) = \\ = (x_1-x_2)^2(x_1-x_3)^2\ldots(x_1-x_n)^2 \\ (x_2-x_3)^2\ldots(x_2-x_n)^2 \\ \ldots\ldots\ldots\ldots\ldots \\ (x_{n-1}-x_n)^2\end{aligned}$$

Итак,

$$D=\prod(x_i-x_k)^2$$

Равенство нулю дискриминанта есть условие необходимое и достаточное для того, чтобы существовали в уравнении одинаковые так называемые кратные корни.

Вычислим дискриминант для уравнения 3-ей степени

$$x^3+px+q=0; \tag{1}$$

производная будет:

$$3x^2+p=0, \tag{2}$$

тогда дискриминант, независимо от знака, будет:

$$D=(3x_1^2+p)(3x_2^2+p)(3x_3^2+p)=27q^2+4p^3$$

Так как при вычислении результанта можно корни безразлично какого уравнения подставлять в другое, то мы могли бы корни производной подставить в заданное уравнение; получается второй способ вычисления дискриминанта.

Пусть β_1 и β_2 будут корни производной (2), так что

$$\beta_1+\beta_2=0, \quad \beta_1\beta_2=\frac{p}{3}$$

Дискриминант принимает вид:

$$(\beta_1^3+p\beta_1+q)(\beta_2^3+p\beta_2+q)=q^2+\frac{4}{27}p^3$$

Под корнем квадратным в формулах Кардана находится

$$\frac{D}{4\,.\,27}$$

НЕВОЗМОЖНОСТЬ АЛГЕБРАИЧЕСКОГО РЕШЕНИЯ ОБЩИХ УРАВНЕНИЙ ВЫШЕ ЧЕТВЕРТОГО ПОРЯДКА

§ 97. Рассмотрим уравнение

$$x^n+p_1x^{n-1}+p_2x^{n-2}+\ldots+p_n=0, \tag{1}$$

где коэфициенты суть переменные независимые. Его корни $x, x_2, \ldots, x_n$ будут тогда тоже независимыми переменными. Такие общие уравнения часто называют буквенными, подчеркивая этим, что коэфициенты обозначаются буквами, которые можно считать переменными независимыми, так как этим буквам не дается никаких численных значений. В отличие от буквенных другие уравнения называются численными. Откладывая разбор уравнений численных до дальнейшего, мы займемся уравнениями буквенными.

Допустим, что корни выражаются через коэфициенты при помощи радикалов. Начнем с рассмотрения первого (внутреннего) радикала. Мы его можем всегда предполагать простой степени, ибо радикал составной степени rqp:

$$\sqrt[rqp]{\cdots}=\sqrt[r]{\sqrt[q]{\sqrt[p]{\cdots}}}$$

может рассматриваться как последовательность извлечений радикалов простой степени.

Пусть

$$y=\sqrt[p]{\varphi(x_1, x_2, \ldots, x_n)}, \tag{2}$$

причем функция φ будет симметрическая, как рациональная функция от коэфициентов.

Так как после всех присоединений радикалов должно получиться равенство:

$$x_1=\psi(x_1,\ x_2,\ x_3, \cdots, x_n), \tag{3}$$

где ϕ рациональная функция от корней, то радикал (2) должен быть рациональной функцией от корней. В самом деле, если бы радикал (2) был иррациональным от независимых переменных, то невозможно было бы в конце-концов получить формулу (3), ибо иррациональность радикала сохранилась бы до конца, так как эту иррациональность нельзя было бы уничтожить дальнейшим присоединением функций от корней ввиду того, что между корнями не существует никаких соотношений.

Итак, радикал y должен равняться рациональной функции

$$\varphi_1(x_1, x_2, \ldots, x_n)$$

от корней. Эта функция, конечно, не может быть симметрическою, ибо тогда радикал выражался бы рационально через коэфициенты.

Покажем на простом примере, что иррациональный радикал из функции от коэфициентов может выражаться рационально через корни.

Квадрат знакопеременной функции V (1) § 71 есть симметрическая функция от корней, которая есть, как мы уже видели, дискриминантом уравнения:

$$\begin{aligned}\sqrt{D} = (x_1 - x_2)(x_1 - x_3) & \cdots \\ (x_2 - x_3) & \cdots \\ \cdot \; \cdot \; \cdot \; \cdot & \; \cdot\end{aligned}$$

Итак, радикал второй степени из дискриминанта есть рациональная функция от корней.

Например, для квадратного уравнения $x^2 + p_1 x + p_2 = 0$:

$$\sqrt{\frac{p_1^2}{4} - p_2} = \frac{x_1 - x_2}{2}$$

Радикал y (2) будет корнем уравнения:

$$y^p = \varphi(x_1, x_2, \ldots x_n)$$

Итак, предположим, что

$$y = \varphi_1(x_1, x_2, \ldots, x_n)$$

Если мы присоединим уже к коэфициентам уравнения $\sqrt{D}$, что всегда можно сделать, ибо для всякого уравнения можно вычислить его дискриминант, то группа уравнения будет знакопеременной $\mathfrak{A}$, порядок которой есть $\frac{1}{2}n!$ Тогда группа $\mathfrak{A}$ будет играть роль симметрической в том смысле, что всякая рациональная функция от новых коэфициентов (с присоединением $\sqrt{D}$) будет иметь группу $\mathfrak{A}$.

Итак, группа радикала $y = \varphi_1$ будет некоторою подгруппой Q знакопеременной группы.

Различные значения функции φ_1, которые эта функция принимает при всех подстановках $\mathfrak{A}$, будут:

$$\varphi_1, \alpha\varphi_1, \alpha^2\varphi_1, \ldots, \alpha^{p-1}\varphi_1, \tag{4}$$

где α есть корень уравнения $\alpha^p = 1$.

Величины (4) отличаются от φ_1 только множителями α^k, которые суть постоянные числа и не влияют на подстановки корней, а потому все величины (4) имеют одну и ту же группу Q, так что Q есть инвариантная подгруппа $\mathfrak{A}$ индекса p.

Но мы знаем уже, что группа $\mathfrak{A}$ при $n > 4$ простая, а потому уравнение (1) при $n > 4$ не может решаться в радикалах.

§ 98. Уравнения 4-ой степени решаются в радикалах, потому что при $n = 4$ группа $\mathfrak{A}$ не простая. Этот случай мы подробно рассмотрим.

Все перемещения четырех элементов 1, 2, 3, 4 суть:

1 2 3 4	2 1 3 4	3 1 2 4	4 1 2 3
1 2 4 3	2 1 4 3	3 1 4 2	4 1 3 2
1 3 2 4	2 3 1 4	3 2 1 4	4 2 1 3
1 3 4 2	2 3 4 1	3 2 4 1	4 2 3 1
1 4 2 3	2 4 1 3	3 4 1 2	4 3 1 2
1 4 3 2	2 4 3 1	3 4 2 1	4 3 2 1

Эти перемещения получаются из основного 1 2 3 4 при помощи подстановок:

	1	(1 2)	(1 3 2)	(1 4 3 2)
	(3 4)	(1 2) (3 4)	(1 3 4 2)	(1 4 2)
$\sum$	(2 3)	(1 2 3)	(1 3)	(1 4 3)
	(2 4 3)	(1 2 3 4)	(1 3 4)	(1 4)
	(2 4)	(1 2 4 3)	(1 3) (2 4)	(1 4 2 3)
	(2 3 4)	(1 2 4)	(1 3 2 4)	(1 4) (2 3)

Это есть симметрическая группа $\sum$ порядка $1 \cdot 2 \cdot 3 \cdot 4 = 24$. Знакопеременная группа $\mathfrak{A}$ будет:

$$1,\ (1\,2)(3\,4),\ (1\,3)(2\,4),\ (1\,4)(2\,3),$$

$$(1\,2\,3),\ (1\,3\,2),\ (1\,4\,2),\ (1\,2\,4),\ (1\,3\,4),\ (1\,4\,3),\ (2\,3\,4),\ (2\,4\,3)$$

Она имеет порядок $3 \cdot 4 = 12$.

У этой группы есть инвариантная подгруппа $\mathfrak{B}$ порядка 4:

$$1,\ (1\,2)(3\,4),\ (1\,3)(2\,4),\ (1\,4)(2\,3)$$

И, наконец, у этой группы существует инвариантная подгруппа $\mathfrak{B}$ порядка 2:

$$1,\ (1\,2)(3\,4)$$

Окончательно мы приходим при решении уравнения к единичной группе.

Индексы последовательного понижения групп суть:

$$\sum\underbrace{\ }_{2}\mathfrak{A}\underbrace{\ }_{3}\mathfrak{B}\underbrace{\ }_{2}\mathfrak{B}\underbrace{\ }_{2}1$$

И действительно, в решение уравнения 4-й степени входят радикалы 2-ой, 3-ей, 2-ой, 2-ой степеней.

Припомним, что мы сказали в § 59 о решении уравнения 4-й степени.

Так, y есть корень уравнения третьей степени и, значит, по формулам Кардана он вводит радикал квадратный и радикал третьей степени. Далее мы получаем число $\alpha = \sqrt{y}$, что вводит еще один радикал квадратный и, наконец, подставляя α в квадратные уравнения, получим еще последний радикал 2-ой степени.

Теперь нам следует перейти к рассмотрению численных уравнений, т. е. к изложению теории Галуа, но предварительно мы нуждаемся в ряде новых фактов из исследований старых математиков.

ОБЩИЙ НАИБОЛЬШИЙ ДЕЛИТЕЛЬ ДВУХ ПОЛИНОМОВ

§ 99. В элементарной алгебре даются правила для деления одного полинома на другой. Эти правила аналогичны правилам деления целых чисел.

Изложенные в § 9 правила нахождения общего наибольшего делителя двух целых чисел переводятся дословно на полиномы.

Пусть заданы два полинома

$$a \text{ и } b$$

и пусть полином a имеет степень не ниже b, тогда можем делить a на b. Пусть частное будет q, а остаток r, который будет полином степени меньше b.

Мы будем иметь последовательные равенства:

$$a = bq + r$$

$$b = rq_1 + r_1$$

$$\cdot \; \cdot \; \cdot \; \cdot \; \cdot \; \cdot$$

$$r_{n-2} = r_{n-1} q_n + r_n$$

Так как степени остатков $r, r_1, r_2, \ldots, r_n$ идут убывая, то после конечного числа операций мы дойдем до остатка нулевой степени, который будет постоянным числом. Если он не равен нулю, то полиномы a и b взаимно простые и не имеют общих корней. Если он равен нулю, то полиномы имеют общие корни. Значит, это постоянное, равное нулю число будет результантом двух полиномов.

Когда результант равен нулю, то $r_n = 0$ и предыдущий остаток r_{n-1} будет общим наибольшим делителем двух полиномов.

Если общий наибольший делитель — первой степени, то оба полинома имеют только один общий корень, который получается, когда приравним нулю общий наибольший делитель:

$$\alpha x + \beta = 0$$

Коэфициенты α и β этого наибольшего делителя выражаются рационально через коэфициенты обоих полиномов, ибо никаких иррациональных действий при последовательных делениях мы не производим.

Если мы будем считать коэфициенты обоих полиномов заданными числами, то будет заданным числом также и общий корень двух полиномов, если только он единственный.

ОСВОБОЖДЕНИЕ УРАВНЕНИЯ ОТ КРАТНЫХ КОРНЕЙ

§ 100. В формуле (10) Тейлора § 84 заменяем:

$$x \text{ на } a$$

$$h \text{ на } x-a$$

Получаем формулу:

$$f(x)=f(a)+(x-a)f'(a)+\frac{(x-a)^2}{1\cdot 2}f''(a)+\ldots$$
$$\ldots+\frac{(x-a)^{k-1}}{(k-1)!}f^{(k-1)}(a)+(x-a)^k Q,$$

где

$$Q=\frac{1}{k!}f^{(k)}(a)+\frac{1}{(k+1)!}(x-a)f^{(k+1)}(a)+\ldots$$

Чтобы корень a был k-кратный, необходимо, чтобы $f(x)$ делилась на $(x-a)^k$.

От такого деления мы имеем частное Q и остаток

$$f(a)+(x-a)f'(a)+\frac{(x-a)^2}{1\cdot 2}f''(a)+\ldots+\frac{(x-a)^{k-1}}{(k-1)!}f^{(k-1)}(a)$$

Этот остаток должен тождественно равняться нулю, и мы получаем условия необходимые:

$$f(a)=0,\ f'(a)=0,\ f''(a)=0,\ \ldots,\ f^{(k-1)}(a)=0 \tag{1}$$

Для получения достаточных условий надо, чтобы частное Q не делилось более на $x-a$, т. е.

$$f^{(k)}(a)\neq 0 \tag{2}$$

Очевидно, что корень a кратности k для $f(x)$ будет кратности $k-1$ для производной $f'(x)$.

Итак, если

$$f(x)=(x-a)^\lambda (x-b)^\mu \ldots (x-g)^\tau,$$

то производная будет иметь вид:

$$(x-a)^{\lambda-1}(x-b)^{\mu-1}\ldots(x-g)^{\tau-1}\varphi(x),$$

где функция $\varphi(x)$ не имеет большее число корней, чем функция $f(x)$.

Если все корни заданной функции будут простые, т. е.

$$\lambda=\mu=\ldots=\tau=1,$$

то производная равна $\varphi(x)$.

Общий наибольший делитель функции и проиводной будет:

$$P = (x-a)^{\lambda-1}(x-b)^{\mu-1}\ldots(x-g)^{\tau-1}$$

Тогда делим $f(x)$ на P и получаем полином:

$$(x-a)(x-b)(x-c)\ldots(x-g),$$

не имеющий уже кратных корней.

Итак, освобождение уравнения от кратных корней совершается при помощи нахождения общего наибольшего делителя функции $f(x)$, первой части заданного уравнения и ее производной $f'(x)$, и совершается при помощи конечного числа самых простых рациональных операций.

О НЕПРИВОДИМОСТИ

§ 101. Говорят, что целая функция $f(x)$ обладает свойством неприводимости в области рациональных чисел, если она имеет рациональные коэфициенты и не разлагается на множители с рациональными коэфициентами.

Так, например, функция

$$f(x) = x^4 + 1,$$

будучи неприводимою в рациональных числах, делается приводимою, если мы к рациональным числам присоединим иррациональное число $\sqrt{2}$:

$$x^4 + 1 = (x^2 + x\sqrt{2} + 1)(x^2 - x\sqrt{2} + 1)$$

Если мы присоединим все иррациональные, а также мнимые числа, то неприводимых полиномов не существует, ибо тогда функция по теореме Гаусса раскладывается на линейные множители.

Приведем несколько основных положений относительно неприводимых функций. Будем ограничиваться функциями из поля R рациональных чисел.

Пусть задана неприводимая функция $f(x)$. Рассмотрим другую целую функцию $F(x)$ из того же числа R и будем искать общий наибольший делитель этих двух функций.

Пусть этот общий наибольший делитель будет $\varphi(x)$. Так как нахождение общего наибольшего делителя двух целых функций совершается посредством рациональных операций, то, если коэфициенты обеих функций принадлежат к полю R, то к тому же полю будут принадлежать и коэфициенты $\varphi(x)$; отсюда мы видим, что функция $\varphi(x)$ должна быть или постоянным числом, или же равняться $f(x)$, так как, по определению, неприводимая функция $f(x)$ не может иметь никакого делителя $\varphi(x)$ с рациональными коэфициентами меньшей степени.

Таким образом, мы видим, что функция $F(x)$ или взаимно простая с $f(x)$, или делится на $f(x)$. Отсюда получается теорема:

Теорема. Если функция $F(x)$ с рациональными коэфициентами обращается в нуль при каком-нибудь корне неприводимого уравнения $f(x)=0$, то она должна обращаться в нуль при всех корнях этого уравнения.

Следствие I. Если неприводимое уравнение $f(x)=0$ имеет общий корень с уравнением $\varphi(x)=0$ низшей степени, то все коэфициенты функции $\varphi(x)$ должны равняться нулю и, следовательно, уравнение $\varphi(x)=0$ должно обращаться в тождество. В самом деле, $\varphi(x)$ не может быть взаимно простою с $f(x)$ и не может делиться на $f(x)$, потому что степень ее ниже.

Следствие II. Все корни неприводимого уравнения простые, ибо иначе оно имело бы общие с производною корни, которая степени ниже и не равна тождественно нулю.

Мы в дальнейшем будем рассматривать неприводимость функции в различных полях Ω за исключением поля I всех комплексных чисел, в котором понятие о неприводимости теряется.

О ВЕЩЕСТВЕННЫХ КОРНЯХ УРАВНЕНИЙ

§ 102. Уравнения с вещественными коэфициентами, или, иначе говоря, уравнения в поле W играют главную роль в приложениях. Особенно интересуются их вещественными корнями, хотя надо признать, что в последнее время, особенно в электротехнике, играют роль также и мнимые корни.

При рассмотрении вещественных корней мы будем пользоваться помощью общего анализа.

Итак, пока особо не будет сказано обратное, мы будем рассматривать функции в поле W.

НЕПРЕРЫВНОСТЬ ЦЕЛОЙ ФУНКЦИИ $f(x)$

§ **103.** Дадим переменной независимой приращение h, абсолютную величину которого обозначим через δ.

Покажем, что величине δ можно дать настолько малое значение, чтобы было:

$$|f(x+h)-f(x)|<\varepsilon, \tag{1}$$

где ε произвольно мало взятое положительное число.

По формуле Тейлора:

$$f(x+h)-f(x)=h\left\{f'(x)+\frac{h}{1\cdot 2}f''(x)\pm\ldots\right\};$$

выражение, стоящее в фигурных скобках, есть некоторая целая функция от двух переменных h и x.

Если мы будем предполагать абсолютную величину h меньше единицы, то абсолютная величина этого выражения будет меньше некоторого положительного числа α, которое можно указать так: все знаки в многочлене заменить знаком $+$, h заменить единицей, а переменную x заменить ее абсолютной величиною; тогда

$$|f(x+h)-f(x)|<\delta\alpha$$

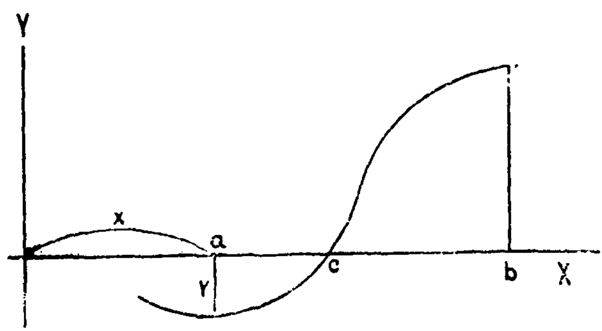

Рис. 15.

Стоит только удовлетворить неравенству $\delta\alpha<\varepsilon$ соответственным выбором δ, как получим требуемое неравенство (1).

§ **104.** Непрерывность функций в математическом смысле ставится в соответствие с понятием геометрической непрерывности кривых линий.

В самом деле, уравнение:

$$y=f(x)$$

можно рассматривать геометрически; причем различным значениям x можно сопоставлять значения y, которые будем откладывать параллельно оси y.

Из геометрических соображений требуется, чтобы при изменении x кривая, определяемая непрерывной функцией $f(x)$, шла непрерывно, причем $f(x)$ должна проходить через все промежуточные значения.

В анализе это свойство доказывается, т. е. что из непрерывности в смысле § 103 следует непрерывность в том смысле, что функция проходит через все промежуточные значения.

Отсюда следует, что, если при двух значениях $x=a$ и $x=b$ непрерывная функция имеет различные по знаку значения, то между a и b должно существовать по крайней мере одно значение $x=c$, при котором функция равна нулю.

ОБРАЩЕНИЕ ФУНКЦИИ В БЕСКОНЕЧНОСТЬ

§ 105. Так как очевидно, что для всякого конечного значения x целая функция имеет конечное значение, то она может обратиться в бесконечность только при

$$x=+\infty \quad \text{или} \quad x=-\infty$$

Докажем это.

$$f(x)=x^n\left\{p_0+\frac{p_1}{x}+\frac{p_2}{x^2}+\ldots\right\} \tag{1}$$

При больших значениях x по абсолютной величине выражение:

$$\frac{p_1}{x}+\frac{p_2}{x^2}+\ldots+\frac{p_n}{x^n}$$

как сумма конечного числа бесконечно малых величин сама будет бесконечно малая величина.

В выражении (1) в фигурных скобках мы имеем *число*, мало отличающееся от p_0, а тогда беспредельное возрастание x^n заставит функцию возрастать беспредельно.

Так как при достаточно большом значении $|x|$ выраженне в фигурных скобках имеет знак p_0, то знак $f(x)$ при больших значениях x будет совпадать со знаком главного члена

$$p_0x^n$$

Отсюда мы имеем сразу несколько важных замечаний.

Всякое уравнение нечетной степени имеет по крайней мере один вещественный корень.

Разделив уравнение (1) на p_0, мы получаем:

$$x^n + \frac{p_1}{p_0} x^{n-1} + \ldots = 0,$$

где n число нечетное.

При

$$x = -\infty, \quad x = +\infty$$

мы имеем знаки функции:

$$-, \; +,$$

значит, должен существовать по крайней мере один корень.

Всякое уравнение четной степени, у которого крайние коэфициенты имеют разные знаки, имеет по крайней мере два корня разных знаков.

Возьмем уравнение:

$$x^n + \ldots + x \frac{p_{n-1}}{p_0} + \frac{p_n}{p_0} = 0,$$

где n число четное, а $\frac{p_n}{p_0}$ число отрицательное.

Тогда, если мы рассмотрим два промежутка:

$$(x = -\infty, \; x = 0) \qquad (x = 0, \; x = +\infty),$$

мы получим знаки:

$$(+, -), \; (-, +)$$

и, значит, в обоих промежутках имеется по крайней мере по одному корню.

ПОПАРНАЯ СОПРЯЖЕННОСТЬ МНИМЫХ КОРНЕЙ

§ 106. Рассмотрим уравнение из поля W. Если оно имеет мнимый корень:

$$x = \alpha + \beta i,$$

то подставляя его в уравнение, получим в результате:

$$A + iB = 0,$$

где A и B выражаются через числа α, β и коэфициенты уравнения.

Если $\alpha+\beta i$ — корень уравнения, то должно быть:

$$A=0, \quad B=0,$$

а значит, будет и

$$A-iB=0$$

Другими словами, величина $\alpha-i\beta$ будет также корнем уравнения.

ТЕОРЕМА ШТУРМА

§ 107. Старые методы приближенного вычисления вещественных корней сводились к двум операциям: к так называемому отделению корня и собственно к его вычислению.

Под отделением корня разумелась задача нахождения двух чисел α и β, между которыми был бы только один корень.

Если мы возьмем два числа α и β произвольно, и если между ними окажется только один корень, то задача отделения решена. Также задача будет решена, если между α и β не будет ни одного корня.

Если же между α и β окажется несколько корней, то необходимо уменьшать промежуток до тех пор, пока не произойдет отделение корня.

Во-первых, возможность отделения корней следует из того соображения, что число вещественных корней конечно. Тогда, если мы составим всевозможные разности двух корней, то число таких разностей будет также конечное: $\frac{n(n-1)}{2}$. Из конечного числа чисел возьмем наименьшее по абсолютной величине.

Возьмем арифметическую прогрессию с разностью λ, меньше найденной нами наименьшей разности корней; тогда, очевидно, числа этой прогрессии будут отделять все корни уравнения.

Таким путем решили задачу отделения корней Варинг и Лагранж. Они составили уравнение, имеющее корни, равные квадратам разностей корней заданного уравнения:

$$(\alpha-\beta)^2, \quad (\alpha-\gamma)^2, \quad (\beta-\gamma)^2$$

Это уравнение было степени $\frac{n(n-1)}{2}$. Тогда они брали за λ наименьший предел положительных корней.

Последний коэфициент этого уравнения был, очевидно, дискриминантом заданного уравнения.

Коши обратил внимание, что составление всего уравнения в квадратах разностей не обязательно. К числу λ можно будет притти, рассматривая только дискриминант.

Все такие сложные рассуждения излишни, потому что задача отделения корнéй вовсе не так необходима для вычисления корней.

В 1803 году Бюданом была сообщена теорема, значительно упрощавшая задачу отделения корня. Но эта теорема оставляла еще много неопределенного, пока, наконец, Штурм не дал метод безупречный в теоретическом отношении, который давал возможность безошибочно указывать точно число корней между каждыми двумя числами

$$\alpha \text{ и } \beta$$

Эта теорема доставила Штурму громадную популярность, так что Штурм называл свою теорему: „теоремой, имя которой я имею честь носить".

§ 108. Штурм рассуждал так. Прежде всего он предлагает освободиться от кратных корней. Затем надо произвести действия последовательного деления, как бы для нахождения общего наибольшего делителя функции $f(x)$ и ее производной $f'(x)$. Положим, $f_1(x)=f'(x)$; будем брать последовательные остатки со знаком минус:

$$\begin{aligned} f &= f_1 q_1 - f_2 \\ f_1 &= f_2 q_2 - f_3 \\ &\cdots\cdots \\ f_{m-2} &= f_{m-1} q_{m-1} - f_m \end{aligned} \tag{1}$$

Ряд функций:

$$f,\ f_1, f_2, \ldots, f_m \tag{2}$$

есть так называемый ряд Штурма. Степени f_k по мере увеличения значка k убывают, и мы можем дойти, наконец, до нулевой степени, т. е. до постоянного числа не равного нулю, ибо функция и производная, по предположению, общих корней иметь не могут.

Мы можем остановиться раньше на такой функции f_m, которая не имеет корней в промежутке

$$\alpha \quad \text{и} \quad \beta$$

В первых двух функциях:

$$f(x) \quad \text{и} \quad f'(x)$$

при переходе через корень a первой функции от меньших значений к большим теряется перемена знака.

В самом деле,

$$\frac{f(a+h)}{f'(a+h)} = \frac{hf'(a)+\ldots}{f'(a)+\frac{h}{1}f''(a)+\ldots} = h\,\frac{1+\frac{h}{2}\,\frac{f''(a)}{f'(a)}+\ldots}{1+\frac{h}{1}\,\frac{f''(a)}{f'(a)}+\ldots} \tag{3}$$

При малых значениях h дробь близка к единице и знак выражения (3) зависит от знака h.

При $h<0$ функции $f(x)$, $f'(x)$ представляют перемену знака, а при $h>0$ — постоянство знака.

Итак, при возрастании x и при переходе через корень a первой функции в ряде Штурма теряется одна перемена знака.

Покажем, что при переходе через нуль одной из средних функций ряда Штурма не происходит потери перемены знака.

Две рядом стоящие функции f_k и f_{k+1} не могут обращаться одновременно в нуль, ибо тогда на основании равенств (1) должны были бы обращаться в нуль и все следующие функции, в том числе и последняя f_m, что противоречит предположению.

Если же $f_k = 0$, то мы имеем:

$$f_{k-1} = -f_{k+1},$$

т. е. в трех функциях:

$$f_{k-1},\ f_k,\ f_{k+1}$$

при переходе через корень f_k сохраняется одна перемена знака, и мы приходим к теореме Штурма.

Число вещественных корней в промежутке α и $\beta>\alpha$ равно точно числу потерь перемен знака, в ряде функций Штурма при переходе от α до β.

ТЕОРЕМА БЮДАНА—ФУРЬЕ

§ 109. Бюдан заменяет ряд функций Штурма рядом производных:

$$f(x),\ f'(x),\ f''(x),\ \ldots,\ f^{n}(x) \tag{1}$$

Вычисление этого ряда (1) проще, чем вычисление ряда функций Штурма, но зато мы приходим к заключениям менее определенным.

Теорема Бюдана. При переходе от вещественного числа α к большему числу β в ряде Бюдана для функции $f(x)$ теряется такое число перемен знака, которое или равно числу вещественных корней уравнения $f(x)=0$ в промежутке (α, β) или больше этого числа на число четное.

Доказательство состоит в том, что при переходе через корень γ одной из промежуточных функций $f(x)$ ряд Бюдана теряет всегда четное число потерь перемен знака.

Предположим теперь, что целое число μ не равно нулю, и рассмотрим часть ряда Бюдана, образованную функциями:

$$f^{(\mu-1)}(x),\quad f^{(\mu)}(x),\quad \ldots,\quad f^{(\mu+k)}(x),$$

причем

$$f^{(\mu-1)}(x)\gtrless 0,\quad f^{(\mu)}(x)=0,\quad \ldots,\quad f^{(\mu+k-1)}(x)=0,\quad f^{(\mu+k)}(x)\gtrless 0 \tag{2}$$

Покажем, что ряд (2) теряет всегда четное число перемен знака.

В предыдущем параграфе мы видели, что

$$\frac{f(x)}{f'(x)}$$

при возрастании x и переходе через простой корень $f(x)$ переходит от отрицательных значений к положительным.

То же самое происходит и в случае кратного корня:

$$\frac{f(\gamma+h)}{f'(\gamma+h)}=-\frac{h^{l}\dfrac{1}{l!}f^{(l)}(\gamma)+\cdots}{h^{l-1}\dfrac{1}{(l-1)!}f^{(l)}(\gamma)+\cdots}=h\left(\frac{1}{l}+hA\right)$$

В ряде функций (2) перед корнем γ функции $f^{(\mu)}(x)$ ряд представляет k перемен знака, а после корня будут все знаки постоянны. Рассмотрим первые две функции (2):

$$f^{(\mu-1)}(x), \quad f^{(\mu)}(x) = (x-\gamma)^k \varphi(x) \tag{3}$$

Если k четное число, то при переходе x через γ не произойдет ни потери, ни приобретения перемен знака в двух функциях (3), значит, число потерь перемен знака в ряде (2) будет четное.

Если k число нечетное, то при переходе x через γ выражение $(x-\gamma)^k$ меняет знак, и, следовательно, к нечетному числу потерь перемен знака в ряде (2) прибавляется или отпадает одна перемена знака в функциях (3), т. е. общее число потерь перемен знака будет четное, и теорема доказана.

ТЕОРЕМА ДЕКАРТА

§ 110. Как следствие теоремы Бюдана получается весьма важная в практическом отношении теорема, указанная много раньше Декартом.

Теорема. Число положительных корней функции $f(x)$ не превосходит числа перемен знака в ряде коэфициентов функции $f(x)$, и если они меньше, то на число четное.

Применяя формулу Маклорена (§ 100) мы можем написать

$$f(x) = f(0) + xf'(0) + \frac{x^2}{1 \cdot 2} f''(0) + \ldots + \frac{x^n}{n!} f^{(n)}(0)$$

Отсюда видно, что знаки коэфициентов функции $f(x)$ не отличаются от знаков ряда:

$$f(0), \quad f'(0), \quad f''(0), \quad \ldots, \quad f^{(n)}(0) \tag{1}$$

Итак, число перемен знака в коэфициентах функции $f(x)$ равно числу перемен знака в ряде Бюдана для данной функции при $x=0$. По теореме Бюдана число положительных корней функции $f(x)$ может отличаться на четное число от числа потерь перемен знака в ряде:

$$f(x), \quad f'(x), \quad f''(x), \quad \ldots, \quad f^{(n)}(x) \tag{2}$$

при переходе от $x=0$ до $x=+\infty$, но при $x=+\infty$ ряд (2) представляет только повторения знака, следовательно, число положительных корней функции $f(x)$ будет отличаться на четное число от числа перемен знака в ряде (1), и теорема Декарта доказана.

§ 111. Расположим члены в $f(x)$ по убывающим степеням и будем рассматривать разности между степенями каждых двух последовательных членов.

Пусть μ будет число таких случаев, где разность степеней нечетная:

$$2k_1+1,\quad 2k_2+1,\quad \ldots,\quad 2k_\mu+1$$

Кроме того, пусть будет ν пар членов различных знаков разность степеней которых будет четная:

$$2h_1+2,\quad 2h_2+2,\quad \ldots,\quad 2h_\nu+2$$

и, наконец, пусть будет ρ пар чисел одинакового знака с четною разностью степеней:

$$2g_1,\quad 2g_2,\quad \ldots,\quad 2g_\rho$$

Рассмотрим, какое число членов будет в заданном уравнении.

Так как число пар первой категории будет μ, второй ν, третьей ρ, то общее число членов будет, очевидно, на единицу более общего числа пар, т. е. будет:

$$\mu+\nu+\rho+1$$

Посмотрим какое число членов не будет входить в уравнение. Если разность степеней рядом стоящих членов будет m, то это будет соответствовать пропуску $m-1$ члена.

Итак, число пропущенных членов будет:

$$2k_1+2k_2+\ldots+2k_\mu+(2h_1+1)+(2h_2+1)+\ldots+(2h_\nu+1)+$$
$$+(2g_1-1)+(2g_2-1)+\ldots+(2g_\rho-1)=2s+\nu-\rho,$$

где

$$s=k_1+k_2+\ldots+k_\mu+h_1+h_2+\ldots+h_\nu+g_1+\ldots+g_\rho$$

Итак, складывая число $\mu+\nu+\rho+1$ членов, входящих в уравнение с числом $2s+\nu-\rho$ пропущенных членов, мы должны получить общее число $n+1$ членов функции n-ой степени:

$$2s+\mu+2\nu+1=n+1,$$

откуда

$$n=2s+\mu+2\nu \tag{1}$$

Будем рассматривать число перемен знака в функции $f(x)$ и обозначим его через V, а через V'—число перемен знака в полиноме $f(-x)$, тогда нетрудно показать, чему равно $V+V'$.

В самом деле, пары членов одного знака с четными разностями степеней не дают перемен знака ни в составе V, ни в составе V'. Каждая пара с нечетною разностью степеней, если она давала повторение знака при x, будет давать перемену знака при $-x$, и обратно. Следовательно, такая пара будет давать единицу в сумме $V+V'$. Число перемен знака, введенных такими парами, очевидно, будет μ и, наконец, пары членов разных знаков с четною разностью степеней будет давать перемену знака как при x, так и при $-x$ и, следовательно, каждая такая пара введет в сумму $V+V'$ две единицы.

Таким образом, окончательно:

$$V+V'=\mu+2\nu$$

или из (1) мы получим:

$$n=2s+V+V' \tag{2}$$

Обозначим через P число положительных корней уравнения, а через P' — число отрицательных корней, тогда общее число корней будет:

$$n=P+P'+2y, \tag{3}$$

где $2y$ число мнимых корней.

Сравнивая (2) и (3), мы получим:

$$2y=(V-P)+(V'-P')+2s, \tag{4}$$

но обе разности $V-P$ і $V'-P'$ не отрицательные, и мы получаем:

$$y \geqslant s \tag{5}$$

Отсюда видим, что если по крайней мере одно из чисел k_1 $k_2, \ldots, h_1, h_2, \ldots, g_1, g_2, \ldots$ отлично от нуля, то число s положительное, и уравнение наверно имеет мнимые корни. И мы приходим к заключению:

Если в уравнении имеется пропуск одного члена между членами одного знака или же пропуск числа членов более одного, то уравнение имеет наверное мнимые корни.

Например, следующие уравнения имеют мнимые корни:

$$x^7+3x^5-4x^4+x^3-2x^2-x-1=0$$

$$x^7+x^3+x+1=0$$

$$x^5-4x^4-5x^2+1=0$$

$$x^5-4x^4-5x^2+1=0$$

$$x^5-x^2+1=0$$

Знаменитый французский математик Эрмит в бытность его учеником в лицее Louis le Grand в 1842 году указал на такую теорему: „Если четыре последовательных коэфициента уравнения $f(x)=0$ представляют арифметическую прогрессию, то это уравнение наверное имеет мнимые корни.

Для доказательства достаточно заметить, что произведение $f(x)(x^2-2x+1)$ будет иметь пропуск двух членов.

ТЕОРЕМА РОЛЛЯ

§ 112. Между двумя последовательными корнями функции лежит по крайней мере один корень ее производной.

Рассмотрим два последовательных корня a и b функции $f(x)$, причем $b>a$. Предположим h достаточно малым положительным числом. Мы уже видели, что

$$\frac{f(a+h)}{f'(a+h)}>0, \quad \frac{f(b-h)}{f'(b-h)}<0 \tag{1}$$

Так как a и b суть два последовательных корня заданной функции, то между числами $a+h$ i $b-h$ не существует корней функции $f(x)$ и, следовательно, два результата:

$$f(a+h) \quad \text{и} \quad f'(b-h)$$

должны иметь один и тот же знак. Но тогда, на основании неравенств (1), выражения:

$$f'(a+h) \quad \text{и} \quad f'(b-h)$$

должны быть разных знаков и, следовательно, производная $f(x)$ должна иметь нечетное число корней в промежутке между числами:

$$a+h \quad \text{и} \quad b-h,$$

что и требовалось доказать.

О ФУНКЦИЯХ С ПЕРЕМЕЖАЮЩИМИСЯ КОРНЯМИ

§ 113. Рассмотрим функцию $f(x)$ из W, все корни которой $\alpha_1, \alpha_2, \ldots, \alpha_n$ — вещественные и различные, и пусть кроме того имеет место неравенство:

$$\alpha_1 < \alpha_2 < \alpha_3 < \ldots < \alpha_n \tag{1}$$

Так как число промежутков между корнями (1) есть $n-1$ и, кроме того, у производной, как у функции степени $n-1$, число корней есть также $n-1$, то, как следствие теоремы Ролля, получится, что все корни:

$$\beta_1, \beta_2, \beta_3, \ldots, \beta_n \tag{2}$$

производной должны быть вещественны и должны заключаться по одному в промежутках между корнями (1). Другими словами, между корнями (1) и (2) должны существовать неравенства:

$$\alpha_1 < \beta_1 < \alpha_2 < \beta_2 < \alpha_3 \ldots < \beta_{n-1} < \alpha_n \tag{3}$$

Неравенства (3) показывают, что, и обратно, в этом случае между каждыми двумя последовательными корнями производной находится корень заданной функции.

Говорят, что корни функции $f(x)$, если они все вещественные, *перемежаются* с корнями производной.

Обобщая это понятие, мы назовем две функции $f(x)$ и $\varphi(x)$ функциями с перемежающимися корнями, если все корни этих функций вещественны и между каждыми двумя последовательными корнями одной функции лежит корень другой.

Очевидно, что функции с перемежающимися корнями должны быть или одинаковых степеней, или степени их могут отличаться на единицу.

Теорема. Если корни функций $f(x)$ и $\varphi(x)$ перемежаются, то уравнение:

$$f(x)\varphi'(x) - f'(x)\varphi(x) = 0 \tag{4}$$

не имеет вещественных корней.

Предположим, что степень функции $f(x)$ не превосходит степени $\varphi(x)$, тогда по формуле Лагранжа:

$$\frac{f(x)}{\varphi(x)} = C + \sum_i \frac{f(\alpha_i)}{\varphi'(\alpha_i)} \frac{1}{x-\alpha_i},$$

где C постоянная, если степени функций $f(x)$ и $\varphi(x)$ одинаковы, и нуль, если степень $f(x)$ ниже степени $\varphi(x)$; величины α_i суть корни функции $\varphi(x)$.

Взяв от обеих частей производную, получим:

$$\frac{\varphi(x)f'(x)-f(x)\varphi'(x)}{[\varphi(x)]^2}=-\sum_i \frac{f(\alpha_i)}{\varphi'(\alpha_i)}\frac{1}{(x-\alpha_i)^2}$$

Умножая на $[\varphi(x)]^2$, получим (см. § 89):

$$\varphi(x)f'(x)-f(x)\varphi'(x)=-\sum_i \frac{f(\alpha_i)}{\varphi'(\alpha_i)}[\varphi_i(x)]^2 \tag{5}$$

Нетрудно видеть, что сумма во второй части (5) сохраняет свой знак при всех значениях x.

В самом деле, рассмотрим два последовательных корня:

$$\alpha_i \quad \text{и} \quad \alpha_{i+1}$$

функции $\varphi(x)$. Так как корни производной $\varphi'(x)$ перемежаются с корнями функции $\varphi(x)$, то

$$\varphi'(\alpha_i) \quad \text{и} \quad \varphi'(\alpha_{i+1})$$

— разных знаков. Подобным же образом будут разных знаков $f(\alpha_i)$ и $f(\alpha_{i+1})$, потому что по условию перемежаются корни $f(x)$ с корнями $\varphi(x)$, следовательно, дроби:

$$\frac{f(\alpha_i)}{\varphi'(\alpha_i)} \quad \text{и} \quad \frac{f(\alpha_{i+1})}{\varphi'(\alpha_{i+1})}$$

— одного знака функция.

$$\varphi(x)f'(x)-f(x)\varphi'(x)$$

не меняет своего знака при всевозможных значениях x.

Это выражение не может обратиться в нуль ни при каком значении β числа x. В самом деле, такое обращение могло бы иметь место, если бы β обращало в нуль сразу все функции

$$\varphi_1(x), \quad \varphi_2(x), \quad \ldots, \quad \varphi_n(x),$$

что невозможно.

ТЕОРЕМА ВЛАДИМИРА МАРКОВА

§ 114. Из теоремы предыдущего параграфа вытекает такая теорема:

Если корни двух целых функций $f(x)$ и $\varphi(x)$ перемежаются, то перемежаются также корни их производных $f'(x)$ и $\varphi'(x)$.

В самом деле, рассмотрим функцию:

$$\varphi(x)f'(x)-f(x)\varphi'(x) \tag{1}$$

Пусть α_1 и α_2 два последовательных корня производной $\varphi'(x)$. По теореме предыдущего параграфа результаты подстановки чисел α_1 и α_2 в выражение (1) — одного знака.

Эти результаты будут:

$$\varphi(\alpha_1)f'(\alpha_1) \quad \text{и} \quad \varphi(\alpha_2)f'(\alpha_2)$$

Но числа $\varphi(\alpha_1)$ и $\varphi(\alpha_2)$ — разных знаков, следовательно, должны быть разных знаков и числа $f'(\alpha_1)$ и $f'(\alpha_2)$, и теорема доказана.

Эту теорему напечатал Владимир Марков в своем студенческом сочинении: „О функциях, наименее уклоняющихся от нуля в данном промежутке“ (СПБ 1892)

Указанное сочинение В. А. Маркова замечательно по целому ряду результатов важного значения.

REGULA FALSI

§ 115. Если корень отделен, то два числа α и β таковы, что $f(\alpha)$ и $f(\beta)$ — разных знаков.

Для ясности будем трактовать задачу геометрически и будем рассматривать соответствующее уравнение

$$y=f(x) \tag{1}$$

в прямоугольных координатах; тогда абсциссы α и β будут по разные стороны корня L и им будут соответствовать ординаты разных знаков. Корень, лежащий в промежутке (α, β), будет абсциссой точки L, в которой кривая (1) пересекает ось x-ов.

Если границы промежутка достаточно близки, то, проведя хорду MN, соединяющую точки кривой с абсциссами α и β, можно принять за приближенное значение корня абсциссу точки K встречи с осью x-ов хорды MN.

Другими словами, мы принимаем за приближенное значение корня абсциссу точки, делящей отрезок (α, β) пропорционально величинам $f(\alpha)$, $f(\beta)$.

Такой способ имеет важное практическое значение, например, в артиллерии, когда из недолета и перелета вычисляется настоящий прицел.

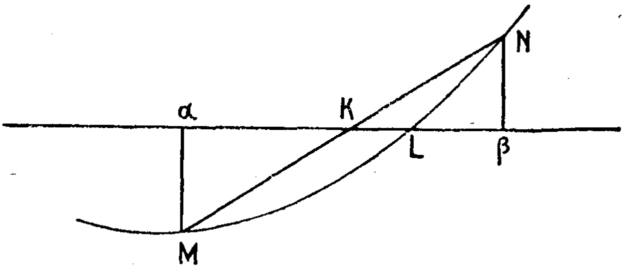

Рис. 16.

Найдем формулу для вычисления абсциссы точки K.

Уравнение хорды MN будет:

$$\frac{y - f(\alpha)}{f(\beta) - f(\alpha)} = \frac{x - \alpha}{\beta - \alpha};$$

абсцисса точки встречи ее с осью x-ов получится, полагая $y = 0$, т.-е. из уравнения:

$$\frac{-f(\alpha)}{f(\beta) - f(\alpha)} = \frac{x - \alpha}{\beta - \alpha},$$

или, окончательно,

$$x = \frac{\alpha f(\beta) - \beta f(\alpha)}{f(\beta) - f(\alpha)} \tag{2}$$

Эту формулу и вообще этот прием рассуждения дали в средние века арабы, которые имели в виду, между прочим, задачи элементарной арифметики, где уравнения — все первой степени, а потому они выражаются прямыми и, следовательно, хорда совпадает с кривою. Итак, правило regula falsi в арифметике дает не приближенное решение, а т о ч н о е.

Арабы назвали свое правило „хисаб-уль-хатайн", т. е. арифметика двух ошибок *).

---

*) Мориц Кантор перед изданием своей многотомной истории математики, написал довольно большую книгу об истории математики у арабов. Кантор заинтересовался словом „хатайн" и обратился за консультацией к профессорам

СПОСОБ ПОДКАСАТЕЛЬНЫХ НЬЮТОНА

§ 116. Ньютоном был предложен способ, носящий название способа подкасательных. Этот классический прием годится одинаково как для алгебраических уравнений, так и для трансцендентных.

Если задано уравнение $f(x)=0$, то будем рассматривать соответствующую ему линию:

$$y=f(x) \tag{1}$$

Решение уравнения состоит в нахождении точки встречи кривой (1) с осью x-ов, имеющей уравнение $y=0$.

Пусть найдено некоторое приближенное значение α корня уравнения. Если число α—не корень, но очень близко к нему, то соответствующее значение $y_\alpha=f(\alpha)$ будет близко к нулю.

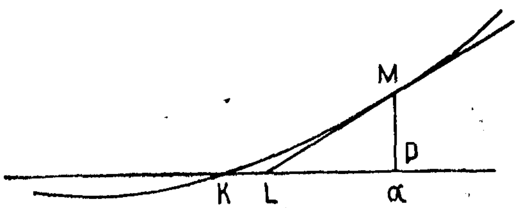

Рис. 17.

Точка с координатами α, $f(\alpha)$ будет близка к оси x-ов. Применяя общий принцип диференциального исчисления, состоящий в замене кривой линии вблизи некоторой точки касательною к этой кривой, мы приходим к мысли искать точку встречи с осью x-ов касательной, проведенной в точке касания α, $f(\alpha)$. Эта точка встречи дает число более близкое к корню, чем α. В этом состоит идея способа Ньютона.

Пишем уравнение касательной ML:

$$y-f(\alpha)=f'(\alpha)(x-\alpha)$$

филологам, но не арабистам. Эти профессора сказали, что тут дело идет о народе хаты, жившем тогда-то и в такой-то местности; а так как „хата=хита=кита", то возможно, что дело идет о китайцах.

Я должен разъяснить это недоразумение: „хата" — по арабски обозначает „ошибка"; „хатани" — двойственное число — „две ошибки"; „хатайн" — родительный падеж.

Значит, „хисаб-уль-хатайн" в переводе будет: „арифметика двух ошибок".

Для нахождения точки встречи с осью x-ов полагаем $y=0$. Тогда, решая относительно x, получим:

$$x=\alpha-\frac{f(\alpha)}{f'(\alpha)}, \tag{2}$$

где $\frac{f(\alpha)}{f'(\alpha)}$ есть подкасательная PL (см. § 86).

Итак, способ Ньютона состоит в следующем: берется приближенное значение α корня, далее вычисляется новое приближение α_1 по формуле:

$$\alpha_1=\alpha-\frac{f(\alpha)}{f'(\alpha)}$$

по этому значению α_1 составляется новое приближение α_2 по такой же формуле:

$$\alpha_2=\alpha_1-\frac{f(\alpha_1)}{f'(\alpha_1)}$$

Продолжая далее вычисление последовательных чисел $\alpha_1, \alpha_2, \alpha_3, \ldots$ по указанным формулам, мы должны приближаться к основному корню заданного уравнения.

Весьма важное обстоятельство состоит в том, что способ Ньютона был первым примером одного довольно широкого метода современной математики — метода так называемой итерации (повторения операций).

Метод итерации состоит в следующем. Берется некоторое число (безразлично вещественное или комплексное) и некоторая функция $\varphi(x)$ и составляется ряд чисел:

$$\alpha_1=\varphi(\alpha), \quad \alpha_2=\varphi(\alpha_1), \quad \alpha_3=\varphi(\alpha_3), \ldots$$

Задача состоит в изучении вопроса, когда ряд чисел:

$$\alpha, \quad \alpha_1, \quad \alpha_2, \ldots$$

имеет предел.

Приведение в порядок метода Ньютона требует решения двух основных вопросов: 1) действительно ли последовательное приближение имеет своим пределом корни уравнения и 2) если предел существует, то необходимо оценить погрешность, которую мы делаем, останавливаясь на каком-нибудь приближении.

Ответ на эти два вопроса был дан Фурье.

АЛГОРИТМ ВЫЧИСЛЕНИЯ КОРНЕЙ

§ 117. В этой главе мы сообщим простое доказательство теоремы Гаусса, что всякий полином имеет по крайней мере один корень. Мы, конечно, должны будем вернуться к общему полю I.

Мы сообщим доказательство теоремы.

Если модуль численного значения $f(a)$ заданной функции, соответствующего численному значению a переменного независимого, больше нуля, то этот модуль можно уменьшить прибавкой к числу a некоторого числа h.

Рассмотрим самый общий случай, когда при значении a сама функция $f(z)$ не обращается в нуль согласно формулировке теоремы, а ряд производных:

$$f'(z), \quad f''(z), \ldots, \quad f^{(m-1)}(z)$$

обращается в нуль при $z=a$, причем $f^{(m)}(a) \neq 0$; тогда по формуле Тейлора имеем:

$$f(a+h)=f(a)+\frac{h^m}{\Pi(m)}f^{(m)}(a)\,[1+Q], \tag{1}$$

где $\Pi(m)=1\cdot 2\cdot 3\ldots m$, а

$$Q=\frac{h}{m+1}\frac{f^{(m+1)}(a)}{f^{(m)}(a)}+\frac{h^2}{(m+1)(m+2)}\frac{f^{(m+2)}(a)}{f^{(m)}(a)}+\ldots$$

Подберем h удовлетворяющим равенству:

$$\frac{h^m}{\Pi(m)}f^{(m)}(a)=-\delta f(a), \tag{2}$$

где δ—некоторая правильная положительная дробь, величину которой можно взять сколь угодно малой. Равенство (1) можно переписать так:

$$f(a+h)=f(a)-\delta f(a)+\frac{h^m}{\Pi(m)}f^{(m)}(a)\,Q=$$

$$=f(a)\,(1-\delta)+\frac{h^m}{\Pi(m)}f^{(m)}(a)\,Q$$

Но модуль суммы не больше суммы модулей слагаемых*):

$$|f(a+h)| \leqslant (1-\delta)|f(a)|+\left|\frac{h^m}{\Pi(m)}f^{(m)}(a)\right|\cdot|Q|; \tag{3}$$

*) Сторона треугольника не больше суммы двух других сторон.

Для нахождения точки встречи с осью x-ов полагаем $y = 0$. Тогда, решая относительно x, получим:

$$x = \alpha - \frac{f(\alpha)}{f'(\alpha)}, \tag{2}$$

где $\frac{f(\alpha)}{f'(\alpha)}$ есть подкасательная PL (см. § 86).

Итак, способ Ньютона состоит в следующем: берется приближенное значение α корня, далее вычисляется новое приближение α_1 по формуле:

$$\alpha_1 = \alpha - \frac{f(\alpha)}{f'(\alpha)}$$

по этому значению α_1 составляется новое приближение α_2 по такой же формуле:

$$\alpha_2 = \alpha_1 - \frac{f(\alpha_1)}{f'(\alpha_1)}$$

Продолжая далее вычисление последовательных чисел α_1, $\alpha_2, \alpha_3, \ldots$ по указанным формулам, мы должны приближаться к основному корню заданного уравнения.

Весьма важное обстоятельство состоит в том, что способ Ньютона был первым примером одного довольно широкого метода современной математики — метода так называемой и т е р а ц и и (повторения операций).

Метод итерации состоит в следующем. Берется некоторое число (безразлично вещественное или комплексное) и некоторая функция $\varphi(x)$ и составляется ряд чисел:

$$\alpha_1 = \varphi(\alpha), \quad \alpha_2 = \varphi(\alpha_1), \quad \alpha_3 = \varphi(\alpha_3), \ldots$$

Задача состоит в изучении вопроса, когда ряд чисел:

$$\alpha, \quad \alpha_1, \quad \alpha_2, \ldots$$

имеет предел.

Приведение в порядок метода Ньютона требует решения двух основных вопросов: 1) действительно ли последовательное приближение имеет своим пределом корни уравнения и 2) если предел существует, то необходимо оценить погрешность, которую мы делаем, останавливаясь на каком-нибудь приближении.

Ответ на эти два вопроса был дан Фурье.

АЛГОРИТМ ВЫЧИСЛЕНИЯ КОРНЕЙ

§ 117. В этой главе мы сообщим простое доказательство теоремы Гаусса, что всякий полином имеет по крайней мере один корень. Мы, конечно, должны будем вернуться к общему полю I.

Мы сообщим доказательство теоремы.

Если модуль численного значения $f(a)$ заданной функции, соответствующего численному значению a переменного независимого, больше нуля, то этот модуль можно уменьшить прибавкой к числу a некоторого числа h.

Рассмотрим самый общий случай, когда при значении a сама функция $f(z)$ не обращается в нуль согласно формулировке теоремы, а ряд производных:

$$f'(z),\quad f''(z), \ldots,\quad f^{(m-1)}(z)$$

обращается в нуль при $z=a$, причем $f^{(m)}(a) \neq 0$; тогда по формуле Тейлора имеем:

$$f(a+h)=f(a)+\frac{h^m}{\Pi(m)} f^{(m)}(a)\,[1+Q], \tag{1}$$

где $\Pi(m)=1\cdot 2\cdot 3\ldots m$, а

$$Q=\frac{h}{m+1}\frac{f^{(m+1)}(a)}{f^{(m)}(a)}+\frac{h^2}{(m+1)(m+2)}\frac{f^{(m+2)}(a)}{f^{(m)}(a)}+\ldots$$

Подберем h удовлетворяющим равенству:

$$\frac{h^m}{\Pi(m)} f^{(m)}(a)=-\delta f(a), \tag{2}$$

где δ—некоторая правильная положительная дробь, величину которой можно взять сколь угодно малой. Равенство (1) можно переписать так:

$$f(a+h)=f(a)-\delta f(a)+\frac{h^m}{\Pi(m)} f^{(m)}(a)\,Q=$$

$$=f(a)\,(1-\delta)+\frac{h^m}{\Pi(m)} f^{(m)}(a)\,Q$$

Но модуль суммы не больше суммы модулей слагаемых*):

$$|f(a+h)| \leqslant (1-\delta)|f(a)|+\left|\frac{h^m}{\Pi(m)} f^{(m)}(a)\right|\cdot|Q|; \tag{3}$$

*) Сторона треугольника не больше суммы двух других сторон.

так как при достаточно малом h величину Q можно сделать сколь угодно малой, то можно будет удовлетворить неравенству

$$|Q| < 1,$$

а тогда на основании равенства (2) будет:

$$\left|\frac{h^m}{\Pi(m)} f^{(m)}(a)\right| = \delta\,|f(a)|,$$

или

$$\left|\frac{h^m}{\Pi(m)} f^{(m)}(a)\right| \cdot |Q| < \delta\,|f(a)|;$$

неравенство (3) обращается в такое:

$$|f(a+h)| < (1-\delta)\,|f(a)| + \delta\,|f(a)|,$$

т. е.

$$|f(a+h)| < |f(a)|,$$

что и требовалось доказать.

§ 118. Очень немного надо добавить к теореме предыдущего параграфа, чтобы получить хорошее простое и ясное доказательство существования корня у целой функции.

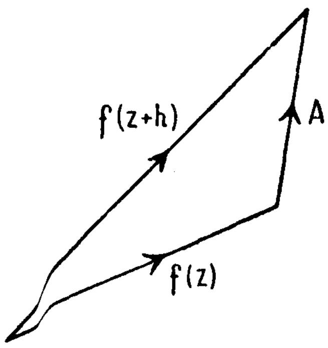

Рис. 18.

Пока теорема § 117 дает только, что нижняя граница модуля $|f(z)|$ не может быть больше нуля, так как тогда ее можно уменьшить.

Необходимо воспользоваться тем, что функция $|f(z)|$ непрерывная и как таковая она должна достигать своей нижней границы. Эта граница должна быть наименьшим значением функции, ее так называемым minimum'ом. Это наименьшее значение функция будет иметь при некотором определенном значении z_0, так что z_0 будет корнем уравнения.

Докажем, следовательно, что модуль целой функции непрерывно изменяется при изменении z.

По теореме Тейлора имеем:

$$f(z+h) - f(z) = A,$$

где модуль A при достаточно малом модуле h может быть сколь угодно мал:

$$f(z+h)=f(z)+A$$

Так как модуль комплексного числа есть расстояние между точкой комплексного числа и началом координат, то мы можем воспользоваться свойством сторон треугольника, а именно, что сторона треугольника больше разности двух других сторон и меньше их суммы:

$$|f(z)|-|A|\leqslant|f(z+h)|\leqslant|f(z)|+|A|,$$

или

$$-|A|\leqslant|f(z+h)|-|f(z)|\leqslant+|A|,$$

но $|A|$ величина бесконечно малая, следовательно, $|f(z)|$ есть функция непрерывная.

§ 119. Так как при бесконечно большом модуле z модуль функции $f(x)$ также бесконечно велик, то наименьшие значе-

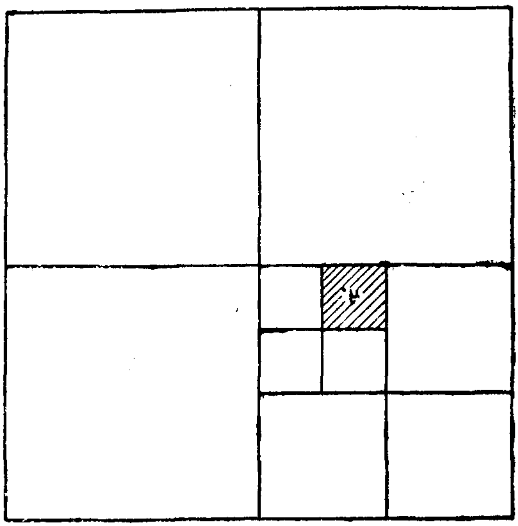

Рис. 19.

ния, равные нулю, могут быть только на конечном расстоянии от начала координат.

Мы возьмем около начала координат настолько больших размеров квадрат, чтобы вне его наверно не было значения нуль модуля $|f(z)|$. Разделим квадрат делением сторон пополам на четыре меньших квадрата.

так как при достаточно малом h величину Q можно сделать сколь угодно малой, то можно будет удовлетворить неравенству

$$|Q| < 1,$$

а тогда на основании равенства (2) будет:

$$\left|\frac{h^m}{\Pi(m)} f^{(m)}(a)\right| = \delta\,|f(a)|,$$

или

$$\left|\frac{h^m}{\Pi(m)} f^{(m)}(a)\right| \cdot |Q| < \delta\,|f(a)|;$$

неравенство (3) обращается в такое:

$$|f(a+h)| < (1-\delta)\,|f(a)| + \delta\,|f(a)|,$$

т. е.

$$|f(a+h)| < |f(a)|,$$

что и требовалось доказать.

§ 118. Очень немного надо добавить к теореме предыдущего параграфа, чтобы получить хорошее простое и ясное доказательство существования корня у целой функции.

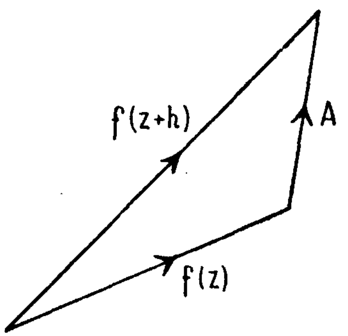

Рис. 18.

Пока теорема § 117 дает только, что нижняя граница модуля $|f(z)|$ не может быть больше нуля, так как тогда ее можно уменьшить.

Необходимо воспользоваться тем, что функция $|f(z)|$ непрерывная и как таковая она должна достигать своей нижней границы. Эта граница должна быть наименьшим значением функции, ее так называемым minimum'ом. Это наименьшее значение функция будет иметь при некотором определенном значении z_0, так что z_0 будет корнем уравнения.

Покажем, следовательно, что модуль целой функции непрерывно изменяется при изменении z.

По теореме Тейлора имеем:

$$f(z+h) - f(z) = A,$$

где модуль A при достаточно малом модуле h может быть сколь угодно мал:

$$f(z+h)=f(z)+A$$

Так как модуль комплексного числа есть расстояние между точкой комплексного числа и началом координат, то мы можем воспользоваться свойством сторон треугольника, а именно, что сторона треугольника больше разности двух других сторон и меньше их суммы:

$$|f(z)|-|A|\leqslant|f(z+h)|\leqslant|f(z)|+|A|,$$

или

$$-|A|\leqslant|f(z+h)|-|f(z)|\leqslant+|A|,$$

но $|A|$ величина бесконечно малая, следовательно, $|f(z)|$ есть функция непрерывная.

§ 119. Так как при бесконечно большом модуле z модуль функции $f(x)$ также бесконечно велик, то наименьшие значе-

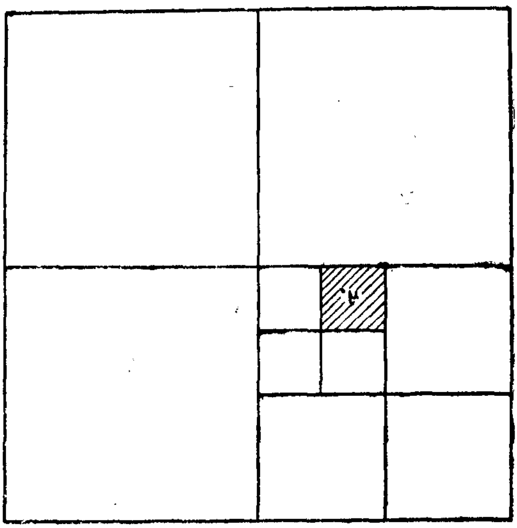

Рис. 19.

ния, равные нулю, могут быть только на конечном расстоянии от начала координат.

Мы возьмем около начала координат настолько больших размеров квадрат, чтобы вне его наверно не было значения нуль модуля $|f(z)|$. Разделим квадрат делением сторон пополам на четыре меньших квадрата.

Если низшая граница 0 была во всем квадрате, то она должна быть также в одном из четырех меньших, ибо если бы ее не было ни в одном из них, то ее не могло быть и во всем квадрате. Пусть эта нижняя граница 0 находится в правом нижнем квадрате. Делим его стороны пополам, получаем четыре меньших квадрата, в одном из которых нижняя граница должна быть нулем. Продолжая далее уменьшение квадратов до бесконечности, мы приходим к некоторой предельной точке μ, в которую суживаются постепенно квадраты. Эта точка μ лежит внутри каждого из ряда выбранных нами квадратов. Легко проверить, на основании непрерывности функции $|f(z)|$, что $|f(\mu)| = 0$. Таким образом, мы находим то значение z, которое дает наименьшее значение функции.

§ 120. Данное нами доказательство существования корня алгебраического уравнения в смысле компактности не оставляет желать ничего лучшего, но имеет еще один недостаток, что оно не дает средств, как можно вычислить корень при помощи сходящегося способа вычисления.

Мы приведем следующие соображения, которые направлены к тому, чтобы исправить этот недостаток, хотя бы теоретически. Эти соображения дают второе доказательство основной теоремы о существовании корня. Они указаны в общих чертах Лифшицем *). Соображения Лифшица подверглись упрощениям со стороны Дедекинда, Фробениуса и Г. Вебера **).

Прием приближения к корню основан на применении формулы, подобной способу подкасательных Ньютона, переведенной на комплексные числа, а именно формулы:

$$h = -\delta \frac{f(\alpha)}{f'(\alpha)},$$

где δ достаточно малое положительное число.

Мы имеем:

$$f(\alpha + h) = (1-\delta) f(\alpha) + \frac{\delta^2}{2} f(\alpha) \left[\frac{f(\alpha) f''(\alpha)}{f'(\alpha)^2} - \frac{\delta}{3} \frac{f(\alpha)^2 f'''(\alpha)}{f'(\alpha)^3} + \cdots \right]$$

Можно предположить, что мы предварительно освободили функцию $f(\alpha)$ от кратных корней, и тогда $f'(\alpha)$ — не нуль. Можно

*) Lehrbuch der Algebra, Bd. I, § 61.

**) См. Weber, Lehrbuch der Algebra, Bd. I, § 42.

найти положительное число Q, достаточно большое для того, чтобы было:

$$Q>1, \quad Q>\left|\frac{f(\alpha)f''(\alpha)}{f'(\alpha)^2}+\cdots\right. \tag{1}$$

Обозначим:

$$\alpha+h=\alpha_1, \quad |f(\alpha)|=a, \quad |f(\alpha_1)|=a_1$$

Мы имеем:

$$a_1<a\left(1-\delta+\frac{\delta^2}{2}Q\right)$$

Положим, так как ничто не мешает это нам сделать,

$$\delta=Q^{-1},$$

тогда будем иметь:

$$\alpha_1=\alpha-\frac{1}{Q}\frac{f(\alpha)}{f'(\alpha)} \tag{2}$$

$$a_1<a\left(1-\frac{1}{2Q}\right) \quad \text{и} \quad a-a_1>\frac{a}{2Q} \tag{3}$$

Вебер так ограничил рассуждение, что он иолучил одно и то же значение Q, которое удовлетворяет (1) для всех точек той области, на которой он рассматривает задачу.

Полагая:

$$\alpha_2=\alpha_1-\frac{1}{Q}\frac{f(\alpha_1)}{f'(\alpha_1)}, \qquad \alpha_3=\alpha_2-\frac{1}{Q}\frac{f(\alpha_2)}{f'(\alpha_2)}$$

и

$$a_2=|f(\alpha_2)|, \quad a_3=|f(\alpha_3)|, \cdots,$$

а также

$$\theta=1-\frac{1}{2Q},$$

получим:

$$a_1<a\,\theta, \quad a_2<a_1\theta, \quad \cdots, \quad a_\nu<a_{\nu-1}\theta,$$

откуда

$$a_\nu=a\,\theta^\nu,$$

и для $\nu=\infty$ мы получим:

$$\lim a_\nu=0$$

С другой стороны, на основании (3),

$$|\alpha-\alpha_1|<\frac{a}{Qk}<\frac{2(a-a_1)}{k}, \quad 0<k<|f'(\alpha)|;$$

мы получаем:

$$|\alpha - \alpha_{\nu-1}| < \frac{2(a_\nu - a_{\nu-1})}{k}$$

Отсюда, если примем в основание неравенство:

$$|\alpha_\mu - \alpha_\nu| < |\alpha_\mu - \alpha_{\mu+1}| + |\alpha_{\mu+1} - \alpha_{\mu+2}| + \cdots,$$

получим:

$$|\alpha_\mu - \alpha_\nu| < \frac{2(a_\mu - a_\nu)}{k}$$

При $\mu = \infty$ і $\nu = \infty$ получается:

$$|\alpha_\mu - \alpha_\nu| = 0$$

Таким образом, мы удостоверяемся, что числа ряда:

$$\alpha,\ \alpha_1,\ \alpha_2, \ldots,\ \alpha_n, \ldots$$

приближаются к некоторому пределу ξ, который будет корнем функции, ибо вследствие непрерывности функции:

$$f(\xi) = \lim f(\alpha_i) = \lim a_i = 0$$

§ 121. Я сделал некоторое добавление к этому алгоритму в статье „Algorithme du calcul des racines des équations algébriques", 1936.

Алгоритм состоит в том, что можно начать с произвольного числа α, которое я называю р е п е р о м корня, и последовательным рядом действий с помощью

$$\alpha,\ \alpha_1,\ \alpha_2, \ldots,\ \alpha_n, \ldots$$

приближаться к корню.

Я считаю недостатком метода, что мы не знаем к какому корню уравнения мы приближаемся.

Я поставил себе задачей н а й т и п о л н у ю с и с т е м у р е п е р о в в числе, равном числу корней уравнения, и такую, чтобы из каждого из этих реперов мы приближались бы к каждому без пропуска корню заданного уравнения. Я показал, как установить правила для нахождения подобной системы реперов.

Между прочим, я показал в моей статье и геометрическое значение формулы:

$$\alpha_1 = \alpha - \delta \frac{f(\alpha)}{f'(\alpha)}$$

Пусть будет

$$f(x+iy)=u+iv,$$

де u и v две вещественные функции от двух вещественных переменных x, y.

Будем x и y рассматривать как координаты на горизонтальной плоскости комплексного переменного

$$x+iy=\xi,$$

букву же z сохраним для обозначения третьей координаты пространства x, y, z; при этом мы будем предполагать, что система будет прямоугольная, т. е. координата z находится на оси, перпендикулярной к плоскости x, y. Все три координаты x, y, z, очевидно, вещественные.

Тогда модуль функции даст вещественную поверхность:

$$z=+\sqrt{u^2+v^2} \tag{1}$$

Возьмем на этой поверхности точку

$$a,\ b,\ c, \tag{2}$$

где

$$\alpha=a+bi, \quad c=|f(\alpha)|$$

Уравнение касательной плоскости в точке (2) будет:

$$z-c=\frac{uu'_x+vv'_x}{\sqrt{u^2+v^2}}(x-a)+\frac{(uu'_y+vv'_y)}{\sqrt{u^2+v^2}}(y-b)$$

Здесь u'_x, v'_x, u'_y, v'_y суть так называемые частные производные, взятые по одной из букв x или y.

Уравнения нормали будут:

$$\frac{z-c}{-\sqrt{u^2+v^2}}=\frac{x-a}{uu'_x+vv'_x}=\frac{y-b}{uu'_y+vv'_y}$$

Проведем через эту нормаль вертикальную плоскость:

$$\frac{x-a}{uu'_x+vv'_x}=\frac{y-b}{uu'_y+vv'_y}$$

Это же самое уравнение будет уравнением подкасательной на горизонтальной плоскости, касательной к линии наибольшего ската (ligne de la plus grande pente).

Мы имеем:

$$x - a = (uu'_x + vv'_x)\mu$$

$$y - b = (uu'_y + vv'_y)\mu$$

Умножая второе уравнение на i и складывая, получим *):

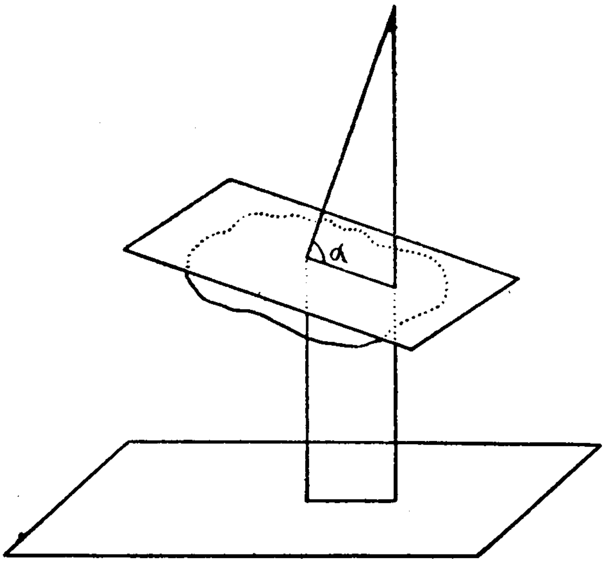

Рис. 20.

$$\xi - \alpha = \mu\,[uu'_x + vv'_x + i\,(uu'_y + vv'_y)] = \mu\,(u + iv)(u'_x - iv'_x) =$$

$$= \mu\,(u'^2_x + v'^2_x)\,\frac{u + iv}{u'_x + iv'_x} = (u'^2_x + v'^2_x)\,\frac{f(\alpha)}{f'(\alpha)}$$

Обозначая вещественное число $\mu\,(u'^2_x + v'^2_x)$ через $-\delta$, получим:

$$\xi = \alpha - \delta\,\frac{f(\alpha)}{f'(\alpha)}$$

Итак, эта формула показывает, что при малом δ перемещение совершается по линии наибольшего ската по поверхности модуля.

---

*) Мы имеем:

$$u'_x = v'_y, \quad u'_y = -v'_x$$

ТРЕХЧЛЕННЫЕ УРАВНЕНИЯ

§ 122. Трехчленными называются уравнения вида:

$$x^{p+q}+2ax^q+\beta=0,$$

которые заключают три члена. Такие уравнения часто встречаются. Кроме случаев квадратного и кубического уравнения мы обращаем внимание на то, что по способу Жерарда уравнение пятой степени приводится к трехчленному:

$$x^5+ax+b=0$$

Я говорю здесь о трехчленных уравнениях, потому что Гаусс*) обратил на эти уравнения свое внимание и дал прекрасный способ их решения. В 1896 году Гундельфинген опубликовал таблицы, облегчающие выкладки этого решения.

Я покажу здесь мое видоизменение способа Гаусса, относящееся к вычислению вещественных корней трехчленного уравнения.

Этот способ в мою бытность студентом Петербургского университета в 1883 году я показывал товарищам. Я ничего не публиковал о нем, ибо подробное теоретическое проведение не привело меня к новым в идейном отношении результатам.

Здесь я приведу мой способ, ибо при практическом вычислении он не хуже способа Гаусса, но имеет преимущество в мнемоническом отношении и его буквально нельзя забыть, если он был один раз известен.

Возвысим уравнение

$$x^q(x^p+2a)=-\beta$$

в степень p:

$$x^{qp}(x^p+2a)^p=(-1)^p.\beta^p$$

и положим:

$$x^p+a=z$$

Тогда уравнение примет вид: (1)

$$(z+a)^p(z-a)^q=b, \tag{2}$$

где

$$b=(-1)^p\beta^p$$

На основании (1) всякому вещественному корню заданного трехчленного уравнения будет соответствовать вещественный же корень преобразованного уравнения (2).

---

*) Gauss, Werke, Bd. III, S. 85.

§ 123. Применим теорему Штурма к уравнению (2) § 122:

$$V = (z+a)^p (z-a)^q - b$$

Его производная будет:

$$V' = (z+a)^{p-1}(z-a)^{q-1}[(p+q)z-(p-q)a]$$

Деля V на V' и изменяя знак остатка, получим:

$$V_2 = (z+a)^{p-1}(z-a)^{q-1} + \frac{b}{a^2}\frac{(p+q)^2}{4pq}$$

Число a положительное, а p и q натуральные числа.

Далее деля V' на V_2 и продолжая процесс последовательного деления, получим остальные две функции Штурма:

$$V_3 = b[(p+q)z-(p-q)a]$$

$$V_4 = (-1)^q \frac{p^p q^q}{(p+q)^{p+q}} - \frac{b}{(2a)^{p+q}}$$

По поводу этих последних двух функций надо заметить, что остаток от деления полинома $\psi(z)$ на $z-A$ будет $\psi(A)$.

Так как общее число функций Штурма есть пять, то уравнение не может иметь более четырех вещественных корней.

§ 124. Уравнение (2) § 122 удобно для вычисления корня при помощи периодического алгоритма.

Уравнение (2) § 122 можно преобразовать так:

$$z = a + \frac{\sqrt[q]{b}}{{}^{\frac{p}{q}}(a+z)} \tag{1}$$

Для удобства я пишу показатель $\frac{p}{q}$ над $(a+z)$ не справа, как обычно, а слева.

Подставляя в скобках знаменателя вместо z все выражение (1), приходим к бесконечному периодическому алгоритму:

$$z = a + \cfrac{\sqrt[q]{b}}{{}^{\frac{p}{q}}\left(2a + \cfrac{\sqrt[q]{b}}{{}^{\frac{p}{q}}(2a + \ldots}\right)} \tag{2}$$

Подобным же образом, преобразуя уравнение (2) § 122 так:

$$z = -a + \frac{\sqrt[p]{b}}{(-a+z)^{\frac{q}{p}}},$$

получаем другой алгоритм:

$$z = -a + \frac{\sqrt[p]{b}}{\left(-2a + \frac{\sqrt[p]{b}}{(-2a + \ldots)^{\frac{q}{p}}}\right)^{\frac{q}{p}}} \tag{3}$$

Этот алгоритм представляет обобщение непрерывных дробей в том смысле, что при непрерывных дробях чередуются две операции: деление и сложение. Здесь же чередуются три операции: возвышение в степень с показателем $\frac{q}{p}$, деление и сложение.

При q четном в алгоритме (4) можно брать радикал с тем или другим знаком; подобным же образом при p четном можно изменять знак при радикале $\sqrt[p]{b}$.

Оказывается, что при помощи четырех полученных таким образом алгоритмов можно вычислять все вещественные корни уравнения (2) § 122.

Покажем приложение этого метода к численному уравнению.

§ 125. Вычислим вещественные корни уравнения:

$$x^5 - 4x - 2 = 0 \tag{1}$$

Полагая

$$x^4 - 2 = z,$$

получим новое уравнение в виде:

$$(z+2)(z-2)^4 = 16$$

По соображениям § 111 уравнение (1) должно иметь два мнимых корня. Мы получим для вычисления трех вещественных корней алгоритмы:

$$\frac{z_1+2}{4} = 1 + \frac{\frac{1}{2\sqrt{2}}}{\sqrt[4]{1 + \frac{\frac{1}{2\sqrt{2}}}{\sqrt[4]{1+\ldots}}}} \tag{2}$$

$$\frac{z_2+2}{4}=1-\frac{\frac{1}{2\sqrt{2}}}{\sqrt[4]{1-\frac{\frac{1}{2\sqrt{2}}}{\sqrt[4]{1-\ldots}}}} \qquad (3)$$

$$\frac{-z_3+2}{4}=1-\frac{2^{-6}}{{}^4\left(1-\frac{2^{-6}}{{}^4(1-\ldots)}\right)} \qquad (4)$$

Мы поясним как получается формула (4).

Мы начинаем с формулы:

$$z_3=-2+\frac{16}{{}^4(-2+z_3)}$$

$$z_3=-2+\frac{16}{{}^4\left(-4+\frac{16}{{}^4(-4+\ldots)}\right)}$$

Можно под знаком возвышения в четвертую степень менять знак:

$$-z_3=2-\frac{16\cdot 4^{-4}}{{}^4\left(1-\frac{4\cdot 4^{-4}}{{}^4(1-\ldots)}\right)}$$

$$\frac{-z_3+2}{4}=1-\frac{4^{-3}}{{}^4\left(1-\frac{4^{-3}}{{}^4(1-\ldots)}\right)}$$

Покажем как окончательно вычислить корень z_3. Для этого воспользуемся указанными в § 27 Гауссовыми логарифмами сумм и разностей*).

Прежде всего:

$$\lg 2^{-6}=(10-0{,}3010300)\cdot 6=(9{,}6989700)\cdot 6=8{,}1938200$$

$$\lg 1-\lg 2^{-6}=0-8{,}1938200=1{,}8061800$$

Находим на странице 700 таблицы Zech-a соответствующий последнему числу аргумент:

$$G=0{,}0068405,$$

*) I. Zech, Tafeln der Additions- und Subtractions-Logarithmen, Berlin 1863.

тогда

$$\lg(1-2^{-6}) = 0 - G = 9{,}9931595,$$

умножим на 4:

$$\lg{}^4(1-2^{-6}) = 9{,}9931595 \cdot 4 = 9{,}9726380$$

Мы приступаем ко второй итерации:

$$\lg\frac{2^{-6}}{^4(1-2^{-6})} = \frac{\begin{array}{r}8{,}1938200\\ -\,9{,}9726380\end{array}}{8{,}2211820} = \lg k_1$$

$$\lg 1 - \lg k_1 = 1{,}7788180$$

По таблицам Zech-a находим:

$$G_2 = 0{,}0072880;$$

тогда

$$\lg(1-k_1) = 0 - G_2 = 9{,}9927120,$$

$$\lg{}^4(1-k_1) = 9{,}9708480$$

	Третья итерация	Четвертая итерация
	8,1938200	8,1838200
	9,9708480	9,9707212
	8,2229720	8,2230988
	1,7770280	1,7769012
	G_3 0,0073197	G_4 0,0073215
	9,9926803	9,9926785
Умножая на 4	9,9707212	

Итак, пятая итерация дает окончательно:

$$\lg\frac{-z_3+2}{4} = \lg\frac{4-x_3^4}{4} = 9{,}9926786 \qquad (5)$$

Мы получаем четвертую степень корня x_3. Для получения самого корня придется извлечь корень четвертой степени, тогда является вопрос, с каким знаком взять величину x_3. Этот вопрос просто решается из таких соображений.

Из уравнения (5) мы имеем:

$$4 - x_3^4 > 0, \quad x_3^4 - 4 < 0,$$

но по уравнению (1)

$$(x_3^4 - 4)\, x_3 = 2\,,$$

откуда

$$x_3 < 0$$

ИДЕИ ДАННИЛА БЕРНУЛЛИ. СПОСОБ ГРЕФФЕ

§ 126. Даниил Бернулли в свою бытность в Петербурге указал на такую мысль *).

Пусть $x_1, x_2, \ldots, x_n$ суть корни уравнения $f(x) = 0$.

Полагая, по обыкновению, $s_k = x_1^k + x_2^k + \ldots + x_n^k$, будем иметь:

$$\frac{s_k}{s_{k-1}} = x_1 \frac{1 + \left(\frac{x_2}{x_1}\right)^k + \ldots + \left(\frac{x_n}{x_1}\right)^k}{1 + \left(\frac{x_2}{x_1}\right)^{k-1} + \ldots + \left(\frac{x_n}{x_1}\right)^{k-1}}$$

Если x_1 имеет наибольший модуль, то при беспредельном возрастании k мы будем иметь:

$$\lim \frac{s_k}{s_{k-1}} = x_1$$

Таким образом, наибольший по модулю корень может быть найден как предел $\frac{s_k}{s_{k-1}}$.

Пусть уравнение:

$$f(x) = x^n + p_1 x^{n-1} + p_2 x^{n-2} + \ldots$$

имеет только вещественные и положительные корни и притом неравные:

$$\alpha_1 > \alpha_2 > \alpha_3 > \ldots > \alpha_{n-1} > \alpha_n$$

Составим уравнение, корнями которого будут:

$$-\alpha_1^{2k},\ -\alpha_2^{2k},\ \ldots,\ \alpha_n^{2k}$$

Пусть это уравнение будет:

$$F(x) = x^n + A_1 x^{n-1} + A_2 x^{n-2} + \ldots + A_n = 0$$

---

*) Comm. Petrop., 3, 1728, p. 92.

Будем иметь:

$$A_1 = \alpha_1^{2k} + \alpha_2^{2k} + \ldots + \alpha_n^{2k}$$

$$A_2 = (\alpha_1 \alpha_2)^{2k} + (\alpha_1 \alpha_3)^{2k} + \ldots$$

$$A_3 = (\alpha_1 \alpha_2 \alpha_3)^{2k} + (\alpha_1 \alpha_2 \alpha_4)^{2k} + \ldots$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$A_n = (\alpha_1 \alpha_2 \alpha_3 \ldots \alpha_n)^{2k}$$

По идее Бернулли, если показатель $2k$ беспредельно возрастает, то в каждой сумме (1) первый член будет настолько велик по сравнению с прочими, что с принятою для вычисления степенью точности можно всеми этими членами пренебречь.

Тогда система (1) заменится такою:

$$A_1 = \alpha_1^{2k}$$

$$A_2 = (\alpha_1\alpha_2)^{2k}$$

$$A_3 = (\alpha_1\alpha_2\alpha_3)^{2k}$$

$$\ldots\ldots\ldots$$

$$A_n = (\alpha_1\alpha_2 \ldots \alpha_n)^{2k},$$

откуда непосредственно находим все корни:

$$\alpha_1^{2k} = A_1, \quad \alpha_2^{2k} = \frac{A_2}{A_1}, \quad \alpha_3^{2k} = \frac{A_3}{A_2}, \ldots$$

§ 127. Эйлер в своем знаменитом сочинении „Introductio in analysin infinitorum (т. I, 17) стремился придать идеям Бернулли практическое значение и развил способ вычисления уравнений при помощи возвратных рядов.

§ 128. Наконец, в 1837 году цюрихский профессор Греффе дал практически удобный способ, основанный на идеях Бернулли. Этот способ состоит в том, чтобы составлять уравнения, корни которых суть взятые со знаком минус квадраты, 4-й степени, 8-й степени и так далее корней заданного уравнения.

Поясним дело на квадратном уравнении

$$Ax^2 + Bx + c = 0 \tag{1}$$

Полагая $x = \sqrt{y}$, получим:

$$Ay + c = -B\sqrt{y};$$

возвышая в квадрат, получим:

$$A^2y^2+(2Ac-B^2)y+c^2=0 \qquad (2)$$

уравнение, корни которого суть квадраты корней уравнения (1). Повторяя тот же прием замены y на $\sqrt{y}$, получим уравнение с четвертыми степенями корней, и так далее.

Приемы вычисления мнимых корней по идеям Бернулли разрабатывали Enke*) и А. Н. Крылов, академик АН СССР.

Кому придется вычислять корни уравнений, я советую обратиться к книге акад. А. Н. Крылова: „Лекции о приближенных вычислениях" (1911).

МЕТОД ЛАГРАНЖА

§ 129. На теории непрерывных дробей основан способ Лагранжа для приближенного вычисления вещественных корней численных уравнений. Этот способ не очень удобен для практики, но он ведет к важным теоретическим выводам, которые будут разъяснены во втором томе Трактата.

Пусть $f(x)=0$ вещественное уравнение, которое имеет по крайней мере один вещественный корень.

По приемам отделения корней мы можем найти всегда целое число a_0 такое, что между a_0 и a_0+1 заключаются один или несколько корней $f(x)$. Преобразуем $f(x)$ при помощи подстановки:

$$x=a_0+\frac{1}{x_1},$$

где $x_1>1$; тогда получится новое уравнение $f_1(x_1)$, имеющее один или несколько корней, которые больше 1. Мы найдем целое положительное число a_1, такое, что между a_1 и a_1+1 будут лежать один или несколько корней $f_1(x_1)$.

Подстановкой:

$$x_1=a_1+\frac{1}{x_2}$$

мы придем к новому уравнению $f_2(x)$.

Продолжая далее тот же прием, получим:

$$x_2=a_2+\frac{1}{x_3},$$

*) Enke, Journ. f. reine u. ang. Math., 22, 1841.

и так далее. Мы приходим к непрерывной дроби:

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ldots}} = (a_0, a_1, a_2, a_3, \ldots)$$

Мы получаем ряд рациональных чисел:

$$(a_0), \quad (a_0, a_1), \quad (a_0, a_1, a_2), \quad (a_0, a_1, a_2, a_3), \ldots,$$

которые попеременно то больше, то меньше некоторого корня x и беспредельно к нему приближаются.

Когда мы дойдем до подходящей дроби:

$$(a_0, a_1, a_2 \ldots, a_{\nu-1}) = \frac{P_\nu}{Q_\nu},$$

то эта дробь отличается от истинного значения корня x меньше чем на

$$\frac{1}{Q_\nu^2}$$

ТЕОРЕМА ЛИУВИЛЯ

§ 130. Мы называем **алгебраическим числом** корень всякого уравнения:

$$f(x) = p_0 x^r + p_1 x^{r-1} + \ldots + p_r = 0, \tag{1}$$

все коэфициенты которого **целые** числа.

Будем раскладывать в непрерывную дробь иррациональный положительный корень x уравнения (1) $f(x) = 0$:

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ldots}}$$

Рассмотрим промежуток $(\mathfrak{a}, \mathfrak{b})$, в котором находится корень

$$x \, (\mathfrak{a} > 0, \mathfrak{b} > 0)$$

Пусть $\frac{P_n}{Q_n}$ некоторая подходящая дробь, настолько близкая к корню x, что она также находится внутри промежутка:

$$\frac{f\left(\frac{P_n}{Q_n}\right)-f(x)}{\frac{P_n}{Q_n}-x}=\psi(x),$$

где ψ — функция $r-1$ степени от x:

$$\psi(x)=p_0\left\{\left(\frac{P_n}{Q_n}\right)^{r-1}+\left(\frac{P_n}{Q_n}\right)^{r-2}x+\ldots\right\}+$$

$$+p_1\left\{\left(\frac{P_n}{Q_n}\right)^{r-2}+\left(\frac{P_n}{Q_n}\right)^{r-3}x+\ldots\right\}+$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

Мы можем подобрать положительное число M так, чтобы было:

$$|\psi(x)|<M$$

Принимая во внимание:

$$\frac{P_n}{Q_n}<\mathfrak{b},\quad x<\mathfrak{b},$$

можем взять за M такое число:

$$M=|p_0|\,r\,\mathfrak{b}^{r-1}+|p_1|(r-1)\,\mathfrak{b}^{r-2}+\ldots$$

Тогда:

$$\left|f\left(\frac{P_n}{Q_n}\right)\right|<\left|\frac{P_n}{Q_n}-x\right|M$$

и, наконец,

$$\left|\frac{P_n}{Q_n}-x\right|>\frac{\left|f\left(\frac{P_n}{Q_n}\right)\right|}{M} \tag{2}$$

Из теории непрерывных дробей известно *):

$$\frac{P_n}{Q_n} - x = \frac{(-1)^n}{Q_n(Q_n x_n + Q_{n-1})}, \quad x_n = a_n + \frac{1}{a_{n+1} + \ldots}$$

Принимая во во внимание, что $x_n > a_n$, получим:

$$\left| \frac{P_n}{Q_n} - x \right| < \frac{1}{a_n Q_n^2} \tag{3}$$

Сопоставляя (2) и (3), получим:

$$a_n < \frac{M}{Q_n \left| f\left(\frac{P_n}{Q_n}\right) \right|} \tag{4}$$

Далее, подставляя $\frac{P_n}{Q_n}$ в первую часть уравнения (1), получим:

$$f\left(\frac{P_n}{Q_n}\right) = \frac{p_0 P_n^r + p_1 P_n^{r-1} Q + \ldots}{Q_n^r}$$

Значит,

$$\left| f\left(\frac{P_n}{Q_n}\right) \right| > \frac{1}{Q_n^r},$$

и мы приходим из (4) к неравенству Лиувиля:

$$a_n < M Q_n^{r-2} \tag{5}$$

Стоит только написать такую непрерывную дробь, у которой неравенство (5) не удовлетворяется, чтобы быть уверенным, что такая дробь не может быть алгебраическим числом. Эта дробь будет числом новой природы, которое называется **трансцендентным**.

К числу трансцендентных чисел принадлежат числа e и π; о них подробно скажем в втором томе.

ПРИНЦИПЫ ТЕОРИИ ГАЛУА

§ 131. Мы приступим теперь к изложению теории**), одной из самых глубоких и плодотворных в математике.

---

*) Д. Граве, Элементарный курс теории чисел, 1913, стр. 187; Д. Граве, Начала алгебры, 1915, стр. 262.

*) Творец ее Эварист Галуа был убит на дуэли в возрасте 21 года.

Займемся задачей, формулировка которой имеет несколько необычный характер.

Если задано конечное число целых функций:

$$\chi_1(x, y, z, \ldots), \quad \chi_2(x, y, z, \ldots), \quad \chi_3(x, y, z, \ldots), \ldots$$

от переменных $x, y, z, \ldots$ с числовыми коэфициентами, причем ни в одной из функций все коэфициенты не равны нулю, то можно бесчисленным числом способов выбрать такие значения $x, y, z, \ldots$, чтобы ни одна из функций не обращалась в нуль.

Обычно главная трудность состоит в решении уравнений, особенно диференциальных и интегральных, а не решить уравнение казалось бы задача не такая трудная.

В случае одной независимой переменной теорема почти очевидна, ибо тогда существует конечное число значений, которые обращают в нуль функции $\chi_1, \chi_2, \chi_3, \ldots$

Далее мы можем видеть справедливость теоремы для $n+1$ переменных, если мы будем предполагать, что она доказана для n переменных.

Расположим все функции по степеням $n+1$-ой переменной t, тогда по предположению можно дать остальным n переменным такие значения, чтобы ни один коэфициент при t ни в одной функции, будучи целой функцией от остальных переменных, не равнялся нулю. Тогда мы имеем функции от одной переменной t и можем дать ей такое значение, что ни одна функция не обращается в нуль.

ФУНКЦИЯ ГАЛУА

§ 132. Мы рассматриваем алгебраическое уравнение степени n:

$$f(x) = 0, \tag{1}$$

которое может быть как буквенным, так и численным.

В случае численных уравнений для нас будет безразлично, будет ли оно приводимым или неприводимым. Для нас важно, чтобы корни:

$$x_1, \ x_2, \ x_3, \ldots, x_n$$

были все неравные. Значит мы избавились по приемам § 100 от кратных корней.

Будем называть функцией Галуа такую рациональную функцию от корней, все значения которой, получающиеся при всех

$$N = 1 \cdot 2 \ldots n = n!$$

подстановках симметрической группы, различны между собой.

На основании соображений § 131, мы можем составить сколько угодно таких функций.

Возьмем функцию:

$$\omega(x_1, x_2, \ldots, x_n, a, b, c)$$

Пусть, когда мы делаем подстановки симметрической группы, мы получаем значения функции:

$$\omega_1, \omega_2, \omega_3, \ldots, \omega_N$$

Чтобы функция ω была функцией Галуа, необходимо подобрать значения параметров $a, b, c, \ldots$ так, чтобы ни одна из разностей

$$\omega_k - \omega_l$$

$$(k, l = 1, 2, 3, \ldots, N)$$

не обращалась в нуль.

Галуа, например, указал простейшую функцию такого вида:

$$y_1 = \alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n, \tag{2}$$

где надо подобрать коэфициенты $\alpha_1, \alpha_2, \ldots, \alpha_n$.

Функция Галуа принадлежит к единичной группе и является, таким образом, как бы антиподом к симметрической функции.

§ 133. Можно выразить всякую рациональную функцию от корней рационально через функцию Галуа, применяя теорему Лагранжа (§ 95).

Всякая рациональная функция $r(x_1, x_2, \ldots, x_n)$, к какой бы группе она ни принадлежала, не меняется при единичной подстановке, т. е. при группе функции Галуа, а потому ее можно сопоставить с функцией Галуа y:

$$\sum \frac{r(x_1 x_2 \ldots x_n)}{z - y} = \frac{\Omega(z)}{f(z)}$$

и получить:

$$r = \frac{\Omega(y_1)}{F'(y_1)}$$

Всякий корень x_i есть функция, принадлежащая к группе порядка $(n-1)!$, не меняющей буквы x_i. Во всяком случае x_i не меняется от единичной подстановки, а потому все корни заданного уравнения выражаются рационально через y_1.

РЕЗОЛЬВЕНТА ГАЛУА

§ 134. Если мы выразим все корни уравнения (1) через функцию Галуа y_1, то мы можем выразить рационально через y_1 также и все N различных значений, которые функция Галуа принимает при подстановках симметрической группы.

Функция y_1 удовлетворяет уравнению:

$$F(y)=0 \tag{1}$$

степени N, обладающему свойством, что через один его корень y_1 выражаются все корни $x_1, x_2, \ldots, x_n$ заданного уравнения, а также через этот корень y_1 выражаются рационально все его другие корни $y_2, y_3, \ldots y_N$.

Разложим первую часть уравнения $F(y)=0$ на неприводимые множители. Пусть один из этих множителей будет:

$$g(y)=0 \tag{2}$$

Уравнение это пусть будет степени $m<N$. Пусть его корни будут:

$$y_1, y_2, \ldots, y_m$$

Уравнение $g(y)=0$ называется резольвентой Галуа, ибо оно помогает при решении заданного уравнения.

ГРУППА ГАЛУА

§ 135. Группа, относящаяся к основному уравнению $f(x)=0$, найдется по резольвенте Галуа.

Составим для всех корней x_i заданного уравнения их рациональные выражения через корень y_1 резольвенты:

$$x_1=H_1(y_1), \quad x_2=H_2(y_1), \quad \ldots, \quad x_n=H_n(y_1) \tag{1}$$

Если мы вместо y_1 подставим в эти равенства y_k, то

$$H_1(y_k), \; H_2(y_k), \; \ldots, \; H_n(y_k)$$

будут давать те же корни:

$$x_1, x, \ldots, x_n,$$

только расположенные в другом порядке, так что переход от y_1 до y_k будет давать подстановку корней заданного уравнения. Давая в ряде (1) вместо y_1 значения:

$$y_2, y_3, \ldots\ldots, y_m,$$

получим m подстановок корней x:

$$s_1 = 1, \ s_2, \ s_3, \ \ldots, \ s_m \tag{2}$$

Покажем, что эти подстановки образуют группу.

Пусть

$$y_k = \theta(y_1),$$

где θ—знак рациональной функции.

Подстановка s_k будет:

$$H_1(\theta y_1), \ H_2(\theta y_1), \ \ldots, \ H_n(\theta y_1);$$

здесь написано θy_1 вместо $\theta(y_1)$.

Под подстановкой s_k произведем другую s_q:

$$s_q s_k$$

Эта подстановка будет выражаться:

$$H_1(\theta y_q), \ H_2(\theta y_q), \ \ldots, \ H_n(\theta y_q) \tag{3}$$

Покажем, что это расположение корней дает подстановку из ряда (2).

Так, как $\theta(y_1) = y_k$ есть корень неприводимого уравнения $g(y) = 0$, то необходимо чтобы уравнение, корни которого суть:

$$\theta(y_1), \ \theta(y_2), \ \ldots., \ \theta(y_m), \tag{4}$$

которое имеет рациональные коэфициенты, совпадало с $g(y) = 0$; но тогда все корни (4) должны быть корнями резольвенты, т. е.

$$\theta(y_k) = y_r,$$

и, значит,

$$s_q s_k = s_r,$$

так что система (2) есть группа.

Это есть так называемая группа Галуа нашего уравнения, которую мы будем обозначать G.

НЕИЗМЕНЯЕМОСТЬ РАЦИОНАЛЬНЫХ ФУНКЦИЙ ОТ КОРНЕЙ

§ 136. Мы подчеркивали для буквенных уравнений, когда корни суть переменные независимые, очевидную теорему, что подстановки, не меняющие вида функции, образуют группу. Одна подстановка не меняет вида функции и другая — тоже; очевидно, что и совокупность их не будет менять функции.

Совсем другое происходит при численных уравнениях, когда надо говорить о неизменности рациональных функций по численной величине. Тогда наша теорема отпадает. Две подстановки не меняют численной величины функции, а их совокупность может менять численную величину функции.

Что это так, можно убедиться на простом примере.

Возьмем, например, уравнение:

$$x^6+x^5+x^4+x^3+x^2+x+1=0,$$

корни которого суть

$$x_k=e^{\frac{2k\pi i}{7}}$$

Очевидно, что $x_1 x_6=1$. Произведение не меняется по своей численной величине, т. е. остается равным единице при двух подстановках:

$$S=(12)(56),\quad T=(16)(23),$$

ибо подстановка S переводит нашу функцию в

$$x_2 x_5=1,$$

а от T она переходит в $x_6\ x_1=1$, но подстановка $ST=(13265)$ переводит x_1x_6 в x_3x_5, а эта величина не равна единице.

Теорема восстанавливается, если мы будем выбирать подстановки не произвольно, а только лишь из группы Галуа.

Мы приходим к самой общей теореме.

Подстановки из группы Галуа, не меняющие численно функции, образуют группу.

Эта теорема годится и для буквенных уравнений, так как группа Галуа для них сводится ко всей симметрической группе.

Для того чтобы убедиться в справедливости этой теоремы, мы должны рассмотреть главнейшие свойства группы Галуа.

§ 137. Мы должны понятие о рациональности уточнить. Будем рассматривать некоторое поле Ω, например, поле R или W, и тогда будем считать рациональными все элементы этого поля.

Мы скажем, что эти элементы—данные числа и, если мы выразим корни заданного уравнения через эти элементы, то уравнение может считаться решенным.

Всякая рациональная функция V с коэфициентами из Ω от корней, численное значение которой не изменяется от подстановок группы G Галуа, выражается рационально через заданные величины.

Функцию V можно выразить рационально через один из корней $g(y)=0$, например, через y_1 так что

$$V=\varphi(y_1),$$

где φ функция рациональная в поле Ω.

Так как подстановки G не меняют по предположению значения V и их действие состоит в замене y_1 на $y_2, y_3, \ldots, y_m$, то мы имеем:

$$V=\varphi(y_1)=\varphi(y_2)=\ldots=\varphi(y_m)$$

и, следовательно,

$$V=\frac{1}{m}[\varphi(y_1)+\varphi(y_2)+\ldots+\varphi(y_m)];$$

функция V выражается через величины известные как симметрическая функция от корней резольвенты $g(y)$.

§ 138. Можно показать свойство обратное.

Рациональная функция от корней, которая может выражаться через элемент поля Ω, остается численно неизменной при применении подстановок группы G.

Пусть M данная величина функции. Выразим все корни, которые входят в M, при помощи y_1; получим:

$$\varphi(y_1)=M,$$

где φ—рациональная функция в Ω. Итак, y_1 есть корень уравнения:

$$\varphi(y)-M=0$$

Это уравнение имеет один корень y_1 резольвенты, которая есть уравнение неприводимое, следовательно, оно должно иметь все ее остальные корни, и мы получаем:

$$\varphi(y_2)=M, \quad \varphi(y_3)=M, \quad \ldots, \quad \varphi(y_m)=M,$$

если только M не меняется при подстановках G.

Теорема остается справедливой, если M также иррациональная величина, только необходимо, чтобы присоединение иррациональностей, заключенных в M, не мешало оставаться резольвенте $g(y)$ неприводимою.

§ 139. Если две рациональные функции от корней φ и ψ равны, то они не перестают быть равными после применения подстановок Галуа.

В самом деле, их разность будет функция рациональная, она равна нулю. Это случай предыдущего параграфа, когда $M = 0$.

Теперь мы можем доказать, что подстановки, не меняющие численно рациональной функции от корней, образуют группу.

Пусть функция $\varphi(x_1, x_2, \ldots, x_n)$, которую мы обозначим для краткости $\varphi(x)$, не меняет своего численного значения от двух подстановок S и T, взятых из группы Галуа. Обозначим то выражение, в которое переходит функция $\varphi(x)$ при подстановке S, знаком $\varphi(x|S)$.

Мы получаем два равенства:

$$\varphi(x|S) = \varphi(x), \quad \varphi(x|T) = \varphi(x) \tag{1}$$

Применяя к первому равенству подстановку T, а ко второму — подстановку S, мы получим:

$$\varphi(x|ST) = \varphi(x|T), \quad \varphi(x|TS) = \varphi(x|S); \tag{2}$$

сравнивая (1) и (2), получим:

$$\varphi(x|ST) = \varphi(x|TS) = \varphi(x),$$

и теорема доказана.

§ 140. Полагая в § 138 $M = 0$, мы замечаем, что подстановки Галуа не нарушают каждого рационального соотношения:

$$\varphi(x_1, x_2, \ldots, x_n) = 0$$

между корнями, поэтому группу Галуа можно определить как группу таких подстановок, которые не нарушают всех соотношений между корнями. Ясное дело, что группа Галуа не должна зависеть от той функции y_1, которую мы выбрали для составления резольвенты $g(y)$.

Теперь мы должны обсудить, так сказать, универсальность теории Галуа.

Покажем, что мы всегда получим о д н у и т у ж е г р у п п у Г а л у а, какую бы функцию Галуа мы ни брали.

В самом деле возьмем произвольную функцию Галуа

$$\eta(x_1, x_2, \ldots, x_n)$$

Она по теореме Лагранжа должна выражаться рационально через y_1, так что

$$\eta = \Theta(y_1)$$

Подставив в эту функцию все корни $y_1, y_2, \ldots, y_m$, составим уравнение, корни которого будут:

$$\Theta(y_1), \ \Theta(y_2), \ \ldots, \ \Theta(y_m)$$

$$g_1(y) = (y - \Theta y_1)(y - \Theta y_2) \ldots (y - \Theta y_m)$$

Здесь мы рассматриваем y как произвольный параметр. Функция $g_1(y)$, как симметрическая от корней y_i, будет выражаться рационально в поле Ω.

Итак, функция $g_1(y)$ будет целая функция в Ω степени m. Она будет неприводимая, ибо подстановки группы Галуа переводят корни — один во все другие.

Очевидно, что переход от $\Theta(y_1)$ к другим корням совершается также при помощи подстановок группы Галуа.

Как частный случай мы рассмотрим другие множители функции $F(y)$ § 134.

Разложим всю симметрическую группу $\sum$ порядка $n!$ на системы, сопряженные с группой Галуа G:

$$\sum = G + GT_2 + GT_3 + \ldots + GT_l,$$

так что

$$ml = n!$$

Если мы введем в рассмотрение:

$$\Theta(y|T_2), \ \Theta(y|T_3), \ \ldots, \ \Theta(y|T_l),$$

то, как мы показали в общем случае, можем построить ряд резольвент одной и той же степени. Другими словами, $F(y)$ разлагается на l множителей одинаковой степени. Каждый из этих множителей может быть взят за резольвенту, и они все приводят к одной и той же группе Галуа относительно корней $x_1, x_2, \ldots, x_n$ заданного уравнения.

§ 141. Мы будем называть по примеру Коши группу **транзитивною**, если среди ее подстановок может быть указана такая, которая переводит одну букву в произвольно выбранную другую. В обратном случае группа называется *интранзитивною*.

Так, например, группа подстановок, не меняющая некоторую букву a, интранзитивна, ибо в группе не существует подстановок, заменяющих букву a на некоторую другую.

Высказанное понятие о транзитивности может быть обобщено следующим образом: группа называется m раз транзитивною, если подстановки ее допускают замену некоторых определенных m букв на m произвольно выбранных других.

В § 71 мы обратили внимание на то, что знакопеременная группа $n-2$ раз транзитивная. Симметрическая группа $n-1$ раз транзитивна.

§ 142. Пусть заданное уравнение $f(x)=0$ степени n *приводимо* в поле Ω и пусть $f_1(x)$ некоторый неприводимый в поле Ω множитель функции $f(x)$. Пусть $f_1(x)$ имеет степень m, где $m<n$.

Обозначим корни множителя $f_1(x)$ через

$$x_1,\ x_2,\ \ldots,\ x_m, \tag{1}$$

а через

$$x_{m+1},\ x_{m+2},\ \ldots,\ x_n \tag{2}$$

— остальные корни уравнения.

Обозначим через x' один из корней (1), а через x'' — один из корней (2).

Мы имеем тождество:

$$f_1(x')=0 \tag{3}$$

Предположим, что группа Галуа заданного уравнения $f(x)=0$ транзитивна. Тогда должна существовать в группе по крайней мере одна подстановка S, переводящая x' в x''.

Так как подстановки группы Галуа прилагаются ко всякому соотношению между корнями, то прилагая S к соотношению (3), получим:

$$f_1(x'')=0,$$

что противоречит предположению, и мы приходим к теореме:

Если уравнение неприводимо, то его группа транзитивна; в случае же приводимости группа должна быть интранзитивна.

Докажем теорему обратную. Пусть группа уравнений интранзитивна, причем пусть она перемещает между собой только корни (1), тогда функция:

$$f_1(x) = (x - x_1)(x - x_2) \dots (x - x_m)$$

не меняется при всех подстановках группы Галуа, значит, коэфициенты $f_1(x)$ принадлежат к полю Ω. Итак, $f_1(x)$ оказывается множителем в поле Ω функции $f(x)$, и уравнение $f(x) = 0$ приводимо.

Условием необходимым и достаточным для приводимости или неприводимости уравнения является интранзитивность или транзитивность его группы.

ПОНЯТИЕ ОБ ИМПРИМИТИВНОСТИ

§ 143. Если все n переставляемых группой букв распадаются на несколько рядов:

$$\begin{array}{llll} a_1, & a_2, & \dots, & a_k \\ a_{k+1}, & a_{k+2}, & \dots, & a_{2k} \\ \cdot & \cdot & \cdot & \cdot \\ a_{n-k+1}, & a_{n-k+2}, & \dots, & a_n \end{array} \qquad (1)$$

по k букв в каждом ряде, причем все буквы перемещаются подстановкой группы только так, что буквы рядов (1) не разделяются, другими словами, две буквы одного ряда не могут замениться буквами разных рядов, то группа называется импримитивною. Ряды (1) называются системами импримитивности.

Если нельзя разбить переставляемые буквы на системы, обладающие вышеуказанным свойством, то группа называется примитивною.

Если число переставляемых букв простое, то всякая группа примитивная.

Группа степеней круговой подстановки из шести букв:

$$s^1 = (a\,b\,c\,d\,e\,f)$$

$$s^2 = (a\,c\,e)(b\,d\,f)$$

$$s^3 = (a\,d)(b\,e)(c\,f)$$

$$s^4 = (a\,e\,c)(b\,f\,d)$$

$$s^5 = (a\,f\,e\,d\,c\,b)$$

двойным образом импримитивна, причем за системы импримитивности можно выбрать или:

$$\begin{matrix} a & c & e \\ b & d & f, \end{matrix}$$

или:

$$\begin{matrix} a & d \\ b & e \\ c & f \end{matrix}$$

§ 144. *Теорема.* Если транзитивная группа подстановок содержит отдельную транспозицию, то она или симметрическая, или импримитивная.

Итак, пусть транзитивная группа содержит транспозицию:

$$(a_1\ a_2)$$

Пусть, кроме того, в группе содержатся транспозиции:

$$(a_1\ a_3),\ (a_1\ a_4),\ (a_1\ a_5),\ \ldots,\ (a_1\ a_m),$$

переводящие букву a_1 в другие:

$$a_2,\ a_3,\ \ldots,\ a_m$$

Число m может быть равно 2, тогда в группу входит только одна транспозиция $(a_1\ a_2)$.

Если $m = n$, где n число всех букв, то группа будет симметрическая, потому что всякую транспозицию можно выразить через транспозиции, имеющие первую букву a_1:

$$(b\ c) = (a_1\ b)(a_1\ c)(a_1\ b)$$

Если $m < n$, то можно показать, что группа импримитивная.

Возьмем какую-нибудь букву b, не принадлежащую к системе:

$$a_1,\ a_2,\ \ldots,\ a_m \tag{1}$$

В группе не могут заключаться транспозиции, перемещающие букву b с какою-нибудь из букв:

$$a_2,\ a_3,\ \ldots,\ a_m$$

В самом деле, допустим обратное, т. е. что в группе находится транспозиция $(a_i\ b)$; тогда замечаем, что должна находиться в группе транспозиция:

$$(a_1\ b) = (a_i\ a_1)(a_i\ b)(a_i\ a_1),$$

что противоречит предположению, ибо a_1 перемещается с буквой b.

Так как группа транзитивна, то будет существовать некоторая подстановка T_1 (не транспозиция), переводящая букву a_1 в b_1, где b_1 не входит в систему (1). Покажем, что подстановка T_1 должна переводить все другие буквы:

$$a_2, a_3, \ldots, a_m$$

в буквы:

$$b_2, b_3, \ldots, b_m,$$

не входящие в систему (1).

Допустим обратное, а именно, что какая-нибудь буква a_i превращается подстановкой в букву a_k той же системы (1), тогда, преобразуя при помощи подстановки T_1 транспозицию $(a_1\ a_i)$, должно получиться:

$$T_1^{-1}(a_1\ a_i)T_1 = (b_1\ a_k)$$

Итак, в группе должна заключаться транспозиция $(b_1\ a_k)$, что, как мы видели, невозможно.

Если система (1) и

$$b_1,\ b_2, \ldots,\ b_m \tag{2}$$

не исчерпывают совокупности переставляемых букв, то должна существовать подстановка T_2, переводящая букву a_1 в букву c_1, не заключающуюся в системах (1) и (2).

Нетрудно видеть, что вся система букв (1) переводится подстановкой T_2 в новую систему:

$$c_1,\ c_2, \ldots,\ c_m \tag{3}$$

Мы уже знаем, что система (3) не может иметь букв, общих с системой (1).

Покажем теперь, что система (3) не заключает также элементов системы (2),

Допустим обратное, что подстановка T_2 переводит некоторую букву, например, a_2 системы (1) в некоторую букву b_i системы (2); тогда в группе должна заключаться транспозиция:

$$T_2^{-1}(a_1\ \ a_2)T_2 = (c_1\ \ b_i)$$

Преобразуем теперь полученную транспозицию при помощи подстановки T_1^{-1}. Если подстановка T_1 переводит систему (1) в (2), то обратная подстановка T_1^{-1} переводит буквы (2) в (1).

Следовательно, буква b_i заменяется некоторою a_k. Пусть подстановка переводит букву c_1 в некоторую α, которая наверно не принадлежит к системе (1); тогда в нашей группе должна существовать транспозиция:

$$T_1(c_1\ b_i)\,T_1^{-1} = (\alpha\ a_k),$$

что невозможно.

Итак, мы видим, что группа импримитивна, если только она не обращается в симметрическую.

§ 145. Покажем связь импримитивных групп с уравнениями. Результат исключения между уравнениями:

$$y^m + p_1 y^{m-1} + \ldots + p_m = 0 \tag{1}$$

$$\varphi_0(y)x^n + \varphi_1(y)x^{n-1} + \ldots + \varphi_n(y) = 0, \tag{2}$$

(где $p_1, p_2, \ldots, p_m$ принадлежат к полю Ω, а $\varphi_0, \varphi_1, \ldots \varphi_n$ суть рациональные функции из поля Ω) имеет импримитивную группу, и обратно, всякое уравнение, группа которого импримитивна, происходит от подобного исключения.

Пусть $y_1, y_2, \ldots, y_m$ будут корни уравнения (1) и пусть

$$x_1^{(\rho)},\ x_2^{(\rho)}, \ldots, x_n^{(\rho)} \tag{3}$$

$$(\rho = 1,\ 2,\ 3, \ldots,\ n)$$

будут корни другого уравнения (2), когда мы там заменим y на y_ρ. Пусть u_ρ будет произвольная симметрическая функция от этих корней уравнения (2), тогда u_ρ будет рациональной функцией от y_ρ.

$$U = (\xi - u_1)(\xi - u_2)\ldots(\xi - u_m),$$

где ξ число произвольное, будет симметрической функцией от корней $y_1, y_2, \ldots, y_m$ и может выражаться рационально. Какова будет группа уравнения степени mn, которая относится ко всем корням (3)? Эта группа не должна изменять U; она или оставляет неизменными $u_1, u_2, \ldots, u_m$, или перемещает их между собой, и следовательно, группа импримитивная.

Справедливо обратное свойство. Пусть G будет импримитивна и пусть m систем импримитивности будут:

$$x_1^{(\rho)},\ x_2^{(\rho)}, \ldots,\ x_m^{(\rho)}$$

где $\rho = 1, 2, 3, \ldots, m$.

Положим:

$$u_\rho = (\eta - x_1^{(\rho)})(\eta - x_2^{(\rho)}) \ldots (\eta - x_n^{(\rho)})$$

и

$$U = (\xi - u_1)(\xi - u_2) \ldots (\xi - u_m),$$

где ξ и η произвольны. U остается не измененным от подстановок, которые переставляют или буквы одной системы импримитивности, или же переставляют системы импримитивности. U остается не измененным от всех подстановок группы G, и может, следовательно, выражаться рационально. При помощи U можем найти все симметрические функции от $u_1, u_2, \ldots, u_m$ в рациональном виде. Величина u, будучи одним из чисел $u_1, u_2, \ldots, u_m$, получается через решение уравнения степен m с рациональными коэфициентами; когда u_ρ будет известно, тогда $x^{(\rho)}$ выразится аналогичным образом при помощи решения уравнения степени n, коэфициенты которого суть рациональные функции от u_ρ.

ПОНИЖЕНИЕ ГРУППЫ ПРИ ПОМОЩИ ПРИСОЕДИНЕНИЯ

§ 146. Порядок группы G равен степени неприводимого уравнения $g(y) = 0$. Если присоединим новые величины так, чтобы это уравнение разложилось на множители, то мы получим новую группу меньшего порядка. Так как подстановка новой группы определяется корнями нового неприводимого уравнения, а эти корни находятся среди величин $y_1, y_2, \ldots, y_m$, то новая группа заключается в прежней.

Если мы присоединим величину z_1 к некоторой рациональной функции корней, то новая группа сделается подгруппой G, которая не меняет z_1.

Величина z_1 после присоединения должна рассматриваться как элемент рациональный, поэтому всякая подстановка новой группы не должна изменять z_1 — функцию от корней. Новая группа может заключать только подстановки прежней, не нарушающие z_1.

Покажем, что кроме этих подстановок новая группа не должна заключать иных.

Рассмотрим произвольную рациональную в Ω функцию от z_1:

$$u = \varphi(z_1)$$

Произведем над этим уравнением подстановку S группы G, которая не нарушает z_1:

$$u_s = \varphi(z_s)$$

Но $z_s = z_1$, следовательно, $u_s = u$.

Итак, подстановка S не изменяет всех функций, которые могут рационально выражаться через z_1 и величины из Ω. Значит, S принадлежит на самом деле к новой группе после присоединения z_1.

О РЕШЕНИИ УРАВНЕНИЯ В РАДИКАЛАХ

§ 147. Теперь мы дадим условия необходимые и достаточные для того, чтобы уравнение могло решаться в радикалах. Если уравнение может быть решено алгебраически, то его группа должна свестись к одной подстановке 1, после присоединения всех радикалов, которые находятся в корнях, и всех корней из единицы. Группа должна сводиться к единице после присоединения корней уравнения вида:

$$z^p = A,$$

где p — простое число, а A есть величина, заключающая все раньше присоединенные величины.

Рассуждениями, приведенными в § 97, мы убеждаемся, что группа радикала $\sqrt[p]{A}$ будет инвариантной подгруппой индекса p группы перед этим присоединением, и мы приходим к теореме:

Условие необходимое и достаточное для того, чтобы уравнение могло быть решено в радикалах, состоит в том, чтобы его группа заключала ряд подгрупп:

$$G,\ G_1,\ G_2, \ldots, G_k,\ 1,$$

причем каждая подгруппа G_i должна быть инвариантною подгруппой простого индекса предыдущей группы G_{i-1}.

ТЕОРЕМА ЭЙЗЕНШТЕЙНА

§ 148. *Теорема*. Если в целой функции:

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$$

целые коэфициенты таковы, что a_0 не делится на целое простое число p, все же остальные коэфициенты $a_1, a_2, a_3, \ldots, a_n$ делятся на p, причем последний коэфициент a_n не делится на p^2, — то функция неприводима.

Допустим обратное, а именно, что функция $f(x)$ приводима, т. е.

$$f(x) = (\alpha_0 x^h + \alpha_1 x^{h-1} + \ldots + \alpha_h)(\beta_0 x^k + \beta_1 x^{k-1} + \ldots + \beta_k);$$

числа h и k — оба больше нуля и дают в сумме n.

Так как $\alpha_h \beta_k = a_n$, то из двух множителей α_h і β_k должен только один делиться на p, а другой не должен делиться. Пусть делится на p коэфициент β_k, а α_h не делится.

Все β не могут делиться на p, ибо иначе делился бы коэфициент a_0, что противоречит предположению. Итак, пусть β_λ последний коэфициент, который не делится на p, а все следующие:

$$\beta_{\lambda+1}, \quad \beta_{\lambda+2}, \ldots, \beta_n$$

делятся. Составив коэфициент при $x^{k-\lambda}$ в произведении полиномов, мы получим:

$$\alpha_h \beta_\lambda + \alpha_{h-1} \beta_{\lambda+1} + \alpha_{h-2} \beta_{\lambda+2} \ldots$$

Этот коэфициент, очевидно, не делится на p, так как первый член $\alpha_h \beta_\lambda$ не делится на p, а все остальные делятся. Приходится предположить, что $k - \lambda = n$, а это невозможно, ибо $k < n$.

§ 149. Применим теорему Эйзенштейна к доказательству неприводимости:

$$X_p(x) = x^{p-1} + x^{p-2} + \ldots + x + 1$$

при p простом.

Мы имеем:

$$X_p = \frac{x^p - 1}{x - 1}$$

Положим $x = z + 1$, тогда получим:

$$X_p(z+1) = \frac{1}{z}[(z+1)^p - 1] =$$

$$= z^{p-1} + pz^{p-2} + \frac{p(p-1)}{1 \cdot 2} z^{p-3} + \ldots + p$$

В правой части все коэфициенты кроме первого делятся на p, причем последний делится только на первую степень p. Значит, $X_p(z+1)$ есть функция неприводимая, а следовательно, то же самое будет иметь место также для функции $X_p(x)$, что и требовалось доказать.

УРАВНЕНИЕ БЕЗ АФФЕКТА

§ 150. Кронекер называет уравнением без аффекта такое уравнение, когда его группа есть вся симметрическая группа подстановок.

Мы видим, что буквенные уравнения суть уравнения без аффекта.

Если уравнение решается в радикалах, то его группа должна быть подгруппой симметрической, и тогда Кронекер говорит, что оно имеет аффект.

В § 97 мы видели, что общее буквенное уравнение при $n > 4$ не решается в радикалах. При помощи аналогичных соображений, основанных на соображениях теории Галуа, численные уравнения без аффекта тоже не будут решаться в радикалах.

Покажем, что существуют численные уравнения без аффекта.

Я приведу пример подобного уравнения:

$$x^5 - p^2x - p = 0, \tag{1}$$

где p простое число. Посмотрим как найти группу уравнения (1).

Так как первая часть уравнения имеет при

$$-\infty, \quad -1, \quad 0, \quad +\infty$$

знаки:

$$-, \quad +, \quad -, \quad +,$$

то существует три вещественных корня уравнения. Остальные два корня обязательно мнимые, ибо в уравнении имеется пропуск трех членов со степенями (см. § 111):

$$x^4, \quad x^3, \quad x^2$$

Так как числа основного поля вещественны, то всякое соотношение между корнями будет иметь вид:

$$a + ib = 0,$$

откуда

$$a=0 \quad \text{и} \quad b=0,$$

а следовательно, и

$$a-ib=0$$

Другими словами, всякое соотношение между корнями не нарушается от изменения знака перед i.

Если мы обозначим через 1 и 2 мнимые корни, то изменение знака перед i осуществляется при помощи транспозиции (1 2); итак, мы видим, что транспозиция должна входить в группу Галуа. По теореме Эйзенштейна уравнение (1) неприводимо в основном поле R, следовательно, его группа транзитивна. Мы видели, что транзитивная группа, если она имеет транспозицию (1 2), — или симметрическая, или же импримитивная.

Уравнение (1) задано — простой степени, значит, число корней простое, а потому группа подстановок этих корней не может быть импримитивною. Итак, мы видим, что группа Галуа уравнения (1) есть симметрическая, т. е. уравнение (1) не имеет аффекта.

ОБ УРАВНЕНИЯХ, РЕШАЮЩИХСЯ В РАДИКАЛАХ

§ 151. Гаусс показал, что уравнения, которые служат делению окружности на равные части, решаются в радикалах. Эти уравнения входят в состав класса уравнений, изученных позднее Абелем, и которые, по предложению Кронекера, носят название абелевых уравнений. Эти уравнения характеризуются свойством, что один корень его может выражаться рационально через другой.

Абелевы уравнения могут всегда приводиться к уравнениям низших степеней и часто даже решаться алгебраически.

ДВУЧЛЕННЫЕ УРАВНЕНИЯ И ДЕЛЕНИЕ КРУГА

§ 152. Мы уже знаем, что корни уравнения

$$x^n-1=0 \tag{1}$$

имеют вид:

$$x=e^{\frac{2k\pi}{n}i}=\cos\frac{2k\pi}{n}+i\sin\frac{2k\pi}{n}$$

$$(k=0,\ 1,\ 2,\ 3,\ldots,\ n-1)$$

В правой части все коэфициенты кроме первого делятся на p, причем последний делится только на первую степень p. Значит, $X_p(z+1)$ есть функция неприводимая, а следовательно, то же самое будет иметь место также для функции $X_p(x)$, что и требовалось доказать.

УРАВНЕНИЕ БЕЗ АФФЕКТА

§ 150. Кронекер называет уравнением без аффекта такое уравнение, когда его группа есть вся симметрическая группа подстановок.

Мы видим, что буквенные уравнения суть уравнения без аффекта.

Если уравнение решается в радикалах, то его группа должна быть подгруппой симметрической, и тогда Кронекер говорит, что оно имеет аффект.

В § 97 мы видели, что общее буквенное уравнение при $n>4$ не решается в радикалах. При помощи аналогичных соображений, основанных на соображениях теории Галуа, численные уравнения без аффекта тоже не будут решаться в радикалах.

Покажем, что существуют численные уравнения без аффекта.

Я приведу пример подобного уравнения:

$$x^5-p^2x-p=0, \tag{1}$$

где p простое число. Посмотрим как найти группу уравнения (1).

Так как первая часть уравнения имеет при

$$-\infty, \quad -1, \quad 0, \quad +\infty$$

знаки:

$$-, \quad +, \quad -, \quad +,$$

то существует три вещественных корня уравнения. Остальные два корня обязательно мнимые, ибо в уравнении имеется пропуск трех членов со степенями (см. § 111):

$$x^4, \quad x^3, \quad x^2$$

Так как числа основного поля вещественны, то всякое соотношение между корнями будет иметь вид:

$$a+ib=0,$$

откуда

$$a=0 \quad \text{и} \quad b=0,$$

а следовательно, и

$$a-ib=0$$

Другими словами, всякое соотношение между корнями не нарушается от изменения знака перед i.

Если мы обозначим через 1 и 2 мнимые корни, то изменение знака перед i осуществляется при помощи транспозиции (1 2); итак, мы видим, что транспозиция должна входить в группу Галуа. По теореме Эйзенштейна уравнение (1) неприводимо в основном поле R, следовательно, его группа транзитивна. Мы видели, что транзитивная группа, если она имеет транспозицию (1 2), — или симметрическая, или же импримитивная.

Уравнение (1) задано — простой степени, значит, число корней простое, а потому группа подстановок этих корней не может быть импримитивною. Итак, мы видим, что группа Галуа уравнения (1) есть симметрическая, т. е. уравнение (1) не имеет аффекта.

ОБ УРАВНЕНИЯХ, РЕШАЮЩИХСЯ В РАДИКАЛАХ

§ 151. Гаусс показал, что уравнения, которые служат делению окружности на равные части, решаются в радикалах. Эти уравнения входят в состав класса уравнений, изученных позднее Абелем, и которые, по предложению Кронекера, носят название *абелевых* уравнений. Эти уравнения характеризуются свойством, что один корень его может выражаться рационально через другой.

Абелевы уравнения могут всегда приводиться к уравнениям низших степеней и часто даже решаться алгебраически.

ДВУЧЛЕННЫЕ УРАВНЕНИЯ И ДЕЛЕНИЕ КРУГА

§ 152. Мы уже знаем, что корни уравнения

$$x^n-1=0 \tag{1}$$

имеют вид:

$$x=e^{\frac{2k\pi}{n}i}=\cos\frac{2k\pi}{n}+i\sin\frac{2k\pi}{n}$$

$$(k=0,\ 1,\ 2,\ 3,\ldots,\ n-1)$$

Отсюда видно, что задача решения уравнения (1) равносильна задаче деления окружности на n равных частей или задаче вписывания в круг правильного многоугольника.

Древним математикам были известны построения циркулем и линейкой вписанных правильных многоугольников, имеющих число сторон, выражаемое одной из следующих формул:

$$2^n, \quad 3 \cdot 2^n, \quad 5 \cdot 2^n, \quad 3 \cdot 5 \cdot 2^n$$

Новый шаг в вопросе построения правильных многоугольников циркулем и линейкой был сделан Гауссом в его знаменитом сочинении „Disquisitiones arithmeticae“ (§§ 365—366). Гаусс дает такую теорему:

Для разрешимости уравнения

$$x^n - 1 = 0$$

в квадратных радикалах необходимо и достаточно, чтобы было одно из трех:

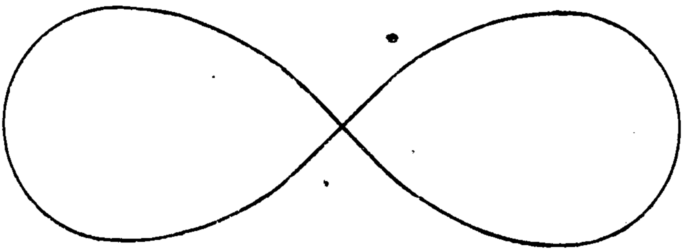

Рис. 21.

1) число n—простое число вида $2^h + 1$;

2) $n = 2^m$;

3) число n есть произведение чисел предыдущих видов.

Гаусс добавляет весьма важное соображение, что для чисел, для которых можно делить циркулем и линейкой окружность круга, можно делить на равные части и обвод кривой линии лемнискаты.

Очевидно, что число h, фигурирующее в теореме Гаусса должно иметь вид:

$$h = 2^k,$$

ибо, если $h = 2^k(2r + 1)$, то число

$$2^h + 1 = [2^{2^k}]^{(2r+1)} + 1$$

делится на $2^{2^k}+1$ и, следовательно, не может быть простым числом.

Таким образом, простые числа надо искать среди чисел

$$2^{2^k}+1$$

Относительно этих чисел Фермат сделал предположение (оказавшееся не верным), что все они простые. В действительности же оказалось, что получаются простые числа при

$$k=0,\ 1,\ 2,\ 3,\ 4,$$

а именно:

$$3,\ 5,\ 17,\ 257,\ 65\,537$$

Построение циркулем и линейкой многоугольника с числом сторон 257 произвел по методу Гаусса Ришело[1]) и, наконец, случай 65 537 выполнил Хермес[1]).

Далее, для числа $k=5$ Эйлер показал, что получается число составное:

$$2^{2^5}+1=4\,294\,967\,297=641\cdot 6\,700\,417$$

Затем сложность числа показал Ландри в случае

$$2^{2^6}+1,$$

и затем Первушин для

$$2^{2^{12}}+1 \quad \text{i} \quad 2^{2^{23}}+1$$

Остается открытым вопрос, будет ли конечным число простых чисел в ряде

$$2^{2^M}+1$$

или нет.

§ 153. Корни уравнения $x^n-1=0$ в их тригонометрической форме суть:

$$r=1, r=e^{\frac{2\pi}{n}i},\ r^2=e^{\frac{2\,.\,2\pi}{n}i}\ ,\ldots,\ r^k=e^{\frac{2k\pi}{n}i},\ \ldots,\ r^{n-1}=e^{\frac{2(n-1)\pi}{n}i}$$

Мы видим, что все корни выражаются степенями одного корня:

$$r=e^{\frac{2\pi i}{n}}=\cos\frac{2\pi}{n}+i\sin\frac{2\pi}{n}$$

---

*) Journal für reine und angew. Math., 9, 11, 1832.

**) Gött. Nachr., 1894.

Такой корень называется первообразным, его первая степень, обращающаяся в единицу, будет n.

Корень

$$r_1^k = e^{\frac{2k\pi}{n} i},$$

в котором k будет делителем числа n, так что $k \cdot l = n$, не будет первообразным, ибо уже l-ая степень корня r_1^k будет давать единицу.

Первообразные корни получаются, когда k будет число меньшее n и взаимно простое с n. Число таких чисел представляет арифметическую функцию от n, которая обычно обозначается $\varphi(n)$. В случае n числа простого будет:

$$\varphi(n) = n - 1$$

Все корни, кроме единицы, будут первообразные, ибо все числа $1, 2, 3, \ldots, n-1$ будут взаимно простые с n.

§ 154. Предполагая число n произвольным, не обязательно простым, обозначим корни уравнения $x^n - 1 = 0$ через:

$$\alpha_0 = 1,\ \alpha_1 = r,\ \alpha_2 = r^2,\ \alpha_3 = r^3, \ldots,\ \alpha_{n-1} = r^{n-1}$$

Вычислим по формулам Ньютона суммы s_k одинаковых степеней корней. Коэфициенты нашего уравнения суть:

$$p_0 = 1,\ p_1 = 0,\ p_2 = 0, \ldots,\ p_{n-1} = 0,\ p_n = -1;$$

тогда про формуле Ньютона получим:

$$s_1 = \alpha_0 + \alpha_1 + \alpha_2 + \ldots + \alpha_{n-1} = 0$$

$$s_2 = \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \ldots + \alpha_{n-1}^2 = 0$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$s_k = \alpha_0^k + \alpha_1^k + \alpha_2^k + \ldots + \alpha_{n-1}^k = 0$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$s_{n-1} = \alpha_0^{n-1} + \alpha_1^{n-1} + \alpha_2^{n-1} + \ldots + \alpha_{n-1}^{n-1} = 0$$

$$s_n = \alpha_0^n + \alpha_1^n + \alpha_2^n + \ldots + \alpha_{n-1}^n = n$$

АБЕЛЕВЫ УРАВНЕНИЯ

§ 155. Мы ограничимся уравнением, корни которого могут быть представлены в форме:

$$x_1,\ x_2 = \theta(x_1),\ x_3 = \theta^2(x_1),\ \ldots,\ x_k = \theta^{k-1}(x_1), \ldots,\ x_n = \theta^{n-1}(x_1),$$

где θ знак рациональной функции из поля Ω, а

$$\theta^2 = \theta\theta,\quad \theta^3 = \theta\theta\theta \text{ и т. д.},$$

причем

$$\theta^n(x_1) = x_1$$

Обозначим через α какой-нибудь корень $x^n = 1$; тогда в выражении:

$$\omega(x_1) = [x_1 + \alpha\theta(x_1) + \alpha^2\theta^2(x_1) + \ldots + \alpha^{n-1}\theta^{n-1}(x_1)]^n \tag{1}$$

мы будем рассматривать α как известное постоянное число. Если вместо x_1 мы подставим $x_2 = \theta(x_1)$, то получим:

$$\omega(x_2) = [\theta(x_1) + \alpha\theta^2(x_1) + \alpha^2\theta^3(x_1) + \ldots + \alpha^{n-1}x_1]^n \tag{2}$$

Выражение в квадратных скобках (2) получается из выражения в квадратных скобках (1) через умножение на α^{n-1}, но так как $\alpha^{n(n-1)} = 1$, то оба выражения одинаковы, и мы получаем:

$$\omega(x_1) = \omega(x_2) = \ldots = \omega(x_n)$$

Отсюда:

$$\omega(x_1) = \frac{1}{n}[\omega(x_1) + \omega(x_2) + \ldots + \omega(x_n)]$$

Итак, ω будучи симметрической функцией от корней, выражается рационально через коэфициенты заданного уравнения, через коэфициенты функции $\theta(x)$ и через α.

Обозначим через

$$u_0,\ u_1,\ u_2, \ldots,\ u_{n-1}$$

выражение $\omega(x)$, если мы подставим в него вместо α значения:

$$\alpha_0,\ \alpha_1,\ \alpha_2, \ldots,\ \alpha_{n-1}$$

Мы получим (§ 154):

$$\begin{aligned}
&x_1 + \theta(x_1) + \theta^2(x_1) + \ldots + \theta^{n-1}(x_1) = \sqrt[n]{u_0} \\
&x_1 + \alpha_1\theta(x_1) + \alpha_1^2\theta^2(x_1) + \ldots + \alpha^{n-1}\theta^{n-1}(x_1) = \sqrt[n]{u_1} \qquad (3)\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
&x_1 + \alpha_{n-1}\theta(x_1) + \alpha_{n-1}^2\theta^2(x_1) + \ldots + \alpha_{n-1}^{n-1}\theta^{n-1}(x) = \sqrt[n]{u_{n-1}}
\end{aligned}$$

$\sqrt{u_0}$, как сумма корней, очевидно, равняется $-A$, где A коэфициент при x^{n-1} в заданном уравнении.

Складывая равенства (3) и принимая во внимание равенства (1) § 154, получим:

$$x_1 = \frac{-A + \sqrt[n]{u_1} + \sqrt[n]{u_2} + \ldots + \sqrt[n]{u_{n-1}}}{n} \tag{4}$$

Умножая уравнения (3) по порядку на

$$\alpha_0^{-m},\ \alpha_1^{-m}, \ldots$$

и складывая, заметим, что, на основании равенств (1) § 154, мы при сложении обратим в нуль все члены, кроме $\theta^m(x_1)$, и мы получим этот корень по формуле:

$$\theta^m(x_1) = \frac{-A + \alpha_2^{-m}\sqrt[n]{u_1} + \alpha_3^{-m}\sqrt[n]{u_2} + \ldots + \alpha_{n-1}^{-m}\sqrt[n]{u_{n-1}}}{n} \tag{5}$$

Так как каждый из радикалов:

$$\sqrt[n]{u_1},\ \sqrt[n]{u_2},\ \ldots,\ \sqrt[n]{u_{n-1}} \tag{6}$$

может иметь n значений, то, очевидно, получается слишком большое число значений, а нам надо получить, применяя выражения (4) и (5), только n корней. Между значениями (6) радикалов должны существовать определенные соотношения.

Покажем, что можно всегда радикал

$$\sqrt[n]{u_p}$$

при всяком p выразить через один из радикалов (6), например, через $\sqrt[n]{u_1}$.

Если в выражении u_1 буква α обозначает примитивный корень из единицы, то другие корни будут:

$$\alpha_p = \alpha^p$$

Тогда мы имеем:

$$\sqrt[n]{u_1} = x + \alpha\theta(x) + \alpha^2\theta^2(x) + \ldots + \alpha^{n-1}\theta^{n-1}(x) \tag{7}$$

$$\sqrt[n]{u_p} = x + \alpha^p\theta(x) + \alpha^{2p}\theta^2(x) + \ldots + \alpha^{p(n-1)}\theta^{n-1}(x) \tag{8}$$

Если мы заменим x на $\theta^m(x)$, то (7) умножится на α^{-m}, а (8) на α^{-pm}; тогда выражение:

$$N = (\sqrt[n]{u_1})^{n-p} \cdot \sqrt[n]{u_p}$$

получит множитель:

$$\alpha^{-m(n-p)} \cdot \alpha^{-mp} = \alpha^{-mn} = 1$$

N не изменяется, если x заменить другим корнем $\theta^m(x)$, значит, подобно тому, что мы сказали об $\omega(x)$, число N выражается рационально через коэфициенты уравнения и коэфициенты функции $\theta(x)$. Обозначим выражение N, соответствующее корню α^p, знаком N_p; мы получим:

$$\sqrt[n]{u_p} = \frac{N_p}{u_1}\left(\sqrt[n]{u_1}\right)^p$$

Итак, все радикалы (6) выражаются через один $\sqrt[n]{u_1}$, и тогда давая радикалу $\sqrt[n]{u_1}$ все его n значений, получим n корней заданного уравнения.

§ 156. Абель делает далее замечание, что, если все корни уравнения выражаются рационально через один:

$$\theta_1(x),\ \theta_2(x),\ \theta_3(x), \ldots,\ \theta_n(x),$$

где θ_i произвольные функции, то уравнение вообще не решается в радикалах. Но если эти функции удовлетворяют равенствам:

$$\theta_k\theta_l(x) = \theta_l\theta_k(x)$$

$$(l,\ k = 1,\ 2, \ldots,\ n),$$

то уравнение решается в радикалах.

Случай x, $\theta(x)$, $\theta^2(x), \ldots,$ $\theta^{n-1}(x)$ — есть частный случай.

УРАВНЕНИЯ ДВУЧЛЕННЫЕ

§ 157. Гаусс показал, что все двучленные уравнения решаются в радикалах. Абель называет изложенный в § 155 метод методом Гаусса. Я бы сказал, что этот метод, как признает сам Гаусс, принадлежит Лагранжу.

Мы ограничимся рассмотрением уравнения:

$$x^{17} - 1 = 0, \tag{1}$$

так как рассмотрение этого уравнения привело Гаусса к построению циркулем и линейкой правильного вписанного в круг 17-угольника.

Обозначим $x=\alpha$ и рассмотрим уравнение 16-ой степени

$$\alpha^{16}+\alpha^{15}+\alpha^{14}+\ldots+\alpha^3+\alpha^2+\alpha+1=0 \qquad (2)$$

Это уравнение принадлежит к так называемым возвратным, ибо его коэфициенты, равно отстоящие от двух концов уравнения, одинаковы.

Тогда, если один корень уравнения есть α, то другой будет $\frac{1}{\alpha}$. Деля уравнение (2) на α^8, получим

$$\left(\alpha^8+\frac{1}{\alpha^8}\right)+\left(\alpha^7+\frac{1}{\alpha^7}\right)+\ldots+\left(\alpha^2+\frac{1}{\alpha^2}\right)+\left(\alpha+\frac{1}{\alpha}\right)+ \\ +1=0 \qquad (3)$$

Если мы обозначим:

$$z=\alpha+\frac{1}{\alpha},$$

то, обозначая:

$$\psi_n(z)=z^n+\frac{1}{z^n},$$

получим:

$$z\,\psi_{n-1}(z)=\left(\alpha+\frac{1}{\alpha}\right)\left(\alpha^{n-1}+\frac{1}{\alpha^{n-1}}\right)=\alpha^n+\frac{1}{\alpha^n}+\alpha^{n-2}+\frac{1}{\alpha^{n-2}}$$

Мы имеем соотношение:

$$\psi_n=z\,\psi_{n-1}-\psi_{n-2};$$

Тогда мы получаем:

$$\psi_1=z,\quad \psi_2=z^2-2,\quad \psi_3=z^3-3z,\quad \psi_4=z^4-4z^2+2,$$
$$\psi_5=z^5-5z^3+5z,\ \psi_6=z^6-6z^4+9z^2-2,\ \psi_7=z^7-7z^5+14z^3-7z,$$
$$\psi_8=z^8-8z^6+20z^4-16z^2+2$$

Подставляя полученные выражения в уравнение (3), сведем наше возвратное уравнение к такому уравнению 8-й степени:

$$z^8+z^7-7z^6-6z^5+15z^4-10z^3+10z^2-4z+1=1; \qquad (4)$$

этому уравнению удовлетворяют величины:

$$z=e^{\frac{2k\pi}{n}i}+e^{\frac{-2k\pi}{17}i}=2\cos\frac{2k\pi}{17},$$

где $k=1,\ 2,\ 3,\ldots,8.$

Уравнение (4) имеет степень с показателем $2^3=8$ и может быть решено по методу Гаусса при помощи трех уравнений второй степени.

§ 158. Мы предпочитаем рассматривать уравнение:

$$\alpha^{16}+\alpha^{15}+\ldots+\alpha^2+\alpha+1=0 \tag{1}$$

и возьмем так называемый примитивный корень сравнения:

$$x^{16}\equiv 1 \pmod{17}$$

Под примитивным корнем этого сравнения мы будем разуметь целое число ρ такое, что все его степени:

$$\rho^0,\ \rho^1,\ \rho^2,\ \rho^3,\ \ldots,\ \rho^{15} \tag{2}$$

различны и при делении на 17 не дают остатка—единицы.

Существование таких первообразных корней мы не будем доказывать. Достаточно указать, что один из таких первообразных корней будет число 3, в чем легко убедиться непосредственно.

Возьмем два выражения:

$$\begin{aligned} y_1&=\alpha^{\rho^0}+\alpha^{\rho^2}+\alpha^{\rho^4}+\alpha^{\rho^6}+\alpha^{\rho^8}+\alpha^{\rho^{10}}+\alpha^{\rho^{12}}+\alpha^{\rho^{14}}\\ y_2&=\alpha^{\rho}+\alpha^{\rho^3}+\alpha^{\rho^5}+\alpha^{\rho^7}+\alpha^{\rho^9}+\alpha^{\rho^{11}}+\alpha^{\rho^{13}}+\alpha^{\rho^{15}} \end{aligned} \tag{3}$$

Так как все показатели различны по модулю 17, то мы имеем 16 корней уравнения (1) и

$$y_1+y_2=-1, \tag{4}$$

как сумма всех корней уравнения.

Будем заменять

$$\alpha \quad \text{на} \quad \alpha^{\rho^k},$$

тогда всякий корень α^{ρ^l} обратится в

$$(\alpha^{\rho^k})^{\rho^l}=\alpha^{\rho^{k+l}},$$

и мы видим, что если l число четное, то после замены y_1 и y не меняются; если же l число нечетное, то y_1 и y_2 перемещаются; отсюда мы видим, что произведение

$$y_1y_2$$

не меняется от подстановки вместо одного корня всех остальных. Значит, это произведение есть симметрическая функция от корней, так что оно есть рациональное число; но всякое произведение двух корней есть также корень, а потому y_1y_2 представляет сумму 64 корней, между которыми не находится единица, ибо два корня, дающие в произведении единицу, заключаются в одной из групп y_1 или y_2.

Итак, функция y_1y_2 есть симметрическая, а потому в нее входят все 16 корней по 4 раза:

$$y_1 y_2 = -4 \tag{5}$$

Мы видим, что y_1 и y_2 суть корни квадратного уравнения:

$$y^2 + y - 4 = 0 \tag{6}$$

Положим теперь:

$$\begin{aligned} \alpha^{\rho^0} + \alpha^{\rho^4} + \alpha^{\rho^8} + \alpha^{\rho^{12}} &= z_1 \\ \alpha^{\rho^2} + \alpha^{\rho^6} + \alpha^{\rho^{10}} + \alpha^{\rho^{14}} &= z_2 \end{aligned} \tag{7}$$

$$\begin{aligned} \alpha^{\rho} + \alpha^{\rho^5} + \alpha^{\rho^9} + \alpha^{\rho^{13}} &= z_3 \\ \alpha^{\rho^3} + \alpha^{\rho^7} + \alpha^{\rho^{11}} + \alpha^{\rho^{15}} &= x_4, \end{aligned} \tag{8}$$

отсюда:

$$z_1 + z_2 = y_1, \quad z_3 + z_4 = y_2$$

Будет проще, если мы не будем рассматривать общее значение ρ, а возьмем:

$$\rho = 3$$

Уравнения (7) и (8) можно будет переписать так:

$$\begin{aligned} \alpha + \alpha^{13} + \alpha^{-1} + \alpha^{-13} &= z_1 \\ \alpha^9 + \alpha^{15} + \alpha^{-9} + \alpha^{-15} &= z_2 \end{aligned} \tag{7'}$$

$$\begin{aligned} \alpha^3 + \alpha^5 + \alpha^{-3} + \alpha^{-5} &= z_3 \\ \alpha^{10} + \alpha^{11} + \alpha^{-10} + \alpha^{-11} &= z_4 \end{aligned} \tag{8'}$$

Составим непосредственно произведение z_1z_2:

$$\begin{aligned} z_1z_2 = \alpha^{10} + \alpha^{16} + \alpha^{-8} + \alpha^{-14} + \\ + \alpha^5 + \alpha^{11} + \alpha^4 + \alpha^{-2} + \\ + \alpha^8 + \alpha^{14} + \alpha^{-10} + \alpha^{-16} + \\ + \alpha^{-4} + \alpha^2 + \alpha^{-5} + \alpha^{11} \end{aligned}$$

Это есть сумма всех корней уравнения (1), и мы получаем:

$$z_1 z_2 = -1 \tag{9}$$

Получим то же самое для произведения z_3z_4, ибо разница состоит в том, что корень α заменяется на α^3, так что

$$z_3 z_4 = -1 \tag{10}$$

Итак, z_1, z_2, z_3, z_4 суть корни двух квадратных уравнений:

$$z^2-y_1z-1=0,\quad z^2-y_2z-1=0 \tag{11}$$

Далее вводим новые неизвестные t_1 і t_2:

$$\begin{aligned} \alpha+\alpha^{-1} &= t_1 \\ \alpha^{13}+\alpha^{-13} &= t_2 \end{aligned} \tag{12}$$

Мы получим:

$$t_1+t_2=z_1$$

Перемножая два выражения (12), получим:

$$t_1\,t_2=\alpha^{-3}+\alpha^5+\alpha^{-5}+\alpha^3=z_3$$

Итак, t_1 и t_2 суть корни уравнения:

$$t^2-z_1t+z_3=0,$$

и мы имеем:

$$\begin{aligned} t_1 &= \alpha+\alpha^{-1}=2\cos a \\ t_2 &= \alpha^4+\alpha^{-4}=2\cos 4a, \end{aligned}$$

где

$$a=\frac{2\pi}{17},$$

а, значит,

$$2\cos 4a=2\cos\frac{8\pi}{17}=2\sin\frac{\pi}{34}$$

Мы видим, что $2\cos 4a$ есть сторона правильного вписанного в круг многоугольника с 34 сторонами.

Итак, мы можем построить эту сторону при помощи циркуля и линейки, построив сначала y_1 и y_2 при помощи уравнения:

$$y^2+y-4=0;$$

далее построим четыре z при помощи уравнений:

$$z^2-y_1z-1=0,\quad z^2-y_2z-1=0$$

и, наконец, находим t_2 при помощи уравнения:

$$t^2-z_1t+z_3=0$$

7. VI 1937
Киев

изведение двух корней есть также корень, а потому $y_1 y_2$ представляет сумму 64 корней, между которыми не находится единица, ибо два корня, дающие в произведении единицу, заключаются в одной из групп y_1 или y_2.

Итак, функция $y_1 y_2$ есть симметрическая, а потому в нее входят все 16 корней по 4 раза:

$$y_1 y_2 = -4 \tag{5}$$

Мы видим, что y_1 и y_2 суть корни квадратного уравнения:

$$y^2 + y - 4 = 0 \tag{6}$$

Положим теперь:

$$\left.\begin{aligned} \alpha^{\rho^0} + \alpha^{\rho^4} + \alpha^{\rho^8} + \alpha^{\rho^{12}} &= z_1 \\ \alpha^{\rho^2} + \alpha^{\rho^6} + \alpha^{\rho^{10}} + \alpha^{\rho^{14}} &= z_2 \end{aligned}\right\} \tag{7}$$

$$\left.\begin{aligned} \alpha^{\rho} + \alpha^{\rho^5} + \alpha^{\rho^9} + \alpha^{\rho^{13}} &= z_3 \\ \alpha^{\rho^3} + \alpha^{\rho^7} + \alpha^{\rho^{11}} + \alpha^{\rho^{15}} &= x_4, \end{aligned}\right\} \tag{8}$$

отсюда:

$$z_1 + z_2 = y_1, \quad z_3 + z_4 = y_2$$

Будет проще, если мы не будем рассматривать общее значение ρ, а возьмем:

$$\rho = 3$$

Уравнения (7) и (8) можно будет переписать так:

$$\left.\begin{aligned} \alpha + \alpha^{13} + \alpha^{-1} + \alpha^{-13} &= z_1 \\ \alpha^9 + \alpha^{15} + \alpha^{-9} + \alpha^{-15} &= z_2 \end{aligned}\right\} \tag{7'}$$

$$\left.\begin{aligned} \alpha^3 + \alpha^5 + \alpha^{-3} + \alpha^{-5} &= z_3 \\ \alpha^{10} + \alpha^{11} + \alpha^{-10} + \alpha^{-11} &= z_4 \end{aligned}\right\} \tag{8'}$$

Составим непосредственно произведение $z_1 z_2$:

$$\begin{aligned} z_1 z_2 = \alpha^{10} + \alpha^{16} + \alpha^{-8} + \alpha^{-14} + \\ + \alpha^5 + \alpha^{11} + \alpha^4 + \alpha^{-2} + \\ + \alpha^8 + \alpha^{14} + \alpha^{-10} + \alpha^{-16} + \\ + \alpha^{-4} + \alpha^2 + \alpha^{-5} + \alpha^{11} \end{aligned}$$

Это есть сумма всех корней уравнения (1), и мы получаем:

$$z_1 z_2 = -1 \tag{9}$$

Получим то же самое для произведения $z_3 z_4$, ибо разница состоит в том, что корень α заменяется на α^3, так что

$$z_3 z_4 = -1 \tag{10}$$

Итак, z_1, z_2, z_3, z_4 суть корни двух квадратных уравнений:

$$z^2 - y_1 z - 1 = 0, \quad z^2 - y_2 z - 1 = 0 \tag{11}$$

Далее вводим новые неизвестные t_1 і t_2:

$$\begin{aligned} \alpha + \alpha^{-1} &= t_1 \\ \alpha^{13} + \alpha^{-13} &= t_2 \end{aligned} \tag{12}$$

Мы получим:

$$t_1 + t_2 = z_1$$

Перемножая два выражения (12), получим:

$$t_1 t_2 = \alpha^{-3} + \alpha^5 + \alpha^{-5} + \alpha^3 = z_3$$

Итак, t_1 и t_2 суть корни уравнения:

$$t^2 - z_1 t + z_3 = 0,$$

и мы имеем:

$$\begin{aligned} t_1 &= \alpha + \alpha^{-1} = 2\cos a \\ t_2 &= \alpha^{4} + \alpha^{-4} = 2\cos 4a, \end{aligned}$$

где

$$a = \frac{2\pi}{17},$$

а, значит,

$$2\cos 4a = 2\cos\frac{8\pi}{17} = 2\sin\frac{\pi}{34}$$

Мы видим, что $2\cos 4a$ есть сторона правильного вписанного в круг многоугольника с 34 сторонами.

Итак, мы можем построить эту сторону при помощи циркуля и линейки, построив сначала y_1 и y_2 при помощи уравнения:

$$y^2 + y - 4 = 0;$$

далее построим четыре z при помощи уравнений:

$$z^2 - y_1 z - 1 = 0, \quad z^2 - y_2 z - 1 = 0$$

и, наконец, находим t_2 при помощи уравнения:

$$t^2 - z_1 t + z_3 = 0$$

7. VI 1937
Киев

INDEX NOMINUM

INDEX RERUM

СОДЕРЖАНИЕ

ПОДГОТОВЛЕН К ПЕЧАТИ ВТОРОЙ ТОМ

ТРАКТАТА ПО АЛГЕБРАИЧЕСКОМУ АНАЛИЗУ

ПОД ЗАГЛАВИЕМ:

ИСТОРИЧЕСКИЙ ОБЗОР

СОДЕРЖАНИЕ

ПОДГОТОВЛЕН К ПЕЧАТИ ВТОРОЙ ТОМ

ТРАКТАТА ПО АЛГЕБРАИЧЕСКОМУ АНАЛИЗУ

ПОД ЗАГЛАВИЕМ:

ИСТОРИЧЕСКИЙ ОБЗОР

СОДЕРЖАНИЕ

Уповнов. Головліту № 2231. Зам. № 556. Вид. № 745. Тир. 3000. Форм. пап. 72×108 *см*. Вага 50,3 *кг*. Пап. арк. 6⁹/₁₆. Друк. зн. в 1 пап. арк. 82 т. Здано до друк. 26/IV 1938 р. Підписано до друку 21/VI 1938 р.