Независимый Московский Университет
Математический колледж

Г. Л. Рыбников

Лекции по алгебре

Первый курс, осенний семестр 1995/96 г.

Москва
1995

Лекция 1.

Большая часть материала этих лекций есть в учебнике А. И. Кострикина «Введение в алгебру. Основы алгебры» (М.: Физматлит, 1994; предыдущее издание: «Введение в алгебру», М.: Наука, 1977), хотя порядок тем и изложение может отличаться от нашего. Я буду считать известным язык и обозначения теории множеств (Кострикин, Гл. 1, §5.1) и принцип математической индукции (Кострикин, Гл. 1, §7).

Определения коммутативного кольца и поля

Первую алгебраическую структуру, с которой мы встречаемся, образуют числа. Алгебраиста интересуют прежде всего алгебраические операции над числами: сложение и умножение. Общий принцип математики — постараться выделить главные (необходимые) свойства интересующего нас объекта и использовать их как аксиомы. Какие же свойства имеют сложение и умножение чисел?

Числа бывают разные: числа натурального ряда ($\mathbb{N}$), целые ($\mathbb{Z}$), рациональные ($\mathbb{Q}$), вещественные ($\mathbb{R}$). Многие из вас знают и комплексные числа ($\mathbb{C}$), к их определению я еще вернусь. Пусть A обозначает $\mathbb{Q}$ или $\mathbb{R}$. Тогда выполнены следующие свойства:

(A1) Коммутативность сложения: для любых a и b из A

$$a + b = b + a.$$

(A2) Ассоциативность сложения: для любых a, b и c из A

$$(a + b) + c = a + (b + c).$$

(A3) Существование нуля: существует такой элемент $0 \in A$, называемый *нулем*, что для любого элемента a из A

$$0 + a = a.$$

(A4) Существование противоположных элементов: для любого a из A уравнение

$$a + x = 0$$

имеет единственное решение. Элемент из A, удовлетворяющий этому уравнению, называется *обратным по сложению* (или *противоположным*) к a и обозначается $-a$.

(M1) Коммутативность умножения: для любых a, и b из A

$$a \cdot b = b \cdot a.$$

(M2) Ассоциативность умножения: для любых a, b и c из A

$$(a \cdot b) \cdot c = a \cdot (b \cdot c).$$

(M3) Существование единицы: существует такой ненулевой элемент $1 \in A$, называемый *единицей*, что для любого элемента a из A

$$1 \cdot a = a \cdot 1 = a.$$

(M4) Существование обратных элементов: для любого $a \neq 0$ из A уравнение

$$a \cdot x = 1$$

имеет единственное решение. Элемент из A, удовлетворяющий этому уравнению, называется *обратным по умножению* (или просто *обратным*) к a и обозначается a^{-1}.

(AM) Дистрибутивность умножения относительно сложения: для любых a, b и c из A

$$a \cdot (b + c) = a \cdot b + a \cdot c.$$

Определение 1.1. *Полем* называется любое множество A с операциями сложения и умножения, для которого выполнены свойства (A1)–(A4), (M1)–(M4) и (AM) (называемые *аксиомами поля*).

Множество $\mathbb{Z}$ целых чисел с обычными сложением и умножением не является полем (не выполняется аксиома (M4)).

Определение 1.2. *Кольцом* называется любое множество A с операциями сложения и умножения, для которого выполнены аксиомы (A1)–(A4) и (AM). Кольцо A называется *коммутативным*, если в нем выполнена аксиома (M1), и *ассоциативным*, если в нем выполнена аксиома (M2). Если в кольце A есть единица, то оно так и называется: *кольцо с единицей*.

В этой и следующей лекциях слово «кольцо» будет означать коммутативное ассоциативное кольцо с единицей.

Следствия аксиом

Единственность нуля и единицы

Предположим, что в кольце A найдутся два нуля: 0 и $0'$. Тогда $0 = 0 + 0' = 0'$, т. е. $0 = 0'$.

Аналогично, в любом кольце есть только одна единица.

Единственность обратных элементов

Отметим, что в аксиоме (A4) мы могли бы не требовать единственности противоположного элемента. Она следует из остальных аксиом. Действительно, предположим, что $a + b = 0$ и $a + b' = 0$. Тогда

$$b' = b' + 0 = b' + (a + b) = (b' + a) + b = 0 + b = b$$

Какие аксиомы мы использовали?

Аналогично проверяется единственность обратного элемента в поле.

Следующие четыре свойства докажите сами.

Вычитание

Для любых двух элементов a и b кольца A уравнение

$$x + b = a$$

имеет единственное решение. Это решение обозначается $a - b$.

Деление

Для любых элементов a и $b \neq 0$ поля $\Bbbk$ уравнение

$$bx = a$$

имеет единственное решение. Это решение обозначается a/b.

Умножение на нуль

Для любого элемента a кольца A выполнено равенство

$$0 \cdot a = 0.$$

Умножение на «минус единицу»

Для любого элемента a кольца A выполнено равенство

$$(-1) \cdot a = -a.$$

«Целые» числа как элементы кольца

Обозначим нуль и единицу кольца A через $\overline{0}$ и $\overline{1}$, чтобы отличать от 0 и 1 в кольце целых чисел $\mathbb{Z}$. Положим $\overline{2} = \overline{1} + \overline{1}$, $\overline{3} = \overline{2} + \overline{1}$, и т. д. Положим также $\overline{-n} = -\overline{n}$.

Упражнение 1.3. *Доказать, что для любых $m, n \in \mathbb{Z}$ выполнены равенства*

$$\overline{m+n} = \overline{m} + \overline{n} \quad \text{и} \quad \overline{m \cdot n} = \overline{m} \cdot \overline{n},$$

а для любых $n \in \mathbb{N}$, $a \in A$

$$\overline{n}a = \underbrace{a + a + \cdots + a}_{n \text{ раз}}.$$

Отметим, что из $m \neq n$ в $\mathbb{Z}$ вовсе не обязательно следует, что $\overline{m} \neq \overline{n}$ в A.

Определение 1.4. *Характеристикой* $\operatorname{char} \Bbbk$ поля $\Bbbk$ называется наименьшее натуральное число n, для которого сумма n единиц равна 0. Если такого n не существует, то считают $\operatorname{char} \Bbbk = 0$.

Упражнение 1.5. *Доказать, что для любого поля $\Bbbk$ если $\operatorname{char} \Bbbk = p \neq 0$, то p — простое число.*

Упражнение 1.6. *Доказать, что в поле $\Bbbk$ характеристики 0 можно определить элементы $\overline{r}$ для всех $r \in \mathbb{Q}$ так, чтобы для целых r это определение совпадало с приведенным выше и для любых $r, s \in \mathbb{Q}$ были выполнены равенства*

$$\overline{r+s} = \overline{r} + \overline{s} \quad \text{и} \quad \overline{r \cdot s} = \overline{r} \cdot \overline{s}.$$

Доказать, что в этом случае $\overline{r} \neq \overline{s}$ при $r \neq s$, то есть мы можем считать поле $\mathbb{Q}$ вложенным в поле $\Bbbk$.

В дальнейшем мы будем писать n вместо $\overline{n}$; из контекста будет понятно, что имеется в виду: целое число n или соответствующий элемент кольца.

Бином Ньютона

Исходя из аксиом кольца, легко доказать все формулы сокращенного умножения, известные вам по школе. Например, для любых двух элементов a и b кольца A

$$(a+b)^2 = (a+b)(a+b) = (a+b)a + (a+b)b = aa + ba + ab + bb = a^2 + 2ab + b^2,$$

где мы использовали стандартное обозначение

$$a^n = \underbrace{a \cdot a \cdot \cdots \cdot a}_{n \text{ раз}}$$

для любых $n \in \mathbb{N}$, $a \in A$.

Аналогично, в любом кольце

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k},$$

где *биномиальный коэффициент* $\binom{n}{k}$ равен числу k-элементных подмножеств n-элементного множества (это число еще называется числом сочетаний из n по k). Действительно, каждому k-элементному подмножеству множества $\{1,\ldots,n\}$ отвечает моном, получившийся при раскрытии скобок в

$$\underbrace{(a+b)\cdot\ldots\cdot(a+b)}_{n\text{ раз}},$$

у которого на местах, отвечающих элементам этого подмножества, стоит a, а на остальных местах стоит b.

Чтобы посчитать $\binom{n}{k}$, вспомним, как вычисляется число перестановок множества $\{1,\ldots,n\}$ — но обозначается $n!$. Первый элемент перестановки можно выбрать n способами, второй, если первый уже выбран, можно выбрать $n-1$ способом, и т. д. Отсюда $n! = n\cdot(n-1)\cdot\ldots\cdot 2\cdot 1$.

Посчитаем теперь число k-элементных последовательностей из неповторяющихся элементов множества $\{1,\ldots,n\}$. С одной стороны, оно равно $n\cdot(n-1)\cdot\ldots\cdot(n-k+1)$. С другой стороны, поскольку k-элементное подмножество мы можем выбрать $\binom{n}{k}$ способами, а затем переставить $k!$ способами, то

$$n\cdot(n-1)\cdot\ldots\cdot(n-k+1) = k!\binom{n}{k}.$$

Поэтому

$$\binom{n}{k} = \frac{n\cdot(n-1)\cdot\ldots\cdot(n-k+1)}{k!}.$$

Примеры колец и полей

Пример 1.7. Построим «минимальный» пример поля. Так как в любом поле должны быть нуль и единица, не равные между собой, то поле не может иметь менее двух элементов. Попробуем обойтись только этими двумя. Положим $\mathbb{F}_2 = \{0,1\}$, где $0+0=0$, $0+1=1$, $1+0=1$, $1+1=0$; $0\cdot 0=0$, $0\cdot 1=0$, $1\cdot 0=0$, $1\cdot 1=1$.

Упражнение 1.8. *Проверить, что* $\mathbb{F}_2$ *является полем.*

Пример 1.9. Обозначим через $\mathbb{Z}\left[\sqrt{2}\right]$ следующее подмножество множества вещественных чисел: $\mathbb{Z}\left[\sqrt{2}\right] = \{m+n\sqrt{2} \mid m,n\in\mathbb{Z}\}$.

Заметим, что любой элемент из $\mathbb{Z}\left[\sqrt{2}\right]$ однозначно определяется парой целых чисел m и n. Действительно, пусть $m+n\sqrt{2} = m'+n'\sqrt{2}$, тогда $(m-m') = (n-n')\sqrt{2}$. В силу иррациональности $\sqrt{2}$ это возможно лишь при $n=n'$, $m=m'$.

Сумма и произведение элементов $\mathbb{Z}\left[\sqrt{2}\right]$ снова лежит в $\mathbb{Z}\left[\sqrt{2}\right]$, там же лежат 0, 1 и элементы, противоположные к элементам $\mathbb{Z}\left[\sqrt{2}\right]$. Аксиомы коммутативности и ассоциативности сложения и умножения в $\mathbb{Z}\left[\sqrt{2}\right]$ следуют из того, что они выполнены в $\mathbb{R}$, то же относится к аксиоме дистрибутивности. Поэтому $\mathbb{Z}\left[\sqrt{2}\right]$ является кольцом.

Пример 1.10. Положим $\mathbb{Q}\left[\sqrt{2}\right] = \{a+b\sqrt{2} \mid a,b\in\mathbb{Q}\}$. Как и в предыдущем примере, это кольцо. Более того, это поле. Действительно,

$$\begin{aligned}\frac{1}{a+b\sqrt{2}} &= \frac{a-b\sqrt{2}}{(a+b\sqrt{2})(a-b\sqrt{2})} = \\ &= \frac{a-b\sqrt{2}}{a^2-2b^2} = \frac{a}{a^2-2b^2} + \frac{-b}{a^2-2b^2}\sqrt{2} \in \mathbb{Q}\left[\sqrt{2}\right]\end{aligned}$$

Заметим, что при рациональных a и b число $a^2-2b^2 \neq 0$.

Комплексные числа

Конструкция поля комплексных чисел $\mathbb{C}$ из поля вещественных чисел $\mathbb{R}$ очень напоминает конструкцию поля $\mathbb{Q}\left[\sqrt{2}\right]$ из поля $\mathbb{Q}$. Как и там, мы присоединяем к исходному полю корень квадратного уравнения, не имеющего в этом поле решений. Так что мы можем написать $\mathbb{C} = \mathbb{R}\left[\sqrt{-1}\right]$. Однако, есть и существенное отличие. Поле $\mathbb{Q}\left[\sqrt{2}\right]$ мы строили как подмножество $\mathbb{R}$, тем самым мы могли использовать тот факт, что $\mathbb{R}$ является полем. Для $\mathbb{C}$ же нам нужна явная конструкция, и мы должны проверить все аксиомы поля.

Определение 1.11. *Поле комплексных чисел* $\mathbb{C}$ есть множество пар вещественных чисел $\{(a,b) \mid a,b \in \mathbb{R}\}$ с операциями сложения

$$(a,b)+(c,d) = (a+c, b+d)$$

и умножения

$$(a,b)\cdot(c,d) = (ac-bd, ad+bc).$$

Упражнение 1.12. *Проверить, что* $\mathbb{C}$ *— поле.*

Мы можем определить операцию умножения вещественного числа x на комплексное число $z = (a,b)$, полагая $xz = (xa, xb)$. Отождествим каждое вещественное число x с комплексным числом $(x,0)$. Легко видеть, что это отождествление согласовано с операциями сложения и умножения. Обозначим пару $(0,1)$ через i. Тогда каждое комплексное число имеет вид $a+bi$, а при вычислениях следует рассматривать i как алгебраический символ, а затем полагать $i^2 = -1$ (Проверьте это!). Число a называется вещественной частью комплексного числа $z = a+bi$, а число b — его мнимой частью (обозначения: $a = \operatorname{Re} z$, $b = \operatorname{Im} z$). Комплексно-сопряженным к числу $z = a+bi$ называется число $\overline{z} = a - bi$; комплексное сопряжение «уважает» операции сложения и умножения: $\overline{wz} = \overline{w}\cdot\overline{z}$, $\overline{w+z} = \overline{w}+\overline{z}$.

Если рассматривать пару вещественных чисел (a,b) как декартовы координаты вектора на евклидовой плоскости, то мы получаем *геометрическую интерпретацию* поля комплексных чисел. Длина $\sqrt{a^2+b^2}$ вектора (a,b) называется *модулем* комплексного числа $z = a+bi$ и обозначается $|z|$, а угол, отсчитанный против часовой стрелки от вектора $(1,0)$ до вектора (a,b), называется *аргументом* z и обозначается $\operatorname{Arg}(z)$ (угол измеряется в радианах). Аргумент комплексного числа определен не однозначно, а с точностью до прибавления целого кратного 2π.

Отметим важную формулу $z\overline{z} = |z|^2$.

Модуль и аргумент хорошо ведут себя при перемножении комплексных чисел:

$$\begin{aligned} |wz| &= |w|\cdot|z|, \\ \operatorname{Arg}(wz) &= \operatorname{Arg}(w)+\operatorname{Arg}(z). \end{aligned} \tag{1}$$

Это легко получить, используя *тригонометрическую форму* комплексного числа:

$$z = r(\cos\varphi + i\sin\varphi),$$

где $r = |z|$, а $\varphi = \operatorname{Arg}(z)$. Действительно,

$$\begin{aligned} &r_1(\cos\varphi_1 + i\sin\varphi_1)\cdot r_2(\cos\varphi_2 + i\sin\varphi_2) = \\ &\qquad = r_1r_2((\cos\varphi_1\cos\varphi_2 - \sin\varphi_1\sin\varphi_2) + i(\cos\varphi_1\sin\varphi_2 + \sin\varphi_1\cos\varphi_2)) = \\ &\qquad\qquad = r_1r_2(\cos(\varphi_1+\varphi_2) + i\sin(\varphi_1+\varphi_2)). \end{aligned}$$

Часто вместо тригонометрической используется *показательная форма* комплексного числа: $z = re^{i\varphi}$, где $r = |z|$, а $\varphi = \operatorname{Arg}(z)$. Я надеюсь, что (довольно мистическое) равенство $e^{i\varphi} = \cos\varphi + i\sin\varphi$ будет вскоре доказано в курсе математического анализа. Пока его можно воспринимать как обозначение (мотивированное равенством $(\cos\varphi_1 + i\sin\varphi_1)\cdot(\cos\varphi_2 + i\sin\varphi_2) = \cos(\varphi_1+\varphi_2) + i\sin(\varphi_1+\varphi_2)$).

Повторно применяя (1), мы получаем *формулу Муавра*

$$\cos n\varphi + i\sin n\varphi = (\cos\varphi + i\sin\varphi)^n.$$

Пример 1.13. Вычислим, используя формулу Муавра, сумму

$$c_n = \cos x + \cos 2x + \dots + \cos nx.$$

Положим $z = \cos x + i\sin x$. По формуле Муавра, $\cos kx = \operatorname{Re} z^k$. Отсюда, при $z \neq 1$, т.е. при $\cos x \neq 1$,

$$c_n = \operatorname{Re}(z + z^2 + \dots + z^n) = \operatorname{Re}\frac{z^{n+1}-z}{z-1} = \frac{\operatorname{Re}\left((\overline{z}-1)(z^{n+1}-z)\right)}{|z-1|^2} =$$
$$= \frac{\operatorname{Re}\left(z^n - z^{n+1} - 1 + z\right)}{2(1-\cos x)} = \frac{(\cos nx - \cos(n+1)x) - (1-\cos x)}{2(1-\cos x)} =$$
$$= \frac{1}{2}\left(\frac{\sin\frac{2n+1}{2}x}{\sin\frac{x}{2}} - 1\right).$$

Многочлены

Многочлены от переменной x над кольцом A определяются как выражения вида $f(x) = a_0 + a_1x + \dots + a_nx^n$, где $a_0, \dots a_n \in A$. При этом мы будем считать, что, не меняя многочлена, к нему можно дописать сколько угодно нулей:

$$a_0 + a_1x + \dots + a_nx^n = a_0 + a_1x + \dots + a_nx^n + 0x^{n+1} + \dots + 0x^{n+k}.$$

Многочлен, у которого все коэффициенты нули, называется нулевым многочленом. Номер последнего ненулевого коэффициента многочлена f называется его степенью и обозначается $\deg f$. Степень нулевого многочлена считают равной $-\infty$.

Суммой двух многочленов $f(x) = a_0 + a_1x + \dots + a_kx^k$ и $g(x) = b_0 + b_1x + \dots + b_lx^l$ будем, по определению, считать многочлен

$$(a_0+b_0) + (a_1+b_1)x + \dots + (a_m+b_m)x^m,$$

где $m = \max(k,l)$ и $a_i = 0$, $b_j = 0$ при $i > k$, $j > l$.

Произведением тех же многочленов называется многочлен $h(x) = c_0 + c_1x + \dots + c_nx^n$, где

$$c_i = \sum_{j=0}^{i} a_j b_{i-j}$$

и $n = k + l$.

Упражнение 1.14. *Проверить, что многочлены над коммутативным кольцом A с введенными выше операциями сложения и умножения образуют коммутативное кольцо.*

Кольцо многочленов от переменной x над коммутативным кольцом A обозначется через $A[x]$.

Особенно хорошими свойствами обладает кольцо многочленов над полем. Например, выполнено следующее

Утверждение 1.15 (Деление многочленов с остатком). *Пусть $\Bbbk$ — поле. Для любых многочленов $f, g \in \Bbbk[x]$, $g \neq 0$, найдутся такие $q, r \in \Bbbk[x]$, что $f = qg + r$, причем $\deg r < \deg g$.*

Доказательство. Если $\deg f < \deg g$, то $q = 0$, $r = f$ удовлетворяют условиям утверждения.

Пусть $\deg f \geqslant \deg g$. Положим $n = \deg g$, $m = \deg f$, a_m и b_n — старшие коэффициенты соответственно f и g. Воспользуемся индукцией по $k = m - n$.

Пусть $k = 0$. Тогда $q = a_m/b_n$ и $r = f - qg$ удовлетворяют условиям утверждения.

Пусть $k_0 > 0$ и для всех $k < k_0$ утверждение доказано. Докажем его для $k = k_0$.

Положим $\tilde{f} = f - (a_m/b_n)x^k g$. Поскольку $\deg \tilde{f} < \deg f$, то найдутся $\tilde{q}$ и r такие, что $\tilde{f} = \tilde{q}g + r$ и $\deg r < \deg g$. Положим $q = \tilde{q} + (a_m/b_n)x^k$. Тогда $f = qg + r$. □

Упражнение 1.16. *Пусть* $\Bbbk$ *— поле. Доказать, что для любых многочленов* $f, g \in \Bbbk[x]$ *выполнено равенство* $\deg fg = \deg f + \deg g$.

Для любого многочлена $f(x) = a_0 + a_1 x + \cdots + a_k x^k \in A[x]$ и любого $\alpha \in A$ определен результат подстановки α в многочлен f:

$$f(\alpha) = a_0 + a_1\alpha + \cdots + a_k\alpha^k \in A.$$

Очень важным (хотя и очевидным) свойством подстановки является ее согласованность с операциями сложения и умножения: $(f + g)(\alpha) = f(\alpha) + g(\alpha)$, $(fg)(\alpha) = f(\alpha)g(\alpha)$.

Пусть f — многочлен над полем $\Bbbk$. Элемент $\alpha \in \Bbbk$ называется корнем многочлена f, если $f(\alpha) = 0$.

Теорема 1.17 (Теорема Безу). *Пусть* α *— корень мнгочлена* $f(x)$ *над полем* $\Bbbk$. *Тогда* $f(x)$ *делится на многочлен* $x - \alpha$, *т. е. существует такой многочлен* $h(x) \in \Bbbk[x]$, *что* $f(x) = (x - \alpha)h(x)$.

Доказательство. Поделим с остатком $f(x)$ на $x - \alpha$:

$$f(x) = (x - \alpha)h(x) + r(x). \tag{2}$$

Поскольку $\deg r(x) < \deg(x - \alpha) = 1$, то $r(x) = r$ — константа. Подставляя α в (2), получаем

$$0 = f(\alpha) = (\alpha - \alpha)h(\alpha) + r = r,$$

т. е. $f(x) = (x - \alpha)h(x)$. □

Следствие 1.18. *Число различных корней ненулевого многочлена не превосходит его степени.*

Доказательство. Воспользуемся индукцией по степени $f(x)$. У многочленов степени нуль корней, очевидно, быть не может.

Предположим, что $\deg f(x) > 0$ и для многочленов меньшей степени утверждение следствия выполнено. Пусть f имеет корень α (если f не имет корней, то и доказывать нечего). По теореме Безу найдется многочлен $h(x) \in \Bbbk[x]$ такой, что $f(x) = (x - \alpha)h(x)$. Подставляя в это равенство другие корни многочлена f, мы убеждаемся, что все они являются корнями многочлена h. Поскольку $\deg h = \deg f - 1$, то, по предположению индукции, этих корней не более чем $\deg f - 1$. Поэтому у многочлена f не более чем $\deg f$ корней (с учетом α). □

Определение 1.19. Пусть многочлен $f(x) \in \Bbbk[x]$ имеет корень α. Кратностью этого корня называется максимальное натуральное число k такое, что $f(x)$ делится на $(x - \alpha)^k$.

Определение 1.20. Поле $\Bbbk$ называется *алгебраически замкнутым*, если любой многочлен из $\Bbbk[x]$ имеет в $\Bbbk$ хотя бы один корень.

Упражнение 1.21. *Доказать, что любой многочлен над алгебраически замкнутым полем может быть представлен как произведение многочленов первой степени.*

Упражнение 1.22. *Доказать, что любой многочлен над алгебраически замкнутым полем имеет ровно столько корней (с учетом кратности), какова его степень.*

Теорема 1.23 (Основная теорема алгебры). *Поле комплексных чисел алгебраически замкнуто.*

Я не буду доказывать эту теорему. На мой взгляд, ее доказательство более уместно в курсе комплексного анализа. «Алгебраическое» доказательство см. в учебнике Кострикина, гл. 6, §3.

Еще одно доказательство формулы бинома

Определим операцию дифференцирования многочлена над произвольным полем $\Bbbk$ следующим образом: пусть $f(x) = \sum_{k=0}^{n} a_k x^k$; тогда положим по определению $f'(x) = \sum_{k=1}^{n} k a_k x^{k-1}$.

Упражнение 1.24. *Доказать, что выполнено правило Лейбница дифференцирования произведения:* $(fg)' = f'g + fg'$.

Пусть $\Bbbk$ — поле характеристики 0. Докажем, что для любого натурального n в кольце многочленов $\Bbbk[x]$ имеет место равенство

$$(1+x)^n = \sum k = 0^n \frac{n(n-1)\dots(n-k+1)}{k!} x^k. \tag{3}$$

Действительно, пусть $f(x) = (1+x)^n$. Обозначим через a_k коэффициент при x^k у этого многочлена. Продифференцируем этот многочлен k раз. Из упражнения 1.24 легко следует, что $f^{(k)}(x) = n(n-1)\dots(n-k+1)(1+x)^{n-k}$. С другой стороны, по определению

$$f^{(k)}(x) = \sum_{m=k}^{n} m(m-1)\dots(m-k+1) a_m x^{m-k}.$$

Отсюда $n(n-1)\dots(n-k+1) = f^{(k)}(0) = k! a_k$, то есть

$$a_k = \frac{n(n-1)\dots(n-k+1)}{k!}. \qquad \square$$

Отметим, что мы нашли не комбинаторное, а чисто алгебраическое доказательство формулы для числа сочетаний из n по k. При этом мы воспользовались тем, что число сочетаний из n по k является k-ым коэффициентом многочлена $(1+x)^n$, то есть $(1+x)^n$ является *производящей функцией* для чисел сочетаний. К понятию производящей функции мы вернемся на следующей лекции, когда будем обсуждать формальные степенные ряды.

Лекция 2.

На прошлой лекции мы видели, что коэффициент при t^k в разложении многочлена $(1+t)^n$ по степеням t имеет комбинаторный смысл: это число сочетаний из n по k. Иначе это говорят так: многочлен $(1+t)^n$ является *производящей функцией* для последовательности (a_k), где $a_k = \binom{n}{k}$. Последовательность (a_k) конечна, поэтому-то производящая функция и является многочленом. Однако в комбинаторике (да и в других областях математики) возникают, как правило, бесконечные последовательности. Поэтому в качестве производящих функций рассматривают

Формальные степенные ряды

Как и на прошлой лекции, слово «кольцо» будет означать коммутативное ассоциативное кольцо с единицей.

Определение 2.1. *Формальным степенным рядом* от переменной t над кольцом A называется выражение вида

$$f(t) = \sum_{k=0}^{\infty} a_k t^k,$$

где $(a_0, a_1, \dots)$ — произвольная бесконечная последовательность элементов кольца A.

Определим на множестве формальных степенных рядов операции сложения и умножения, полагая для $f(t) = \sum_{k=0}^{\infty} a_k t^k$ и $g(t) = \sum_{k=0}^{\infty} b_k t^k$

$$\begin{aligned} f(t) + g(t) &= \sum_{k=0}^{\infty} (a_k + b_k) t^k; \\ f(t) \cdot g(t) &= \sum_{k=0}^{\infty} (\sum_{j=0}^{k} a_j b_{k-j}) t^k. \end{aligned}$$

Заметим, что это определение очень напоминает определение операций в кольце многочленов. Более того, если мы рассмотрим множество формальных степенных рядов, у которых лишь конечное число коэффициентов отлично от нуля, то мы получим в точности кольцо многочленов.

Поскольку n-ый коэффициент произведения формальных степенных рядов зависит только от коэффициентов сомножителей с номерами от 0 до n (тем более это верно для суммы), то проверка аксиом кольца для множества формальных степенных рядов сводится к тем же аксиомам для многочленов. Поэтому формальные степенные ряды над A образуют кольцо. Оно обозначается $A[[t]]$.

Упражнение 2.2. *Найти произведение формальных степенных рядов*

$$(1-t)(1+t+t^2+t^3+\dots).$$

Упражнение 2.3. *Элемент кольца называется обратимым, если у него есть обратный по умножению. Доказать, что степенной ряд $f(t) = \sum_{k=0}^{\infty} a_k t^k$ обратим в $A[[t]]$ тогда и только тогда, когда a_0 обратим в A.*

Упражнение 2.4. *Пусть $f(t) = \sum_{k=0}^{\infty} a_k t^k \in \mathbb{k}[[t]]$, где $\mathbb{k}$ — поле характеристики нуль. Доказать, что степенной ряд $g(t) = \sum_{k=0}^{\infty} b_k t^k \in \mathbb{k}[[t]]$ такой, что $g^2 = f$, существует тогда и только тогда, когда уравнение $x^2 = a_0$ разрешимо в поле $\mathbb{k}$. При этом все коэффициенты формального ряда $g(t)$ однозначно определяются выбором $b_0 = \pm\sqrt{a_0}$.*

Подставлять в формальный степенной ряд $f(t) \in A[[t]]$ элемент кольца A, вообще говоря, нельзя. Однако можно подставить формальный степенной ряд $g(t) = \sum_{k=0}^{\infty} b_k t^k$, если $b_0 = 0$. Результатом подстановки явится вновь формальный степенной ряд.

Упражнение 2.5. *Выразить коэффициенты ряда* $f(g)$ *через коэффициенты рядов* f *и* g.

Упражнение 2.6. *Пусть* $\mathbb{k}$ *— поле характеристики нуль. Положим по определению*

$$\exp(t) = \sum_{k=0}^{\infty} \frac{t^k}{k!}$$

и

$$\log(1+t) = \sum_{k=1}^{\infty} (-1)^{k+1} \frac{t^k}{k}.$$

Проверить, что $\exp(\log(1+t)) = 1+t$.

Общая формула бинома Ньютона

Пусть характеристика поля $\mathbb{k}$ равна нулю. Определим для любого $\alpha \in \mathbb{k}$ и любого $k \in \mathbb{N}$ *биномиальный коэффициент*

$$\binom{\alpha}{k} = \frac{\alpha \cdot (\alpha-1) \cdot \dots \cdot (\alpha-k+1)}{k!}. \tag{4}$$

Пусть α — фиксированный элемент $\mathbb{k}$. Положим

$$(1+t)^{\alpha} = \sum_{k=0}^{\infty} \binom{\alpha}{k} t^k.$$

При натуральных α это равенство выполнено по формуле бинома Ньютона, для остальных же α это пока не более, чем обозначение. Поэтому следующее утверждение не тривиально.

Утверждение 2.7. *Для любых* $\alpha, \beta \in \mathbb{k}$ *выполнено равенство:*

$$(1+t)^{\alpha}(1+t)^{\beta} = (1+t)^{\alpha+\beta}. \tag{5}$$

Доказательство. Согласно определению умножения в кольце формальных степенных рядов равенство (5) сводится к следующему тождеству для биномиальных коэффициентов:

$$\binom{\alpha+\beta}{k} = \sum_{j=0}^{k} \binom{\alpha}{j} \binom{\beta}{k-j} \tag{6}$$

Для натуральных α и β равенство (5), а, следовательно, и (6), выполнено в силу обычной формулы бинома.

Отметим, что определение биномиального коэффициента по формуле (4) имеет смысл и для любого многочлена $\alpha \in \mathbb{k}[x]$; в этом случае $\binom{\alpha}{k}$ является многочленом от x.

Пусть n — некоторое натуральное число. Поскольку поле $\mathbb{k}$ имеет характеристику нуль, то мы можем считать множество натуральных чисел вложенным в $\mathbb{k}$. Рассмотрим многочлен

$$F(x) = \binom{x+n}{k} - \sum_{j=0}^{k} \binom{x}{j} \binom{n}{k-j}$$

как многочлен над $\mathbb{k}$.

Пусть $\beta = n$, а α — любой элемент поля $\mathbb{k}$. В этом случае разность между левой и правой частью (6) равна $F(\alpha)$. Поскольку (6) выполняется при натуральных α и β, то $F(x)$ обращается в нуль при подстановке в него любого натурального числа. Поэтому он имеет бесконечно много корней в поле $\Bbbk$. Следовательно, он равен нулю, и (6) выполняется при натуральных значениях β и любых α.

Зафиксируем теперь произвольное $\alpha \in \Bbbk$ и рассмотрим многочлен

$$G(x) = \binom{\alpha + x}{k} - \sum_{j=0}^{k} \binom{\alpha}{j} \binom{x}{k-j}.$$

Разность между левой и правой частью (6) равна $G(\beta)$. Поскольку, как мы только что установили, (6) выполняется при натуральных значениях β и любых α, то $G(x)$ обращается в нуль при подстановке в него любого натурального числа. Поэтому он имеет бесконечно много корней в поле $\Bbbk$. Следовательно, он равен нулю, и (6) выполняется при любых α и β. $\square$

Примеры.

1)

$$(1+t)^{-1} = \sum_{k=0}^{\infty} \binom{-1}{k} t^k = \sum_{k=0}^{\infty} (-1)^k t^k.$$

Действительно,

$$\binom{-1}{k} = \frac{(-1)\cdot(-2)\cdot\dots\cdot(-k)}{k!} = (-1)^k.$$

Заметим, что мы ликвидировали некоторую двусмысленность в обозначении $(1+t)^{-1}$, доказав равенство (5). Действительно, в частном случае $\alpha = 1$, $\beta = -1$ из (5) следует, что формальный степенной ряд $(1+t)^{-1} = \sum_{k=0}^{\infty} \binom{-1}{k} t^k$ является обратным по умножению к $(1+t)$. Впрочем, это легко проверить и непосредственно.

2)

$$(1+t)^{-m} = \sum_{k=0}^{\infty} \binom{-m}{k} t^k = \sum_{k=0}^{\infty} \binom{k+m-1}{k} (-1)^k t^k.$$

Действительно,

$$\begin{aligned}\binom{-m}{k} &= \frac{(-m)\cdot(-m-1)\cdot\dots\cdot(-m-k+1)}{k!} = \\ &= (-1)^k \frac{(k+m-1)\cdot(k+m-2)\cdot\dots\cdot(m+1)\cdot m}{k!} = \\ &= (-1)^k \binom{k+m-1}{k}.\end{aligned}$$

Пусть m — натуральное число. Из доказанного нами утверждения следует, что $\left((1+t)^{-1}\right)^m = (1+t)^{-m}$. Подставляя в это тождество $-t$ вместо t, получаем

$$\left(\sum_{k=0}^{\infty} t^k\right)^m = \sum_{k=0}^{\infty} \binom{k+m-1}{k} t^k. \tag{7}$$

Если раскрыть левую часть (7) таким же образом, как мы это делали при доказательстве обычной формулы бинома, то мы получим следующее комбинаторное описание коэффициента при t^k: это число различных представлений числа k в виде суммы m неотрицательных целых чисел (порядок слагаемых существен). Это число иногда называется *числом сочетаний с повторениями из m по k* и обозначается $\left(\binom{m}{k}\right)$. Таким образом, $(1-t)^{-m}$ является производящей функцией для числа сочетаний с повторениями. Поэтому формула (7) дает нам следующее комбинаторное тождество:

$$\left(\binom{m}{k}\right) = \binom{k+m-1}{k} = \binom{k+m-1}{m-1},$$

то есть число сочетаний с повторениями из m по k равно числу сочетаний из $k+m-1$ по k. Чисто комбинаторное доказательство этого тождества попробуйте найти самостоятельно.

Разберем еще несколько примеров работы с производящими функциями.

Задача о числе счастливых билетов

Задача очень известная: найти число последовательностей из шести цифр, для которых сумма трех первых цифр равна сумме трех последних.

Напишем сперва производящую функцию для числа последовательностей из n цифр с суммой k. Для $n=1$ она равна

$$f_1(t) = 1 + t + t^2 + \cdots + t^9.$$

Для $n=2$ —

$$f_2(t) = (1 + t + t^2 + \cdots + t^9) \cdot (1 + t + t^2 + \cdots + t^9) = f_1(t)^2.$$

Действительно, коэффициент при t^k в $f_2(t)$ равен числу способов выбрать слагаемое t^{k_1} из первой скобки и слагаемое t^{k_2} из второй скобки так, чтобы $k_1 + k_2 = k$, то есть как раз числу последовательностей из 2 цифр с суммой k. Аналогично,

$$f_3(t) = (1 + t + t^2 + \cdots + t^9) \cdot (1 + t + t^2 + \cdots + t^9) \cdot (1 + t + t^2 + \cdots + t^9) = f_1(t)^3$$

— это производящая функция для числа последовательностей из 3 цифр с суммой k, и так далее. Все эти производящие функции — многочлены из $\mathbb{Q}[t]$.

Напишем теперь производящую функцию для числа последовательностей из 6 цифр, для которых *разность* суммы первых трех и суммы последних трех равна k. Она равна

$$F(t) = (1 + t + t^2 + \cdots + t^9) \cdot (1 + t + t^2 + \cdots + t^9) \cdot (1 + t + t^2 + \cdots + t^9) \cdot$$
$$\cdot (1 + t^{-1} + t^{-2} + \cdots + t^{-9}) \cdot (1 + t^{-1} + t^{-2} + \cdots + t^{-9}) \cdot (1 + t^{-1} + t^{-2} + \cdots + t^{-9}) = f_3(t) \cdot f_3(t^{-1}).$$

Это уже не многочлен, а *многочлен Лорана*.

Определение 2.8. *Многочленом Лорана* над полем $\Bbbk$ называется выражение вида $f(x) = a_m x^m + a_{m+1} x^{m+1} + \cdots + a_n x^n$, где $m, n \in \mathbb{Z}$ и все $a_k \in \Bbbk$. При этом мы будем считать, что, не меняя многочлена Лорана, к нему можно дописать сколько угодно нулей с любой стороны. Сумма и произведение многочленов Лорана определяются очевидным образом.

Упражнение 2.9. *Доказать, что множество $\Bbbk[t, t^{-1}]$ многочленов Лорана над полем $\Bbbk$ является коммутативным ассоциативным кольцом с единицей.*

Определение 2.10. *Формальным рядом Лорана* над полем $\Bbbk$ называется выражение вида $f(x) = \sum\limits_{k=m}^{\infty} a_k x^k$, где $m \in \mathbb{Z}$ и все $a_k \in \Bbbk$. При этом мы будем считать, что, не меняя ряда Лорана, к нему можно дописать слева сколько угодно нулей. Сумма и произведение рядов Лорана определяются теми же формулами, что и для многочленов Лорана.

Упражнение 2.11. *Доказать, что множество $\Bbbk[[t, t^{-1}]$ формальных рядов Лорана над полем $\Bbbk$ является полем.*

Формальные ряды Лорана нам пока не понадобятся, да и от многочленов Лорана мы сейчас избавимся.

Ясно, что решением задачи о счастливых билетах является коэффициент при t^0 в многочлене Лорана $F(t)$. Мы имеем

$$F(t) = t^{-27} \cdot (1 + t + t^2 + \cdots + t^9)^6 = t^{-27} \cdot f_6(t).$$

Таким образом, нам нужен коэффициент при t^{27} у многочлена $f_6(t) = f_1(t)^6$. Найдем его.

Будем рассматривать многочлены от t как формальные степенные ряды. Мы имеем

$$f_1(t) = \frac{1-t^{10}}{1-t}.$$

Отсюда $f_6(t) = (1-t^{10})^6(1-t)^{-6}$. Разлагая $(1-t^{10})^6$ и $(1-t)^{-6}$ по формуле бинома Ньютона, получаем

$$f_6(t) = \left(\sum_{k=0}^{6}(-1)^k\binom{6}{k}t^{10k}\right)\cdot\left(\sum_{l=0}^{\infty}\binom{5+l}{5}t^l\right).$$

Поэтому коэффициент при t^{27} равен

$$\binom{6}{0}\binom{32}{5} - \binom{6}{1}\binom{22}{5} + \binom{6}{2}\binom{12}{5}.$$

Это и есть ответ к задаче о счастливых билетах.

Этот ответ можно получить и без производящих функций. Я коротко опишу соответствующее рассуждение.

Прежде всего, заменяя три последние цифры на их дополнения до 9, мы видим, что счастливых билетов столько же, сколько билетов с суммой цифр 27. Последовательностей из шести неотрицательных целых чисел с суммой 27 всего существует $\binom{32}{5}$. Из них у $\binom{22}{5}$ на i-ом месте стоит число, большее 9 ($i = 1, \dots, 6$); и у $\binom{12}{5}$ на i-ом и j-ом местах стоят числа, большие 9 ($1 \leqslant i < j \leqslant 6$). Остается воспользоваться принципом включения-исключения.

Теорема 2.12 (принцип включения-исключения). *Пусть элементы множества I могут обладать свойствами $c_1, \dots, c_r$. Обозначим число элементов во множестве I через N, число тех из них, которые обладают свойством c_i, через $N(i)$, число тех, которые обладают свойствами c_i и c_j при $i \neq j$, через $N(i,j)$, и так далее. Тогда число элементов множества I, не обладающих ни одним из свойств $c_1, \dots, c_r$, равно*

$$N - \sum_{i=1}^{r} N(i) + \sum_{1\leqslant i<j\leqslant r} N(i,j) - \dots + (-1)^r N(1,2,\dots,r). \tag{8}$$

Доказать принцип включения-исключения можно, например, с помощью индукции по r. Другой способ основан на том, что каждый элемент множества I, обладающий ровно l из свойств $c_1, \dots, c_r$, в знакопеременной сумме (8) учитывается $\binom{l}{0} - \binom{l}{1} + \binom{l}{2} - \dots + (-1)^l\binom{l}{l}$ раз. Это число равно 1 при $l = 0$ и 0 при $l > 0$.

Вернемся к задаче о счастливых билетах. В нашем случае множество I — это множество всех последовательностей из шести неотрицательных целых чисел с суммой 27, а свойство c_i, где $i = 1, \dots, 6$, состоит в том, что на i-ом месте в последовательности стоит число, большее 9. Применяя принцип включения-исключения, получаем уже известный нам ответ.

Рекуррентные формулы и производящие функции

Пусть все члены последовательности $(a_k)_{k=0,1,\dots}$, начиная с некоторого номера m, выражаются однозначно через предыдущие члены этой последовательности, то есть пусть имеет место формула типа

$$a_k = F(k; a_1, \dots, a_{k-1}) \qquad \text{при } k \geqslant m. \tag{9}$$

Такая формула называется *рекуррентной формулой* для последовательности (a_k). Ясно, что последовательность (a_k) определяется формулой (9) и членами $a_0, a_1, \dots, a_{m-1}$ однозначно. Во многих случаях с помощью рекуррентной формулы удается найти производящую функцию $A(t) = \sum\limits_{k=0}^{\infty} a_k t^k$ для последовательности (a_k).

Пример 2.13 (Числа Фибоначчи). Последовательность Фибоначчи (f_k) определяется соотношениями $f_0 = 0$, $f_1 = 1$, $f_k = f_{k-1} + f_{k-2}$ при $k > 1$. Положим

$$F(t) = \sum_{k=0}^{\infty} f_k t^k.$$

Подставляя 0 вместо f_0, 1 вместо f_1 и $f_{k-1} + f_{k-2}$ вместо f_k для всех $k > 1$, получаем

$$F(t) = t + \sum_{k=2}^{\infty} (f_{k-1} + f_{k-2}) t^k = t + tF(t) + t^2 F(t).$$

Отсюда $F(t) = t/(1-t-t^2)$ (мы воспользовались тем, что $1-t-t^2$ обратим в кольце формальных степенных рядов $\mathbb{Q}[[t]]$).

Пример 2.14 (Числа Каталана). *Правильной скобочной структурой длины* k называется любая такая последовательность из k открывающих скобок и k закрывающих скобок, что в любом ее начальном отрезке открывающих скобок не меньше, чем закрывающих. Например, $(()())(())()$ — правильная скобочная структура длины 6. *Числом Каталана* c_k называется число правильных скобочных структур длины k. Ясно, что при $k = 0$ правильная скобочная структура только одна — пустая, поэтому $c_0 = 1$.

В правильной скобочной структуре каждой открывающей скобке соответствует парная ей закрывающая скобка, определяемая тем, что внутри этой пары скобок вновь лежит правильная скобочная структура. (Докажите, что таким образом скобки действительно однозначно разбиваются на пары!)

Найдем в правильной скобочной структуре длины $k > 0$ закрывающую скобку, парную первой открывающей скобке. Внутри этой пары скобок лежит правильная скобочная структура, и после этих скобок идет правильная скобочная структура, причем сумма их длин равна $k-1$. С другой стороны, каждой паре правильных скобочных структур с суммой длин $k-1$ можно поставить в соответствие правильную скобочную структуру длины k, заключив первую структуру в скобки и приписав к ней справа вторую. Очевидно, что построенное соответствие взаимно однозначно, поэтому при $k \geqslant 1$ имеет место рекуррентная формула

$$c_k = \sum_{i=0}^{k-1} c_i c_{k-1-i}.$$

Положим

$$C(t) = \sum_{k=0}^{\infty} c_k t^k.$$

Из рекуррентного соотношения и начального условия $c_0 = 1$ получаем уравнение на $C(t)$

$$C(t) = 1 + tC(t)^2.$$

Решим это уравнение в поле формальных рядов Лорана $\mathbb{Q}[[t, t^{-1}]$.

$$C(t) = \frac{1 \pm \sqrt{1-4t}}{2t}.$$

По условию, все коэффициенты ряда C_t с отрицательными номерами должны равняться нулю, поэтому

$$C(t) = \frac{1 - \sqrt{1-4t}}{2t}.$$

Раскрывая квадратный корень из $1-4t$ по формуле бинома, получаем формулу для чисел Каталана

$$c_k = \frac{(1/2)(1/2)(3/2)\ldots((2k-1)/2)4^{n+1}}{2(n+1)!} = \frac{(2n)!}{n!(n+1)!}.$$

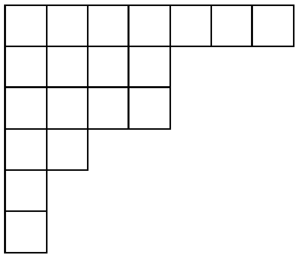
Разбиения

Разбиением неотрицательного целого числа k называется представление его в виде суммы натуральных слагаемых, порядок которых считается неважным. Для определенности будем записывать слагаемые в невозрастающем порядке. Вот, например, все разбиения числа 4:

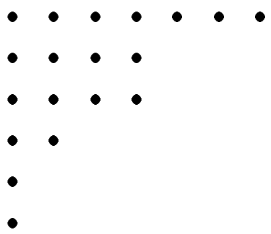
$$4;\quad 3+1;\quad 2+2;\quad 2+1+1;\quad 1+1+1+1.$$

Единственным разбиением числа 0 является его разбиение на пустое множество слагаемых.

Разбиение удобно представлять геометрически с помощью диаграммы Юнга



или диаграммы Ферре



Здесь изображено разбиение $7+4+4+2+1+1$ числа 19.

Обозначим через p_k число разбиений числа k. Положим

$$P(t)=\sum_{k=0}^{\infty} p_k t^k.$$

Докажем, что

$$P(t)=(1+t+t^2+t^3+\ldots)\cdot(1+t^2+t^4+t^6+\ldots)\cdot \\ \cdot(1+t^3+t^6+t^9+\ldots)\cdot\cdots=\prod_{m=1}^{\infty}\left(\sum_{k=0}^{\infty} t^{km}\right). \quad (10)$$

Прежде всего надо придать смысл бесконечному произведению. Заметим, что для любой бесконечной последовательности формальных степенных рядов $(f_m(t))_{m\geqslant 1}$ коэффициент при t^k в произведении

$$\prod_{m=1}^{n}(1+t^m f_m(t))$$

стабилизируется по n, то есть не зависит от n при $n\geqslant k$. Формальный степенной ряд с этими «стабильными» коэффициентами и называется бесконечным произведением

$$\prod_{m=1}^{\infty}(1+t^m f_k(t)).$$

Рассмотрим теперь коэффициент при t^k у бесконечного произведения в (10). Он равен числу способов выбрать слагаемое t^{l_1} из первой скобки, слагаемое t^{2l_2} из второй скобки, слагаемое t^{3l_3}

из третьей скобки, и так далее, так, чтобы $l_1 + 2l_2 + 3l_3 + \dots = k$. Каждому такому выбору соответствует разбиение

$$\dots + \underbrace{3 + \dots + 3}_{l_3} + \underbrace{2 + \dots + 2}_{l_2} + \underbrace{1 + \dots + 1}_{l_1}$$

числа k. Ясно, что это соответствие взаимно однозначно. Поэтому равенство (10) верно.

Пользуясь равенством

$$\sum_{k=0}^{\infty} t^{km} = (1 - t^m)^{-1},$$

получаем

$$P(t) = \prod_{m=1}^{\infty} (1 - t^m)^{-1}.$$

Таким образом, $P(t) = Q(t)^{-1}$, где

$$Q(t) = \prod_{m=1}^{\infty} (1 - t^m).$$

Сходным образом довольно легко написать производящие функции для разбиений с ограничениями. Например, $\prod\limits_{m=1}^{\infty} (1 + t^m)$ для разбиений на различные слагаемые, $\prod\limits_{m=1}^{\infty} (1 - t^{2m-1})^{-1}$ для разбиений на нечетные слагаемые, $\prod\limits_{m=1}^{\infty} (1 + t^{2m-1})$ для разбиений на различные нечетные слагаемые, и так далее.

Теорема 2.15 (Тождество Эйлера).

$$Q(t) = 1 + \sum_{n=1}^{\infty} (-1)^n \left(t^{(3n^2-n)/2} + t^{(3n^2+n)/2} \right).$$

Доказательство. При раскрытии скобок в произведении

$$Q(t) = \prod_{m=1}^{\infty} (1 - t^m)$$

возникают те же члены, что и в производящей функции $\prod\limits_{m=1}^{\infty} (1+t^m)$ для числа разбиений на различные слагаемые, только в коэффициент при t^k каждое разбиение k на четное число слагаемых дает вклад 1, а каждое разбиение k на нечетное число слагаемых дает вклад -1. Тождество Эйлера гласит, что эти вклады почти всегда сокращаются, то есть почти для любого k число его разбиений на нечетное число различных слагаемых равно числу его разбиений на четное число различных слагаемых. Попытаемся установить взаимно однозначное соответствие между разбиениями k на четное и нечетное число различных слагаемых.

Пусть дано разбиение k на различные слагаемые. Изобразим его диаграммой Ферре. Выделим у диаграммы нижнюю строку и «правую диагональ» (см. рисунок 1).

Пусть l — длина нижней строки, d — длина правой диагонали и n — число строк в диаграмме, то есть число слагаемых в разбиении.

Построим новую диаграмму следующим образом:

1) если $l < d = n$ или $l \leqslant d < n$, то отрежем от диаграммы нижнюю строку и приклеем справа как правую диагональ;

2) если $l - 1 > d = n$ или $l > d < n$, то отрежем у диаграммы правую диагональ и приклеем снизу как нижнюю строку;

3) если $l = d = n$ или $l - 1 = d = n$, то ничего менять не будем.

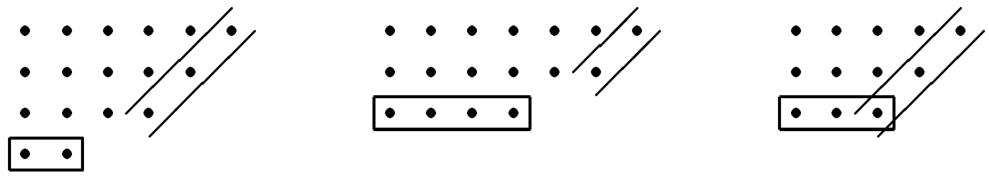


Рис. 1.

Например, первые две диаграммы на рисунке 1 получаются таким образом друг из друга, а последняя не изменяется.

Назовем неизменяющиеся диаграммы исключительными. Легко проверить, что если из диаграммы A получается диаграмма B, то из диаграммы B получается диаграмма A. Кроме того, четность числа строк у неисключительных диаграмм меняется. Поэтому вклады в $Q(t)$ для всех разбиений, отвечающих неисключительным диаграммам, сокращаются.

Для исключительных диаграмм либо $l = d = n$, тогда число точек $k = (3n^2 - n)/2$, либо $l - 1 = d = n$, тогда число точек $k = (3n^2 + n)/2$. Вклад исключительной диаграммы равен $(-1)^n$. Тождество Эйлера доказано. □

Следствие 2.16. *Для числа разбиений p_k при $k > 0$ верна следующая рекуррентная формула*

$$p_k = p_{k-1} + p_{k-2} - p_{k-5} - p_{k-7} + p_{k-12} + \dots = \sum_{n=1}^{\infty} (-1)^{n-1} (p_{k-(3n^2-n)/2} + p_{k-(3n^2+n)/2}),$$

где мы полагаем $p_m = 0$ при $m < 0$.

Доказательство. Это сразу следует из равенства $P(t)Q(t) = 1$ и из тождества Эйлера. □

Лекция 3.

На прошлых лекциях мы рассматривали алгебраические структуры, связанные с обобщением понятия числа. Каждая из этих структур (поле, кольцо) представляет из себя множество с двумя операциями (сложение и умножение), удовлетворяющими некоторым аксиомам. Для изучения таких структур естественно сначала облегчить себе задачу и изучить множества с одной операцией, также удовлетворяющей некоторым естественным аксиомам. Таким образом можно прийти к понятию *группы*.

Однако это важное понятие имеет и другой источник — *группы преобразований*. Именно их мы и будем рассматривать в первую очередь. Но начнем мы с введения (или напоминания) некоторых общих теоретико-множественных понятий.

Отображения множеств

Рассмотрим два множества M и N.

Определение 3.1. *Отображением* φ множества M во множество N

$$\varphi : M \to N \qquad (\text{или}\ \ M \xrightarrow{\varphi} N)$$

называется любое правило, сопоставляющее каждому элементу $m \in M$ некоторый единственный элемент $\varphi(m) \in N$. Этот элемент $\varphi(m)$ называется *образом* элемента m при отображении φ. Вместо $n = \varphi(m)$ пишут также

$$\varphi : m \mapsto n \qquad \text{или} \qquad m \overset{\varphi}{\mapsto} n.$$

Если S — какое-нибудь подмножество в M, то можно рассмотреть в N подмножество, состоящее из образов всех элементов из S при отображении φ. Это подмножество называется *образом* множества S при отображении φ и обозначается через $\varphi(S)$. Запишем это формулой: $\varphi(S) = \{\varphi(m) \mid m \in S\}$.

Наоборот, пусть T — какое-нибудь подмножество в N. Рассмотрим в M подмножество, состоящее из всех элементов множества M, образы которых при отображении φ лежат в T. Это подмножество называется *прообразом* множества T при отображении φ и обозначается через $\varphi^{-1}(T)$ (формальная запись: $\varphi^{-1}(T) = \{m \in M \mid \varphi(m) \in T\}$).

Мы можем, в частности, рассмотреть случай, когда T состоит из одного элемента $n \in N$. В этом случае прообраз $\varphi^{-1}(n)$ элемента n при отображении φ часто называют слоем отображения φ над точкой n.

Из определения отображения сразу следует, что каждый элемент множества M содержится ровно в одном слое отобржения φ. Иначе говоря, слои отображения φ покрывают множество M, попарно не пересекаясь.

Пример 3.2. Пусть $M = \mathbb{C}$ — множество комплексных чисел, $N = \mathbb{R}$, а отображение $\varphi : M \to M$ задается формулой $\varphi(z) = |z|$. Тогда $\varphi(M) = \mathbb{R}_+$ — множество всех неотрицательных вещественных чисел, а слой над числом $r \in N$ пуст, если $r < 0$, и является окружностью с центром в нуле и радиусом r, если $r \geqslant 0$.

Пример 3.3. Пусть M — произвольное множество. Отображение $\varphi : M \to M$, заданное формулой $\varphi(m) = m$, называется *тождественным отображением* множества M в себя, и обозначается через id_M, 1_M или e_M.

В зависимости от свойств слоев принято выделять несколько специальных типов отображений.

Определение 3.4. Отображение $\varphi : M \to N$ называется *сюръективным* (или *сюръекцией*), *инъективным* (или *инъекцией*), *биективным* (или *биекцией*), если, соответственно, каждый слой не пуст, каждый слой состоит не более, чем из одного элемента, каждый слой состоит ровно из одного элемента.

Пример 3.5. Пусть $M = N = \mathbb{R}$, а отображение $\varphi : M \to M$ задается функцией $y = x^2$. Тогда φ не является ни сюръекцией, ни инъекцией (и, значит, ни биекцией). Если рассмотреть функцию $y = \begin{cases} \ln|x|, & x \neq 0, \\ 0, & x = 0, \end{cases}$ то мы получим пример сюръекции, не являющейся инъекцией, а если взять функцию $y = e^x$, то, наоборот, пример инъекции, не являющейся сюръекцией. Функция $y = x^3$ определяет биекцию.

Отметим, что тождественное отображение всегда является биекцией.

Предположим, что заданы три множества M, N и K и два отображения $\varphi : M \to N$ и $\psi : N \to K$. Тогда можно определить отображение $\chi : M \to K$ с помощью формулы $\chi(m) = \psi(\varphi(m))$.

Таким образом, χ является результатом последовательного выполнения отображений φ и ψ. Определенное таким образом отображение χ называется композицией отображений φ и ψ и обозначается через $\psi \circ \varphi$.

Непосредственно проверяется, что для любых четырех множеств M, N, K и L и любых трех отображений $\varphi : M \to N$, $\psi : N \to K$ и $\theta : K \to L$ выполнено равенство:

$$\theta \circ (\psi \circ \varphi) = (\theta \circ \psi) \circ \varphi,$$

то есть операция композиции *ассоциативна.*

Пример 3.6. Пусть $\varphi, \psi : \mathbb{R} \to \mathbb{R}$ — отображения, заданные формулами $\varphi(x) = x^3$ и $\psi(x) = x^2+x$. Проверьте, что $(\varphi \circ \psi)(x) = x^6 + 3x^5 + 3x^4 + x^3$, а $(\psi \circ \varphi)(x) = x^6 + x^3$. Таким образом, операция композиции, вообще говоря, не коммутативна.

Пусть $M_0, M_1, \ldots, M_n$ — произвольные множества, $\varphi_i : M_{i-1} \to M_i$ — отображения между ними. Рассмотрим выражение $\varphi_n \circ \varphi_{n-1} \circ \cdots \circ \varphi_1$. Каждой расстановке скобок в этом выражении отвечает некоторое отображение $M_0 \to M_n$. Из ассоциативности композиции с помощью индукции по n легко вывести, что все эти отображения совпадают (Проделайте это!). Для всех этих совпадающих отображений используется обозначение $\varphi_n \circ \varphi_{n-1} \circ \cdots \circ \varphi_1$.

Факторизация отображений

Кроме операций в алгебре рассматриваются еще отношения. Для любых двух множеств M и N всякое подмножество $R \subseteq M \times N$ называется *бинарным отношением* между M и N (или просто на M, если $N = M$). Обычно для отношения выбирают какой-нибудь символ (например $*$) и пишут $x * y$ для всех пар $(x, y) \in R$ (и только для них). Бинарное отношение на множестве M называется *отношением эквивалентности*, (для такого отношения обычно используется символ $\sim$), если для всех $x, x', x'' \in M$ выполнены следующие свойства:

1) $x \sim x$ (*рефлексивность*),

2) $x \sim x' \Rightarrow x' \sim x$ (*симметричность*),

3) $x \sim x', x' \sim x'' \Rightarrow x \sim x''$ (*транзитивность*).

Подмножество

$$\bar{x} = \{x' \in M \mid x' \sim x\} \subseteq M$$

всех элементов, эквивалентных данному x, называется *классом эквивалентности*, содержащим x.

Ясно, что классы эквивалентности покрывают множество M, попарно не пересекаясь (Почему?), т. е. образуют *разбиение* множества M. Множество классов эквивалентности называется *фактормножеством* M по отношению $\sim$ и обозначается через $M/{\sim}$. Сюръективное отображение $\pi : x \mapsto \bar{x}$ называется *канонической проекцией* M на $M/{\sim}$.

Пример 3.7. Пусть $M = \mathbb{Z}$. Зафиксируем натуральное число n. Введем на M отношение эквивалентности, полагая $k \sim m$ в том и только в том случае, когда $m - k$ делится на n. Классы эквивалентности в этом случае называются *классами вычетов по модулю* n.

Пример 3.8. Пусть M — это плоскость. Введем на ней декартову систему координат. Скажем, что точки (a_1, a_2) и (b_1, b_2) эквивалентны, если $a_1 - b_1 \in \mathbb{Z}$ и $a_2 - b_2 \in \mathbb{Z}$. Геометрически каждый класс эквивалентности представляет собой «решетку» на плоскости.

Попробуем построить естественную модель фактормножества M по этому отношению эквивалентности. Нетрудно убедиться, что полуоткрытый единичый квадрат $\{(a_1, a_2) \in M \mid 0 \leqslant a_1 < 1, 0 \leqslant a_2 < 1\}$ пересекается с каждым классом эквивалентности ровно по одной точке, так что фактормножество может быть отождествлено с таким квадратом. Эта модель обладает тем недостатком, что близким решеткам могут отвечать далекие друг от друга точки квадрата (например, если $\varepsilon > 0$ мало, то решетки $\overline{(0,0)}$ и $\overline{(-\varepsilon, -\varepsilon)}$ близки, а соответствующие точки квадрата $(0,0)$ и $(1-\varepsilon, 1-\varepsilon)$ – далеки). Этого недостатка можно избежать, рассмотрев замкнутый квадрат $\{(a_1, a_2) \in M \mid 0 \leqslant a_1 \leqslant 1, 0 \leqslant a_2 \leqslant 1\}$, а затем «склеив» (т. е. отождествив) точки, лежащие на противоположных сторонах. Склеив вертикальные сторон квадрата мы получим трубку, а склеив между собой верхнюю и нижнюю окружности, в которые превратились горизонтальные стороны квадрата после склеивания вертикальных, мы получим *тор*.

Теорема 3.9. *Пусть $\varphi : M \to N$ — произвольное отображение. Введем на M отношение эквивалентности $\sim_\varphi$, полагая $x \sim_\varphi y \Leftrightarrow \varphi(x) = \varphi(y)$. Пусть $Q = M/\!\sim_\varphi$, а $\pi : M \to Q$ — каноническая проекция. Тогда существует единственное отображение $\psi : Q \to N$, для которого $\varphi = \psi \circ \pi$, или, как говорят, для которого коммутативна следующая диаграмма:*

$$\begin{tikzcd} M \arrow[rr, "\varphi"] \arrow[dr, "\pi"'] & & N \\ & Q \arrow[ur, "\psi"'] & \end{tikzcd}$$

Отображение ψ инъективно, а если φ сюръективно, то ψ биективно.

Доказательство этой теоремы я оставляю в качестве упражнения.

Группы преобразований

Из определения следует, что для любых двух отображений φ и ψ множества M в себя определена их композиция $\varphi \circ \psi$, причем для любого отображения $\varphi : M \to M$ выполнены равенства $1_M \circ \varphi = \varphi$ и $\varphi \circ 1_M = \varphi$. Это оправдывает обозначение 1_M.

Предположим, что отображения φ и ψ множества M в себя являются биекциями. Тогда, как нетрудно проверить, их композиция $\varphi \circ \psi$ тоже является биекцией. Другими словами, множество $S(M)$ биективных отображений M в себя *замкнуто относительно взятия композиции*. Другое важное свойство множества $S(M)$ таково: для любой биекции $\varphi \in S(M)$ найдется, и притом только одна, биекция $\psi \in S(M)$, для которой

$$\varphi \circ \psi = 1_M,$$

т. е. ψ является *правым обратным отображением* к отображению φ, и

$$\psi \circ \varphi = 1_M,$$

т. е. ψ является *левым обратным отображением* к отображению φ. Эта биекция называется *обратной* к φ и обозначается φ^{-1}.

Элементы множества $S(M)$ называются *преобразованиями* множества M.

Если $\varphi \in S(M)$, а n — элемент множества целых чисел $\mathbb{Z}$, то по определению полагают

$$\varphi^n = \begin{cases} \underbrace{\varphi \circ \cdots \circ \varphi}_{n \text{ раз}}, & \text{если } n > 0; \\ 1_M, & \text{если } n = 0; \\ \underbrace{\varphi^{-1} \circ \cdots \circ \varphi^{-1}}_{-n \text{ раз}}, & \text{если } n < 0. \end{cases}$$

Упражнение 3.10. *Доказать, что для любых $m, n \in \mathbb{Z}$ выполнены равенства:*

$$\varphi^{m+n} = \varphi^m \circ \varphi^n \quad \textit{и} \quad (\varphi^n)^m = \varphi^{mn}.$$

Пусть $M = \{1, \ldots, n\}$. В этом случае множество $S(M)$ обозначается через S_n. Элементы S_n мы будем называть *перестановками* (иногда их называют подстановками; аргументацию в пользу принятой здесь терминологии см. в учебнике Кострикина, гл. 4, § 2).

Перестановки обычно задают таблицами вида:

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix},$$

где под каждым элементом множества $\{1, \ldots, n\}$ стоит его образ при преобразовании σ.

Определение 3.11. Непустое подмножество $G \subseteq S(M)$ называется *группой преобразований* множества M, если G замкнуто относительно композиции и взятия обратного преобразования, то есть если $\varphi \circ \psi \in G$ и $\varphi^{-1} \in G$ для любых $\varphi, \psi \in G$.

Из этого определения сразу следует, что если G — группа преобразований множества M, то $1_M \in G$.

Множество $S(M)$ является, конечно, группой преобразований множества M; оно называется *симметрической группой* множества M. Другой пример группы преобразований получается, если рассмотреть для произвольно заданного $\varphi \in S(M)$ множество $\langle\varphi\rangle = \{\psi \in S(M) \mid \psi = \varphi^n$ для некоторого $n \in \mathbb{Z}\}$. То, что $\langle\varphi\rangle$ является группой преобразований, следует из упражнения 3.10. Такая группа преобразований называется *циклической* группой преобразований, порожденной φ.

Приведем еще несколько примеров.

Пример 3.12. Пусть M — плоскость, $X \subseteq M$ — какая-либо геометрическая фигура. Рассмотрим множество G движений плоскости, переводящих фигуру X в себя. Легко проверить, что это — группа преобразований множества M. Она называется *группой симметрий* фигуры X.

Упражнение 3.13. Сколько элементов в группе симметрий правильного n-угольника?

Пример 3.14. Пусть M — трехмерное пространство, $X \subseteq M$ — правильный многогранник. Рассмотрим множество G вращений (вокруг некоторой оси) пространства M, переводящих X в себя. Поскольку композиция вращений вновь является вращением (Проверьте это!), то G — группа преобразований множества M. Она называется *группой вращений* многогранника X. Часто вместо «группа вращений куба (тетраэдра, икосаэдра)» говорят просто «группа куба (соответственно тетраэдра или икосаэдра)».

Вложенный в пространство правильный многоугольник можно считать вырожденным правильным многогранником с двумя гранями — *диэдром*. Группа его вращений называется *группой диэдра*.

Пусть G — произвольная группа преобразований множества M. Сопоставим каждому элементу $m \in M$ множество $G_m = \{\varphi \in G \mid \varphi(m) = m\}$ преобразований из G, оставляющих его на месте. Ясно, что для любого фиксированного элемента $m \in M$ композиция преобразований из G_m вновь лежит в G_m, и обратное преобразование к преобразованию из G_m тоже лежит в G_m. Таким образом, G_m тоже является группой преобразований. Она называется *стационарной подгруппой* или *стабилизатором* элемента m.

Если $\varphi \in G_m$, то m называется *неподвижной точкой* преобразования φ. Множество неподвижных точек преобразования φ обозначается через $Fix\,\varphi$.

С другой стороны, рассмотрим для каждого $m \in M$ множество $G(m) = \{\varphi(m) \mid \varphi \in G\}$ всех элементов множества M, в которые m переходит под действием преобразований из G. Это множество называется *G-орбитой* элемента m.

Замечание. G-орбиты называют также орбитами относительно группы G, или просто орбитами группы G. Говорят даже «орбиты элемента $\varphi \in G$», имея в виду $\langle\varphi\rangle$-орбиты. Как правило, путаница при этом не возникает.

Пример 3.15. Пусть M — плоскость, G — группа движений плоскости. Тогда стабилизатор G_m точки $m \in M$ состоит из всевозможных вращений вокруг точки m, а также отражений относительно всевозможных прямых, проходящих через m.

Поскольку G_m тоже является группой преобразований плоскости, мы можем рассматривать ее орбиты. G_m-орбитой точки n является окружность с центром в точке m, проходящая через n.

Упражнение 3.16. *Доказать, что G-орбита элемента $\varphi(m)$ совпадает с G-орбитой элемента m для любых $m \in M$, $\varphi \in G$.*

Упражнение 3.17. *Доказать, что $G_{\varphi(m)} = \{\varphi \circ \psi \circ \varphi^{-1} \mid \psi \in G_m\}$ для любых $m \in M$, $\varphi \in G$.*

Теорема 3.18. *Пусть G — конечная группа преобразований множества M. Тогда $|G| = |G(m)| \cdot |G_m|$ для любого $m \in M$.*

Доказательство. Выберем для каждого элемента $n \in G(m)$ фиксированное преобразование $g_n \in G$ такое, что $n = g_n(m)$. Поставим в соответствие каждой паре (n, h), где $n \in G(m)$ и $h \in G_m$, преобразование $g_n \circ h$ из G. Докажем, что это соответствие взаимно однозначно.

Пусть

$$g_n \circ h = g_{n'} \circ h', \tag{11}$$

где $n, n' \in G(m)$ и $h, h' \in G_m$. Применим это преобразование к m. Поскольку $h, h' \in G_m$, мы получаем $g_n(m) = g_{n'}(m)$, то есть $n = n'$. Умножая обе части (11) слева на g_n^{-1}, получаем $h = h'$. Поэтому отображение $(n, h) \mapsto g_n \circ h$ инъективно.

Рассмотрим теперь произвольное преобразование $\varphi \in G$. Положим $n = \varphi(m)$. Тогда $n \in G(m)$, поэтому определено преобразование g_n. Положим $h = g_n^{-1} \circ \varphi$. Тогда

$$h(m) = g_n^{-1}(\varphi(m)) = g_n^{-1}(n) = m,$$

то есть $h \in G_m$. При этом $\varphi = g_n \circ g_n^{-1} \circ \varphi = g_n \circ h$. Таким образом, отображение $(n, h) \mapsto g_n \circ h$ сюръективно. Следовательно, оно биективно, и $|G| = |G(m)| \cdot |G_m|$. $\square$

Из упражнения 3.16 следует, что каждая группа преобразований G множества M задает на M отношение эквивалентности, классами эквивалентности по которому являются G-орбиты (а именно, $m \sim n$, если найдется $\varphi \in G$, для которого $n = \varphi(m)$). Рассмотрим фактормножество по этому отношению эквивалентности. Оно называется *пространством орбит* и обозначается через M/G.

Теорема 3.19 (Формула Бернсайда). *Пусть G — группа преобразований конечного множества M. Тогда*

$$|M/G| = \frac{1}{|G|} \sum_{\varphi \in G} |Fix\, \varphi|.$$

Доказательство. Прежде всего отметим, что раз M конечно, то и группа преобразований G тоже конечна.

Рассмотрим множество $\tilde{M} = \{(\varphi, m) \in G \times M \mid \varphi(m) = m\}$. Подсчитаем число элементов этого множества.

С одной стороны,

$$\left|\tilde{M}\right| = \sum_{\varphi \in G} |Fix\, \varphi|. \tag{12}$$

С другой стороны,

$$\left|\tilde{M}\right| = \sum_{m\in M} |G_m| = \sum_{X\in M/G} \Big(\sum_{m\in X} |G_m|\Big), \tag{13}$$

поскольку G-орбиты образуют разбиение множества M. Из упражнения 3.17 следует, что для любых элементов $m, n \in M$, лежащих в одной G-орбите, $|G_m| = |G_n|$. Поэтому для любой G-орбиты $X = G(n)$

$$\sum_{m\in X} |G_m| = |X|\cdot|G_n|,$$

что, по теореме 3.18, равно $|G|$. Поэтому (13) можно переписать следующим образом:

$$\left|\tilde{M}\right| = \sum_{X\in M/G} |G| = |G|\cdot|M/G|. \tag{14}$$

Сравнивая (12) и (14), получаем утверждение теоремы. □

Симметрическая группа

Операцию композиции в группе перестановок обозначают как умножение — точкой (или пустым местом); соответственно результат композиции двух перестановок часто называют их произведением. Тождественную перестановку мы будем обозначать буквой e.

Пусть $i_1, \dots, i_k$ — попарно различные элементы множества M. Обозначим через $(i_1, \dots, i_k)$ перестановку $\sigma \in S_n$, переводящую i_1 в i_2, i_2 в i_3, …, i_{k-1} в i_k, i_k в i_1, а все остальные элементы множества M оставляющую на месте. Такая перестановка называется *циклом*. Число k называется длиной цикла. Из определения ясно, что все циклы длины 1 равны между собой и равны тождественному отображению. Мы будем называть циклы длины 1 тривиальными.

Орбитами цикла $\sigma = (i_1, \dots, i_k)$ (то есть $\langle\sigma\rangle$-орбитами) являются множество $\{i_1, \dots, i_k\}$ и одноэлементные множества $\{i\}$, где $i \in M \setminus \{i_1, \dots, i_k\}$.

Пусть $\sigma = (i_1, \dots, i_k)$ и $\tau = (j_1, \dots, j_l)$ — циклы, причем $\{i_1, \dots, i_k\} \cap \{j_1, \dots, j_l\} = \varnothing$. Тогда $\sigma\tau = \tau\sigma$ (Почему?). Такие циклы называются *независимыми*.

Рассмотрим теперь произвольную перестановку φ. Пусть $I^1, \dots, I^m$ — все ее орбиты, содержащие более одного элемента. Выберем в каждой орбите I^α по элементу i_1^α. Пусть k_α — минимальное натуральное число, для которого $\varphi^{k_\alpha}(i_1^\alpha) = i_1^\alpha$ (если таких натуральных чисел нет, то положим $k_\alpha = \infty$).

Докажем, что $\varphi^r(i_1^\alpha) \neq \varphi^s(i_1^\alpha)$ при $1 \leqslant r < s < k_\alpha$. Действительно, если $\varphi^r(i_1^\alpha) = \varphi^s(i_1^\alpha)$, то $\varphi^{s-r}(i_1^\alpha) = i_1^\alpha$. Согласно определению k_α такого быть не может, поскольку $0 < s - r < k_\alpha$.

Отсюда, в частности, следует, что $k_\alpha < \infty$, поскольку все элементы вида $\varphi^r(i_1^\alpha)$ лежат в конечном множестве I^α.

Положим $i_r^\alpha = \varphi^{r-1}(i_1^\alpha)$ для $r = 2, \dots, k_\alpha$. Как мы показали, все эти элементы попарно различны (и не равны i_1^α). Кроме того, $I^\alpha = \{i_1^\alpha, \dots, i_{k_\alpha}^\alpha\}$. Действительно, по определению, любой элемент $\langle\varphi\rangle$-орбиты числа i_1^α имеет вид $\varphi^t(i_1^\alpha)$ при некотором целом t. Поделим с остатком t на k_α: $t = qk_\alpha + r$, $0 \leqslant r < k_\alpha$. Тогда

$$\varphi^t(i_1^\alpha) = \varphi^r \cdot \varphi^{qk_\alpha}(i_1^\alpha) = \varphi^r \cdot (\varphi^{k_\alpha})^q(i_1^\alpha) = \varphi^r(i_1^\alpha) = i_{r+1}^\alpha.$$

Из всего сказанного следует, что перестановка φ действует на элементы из I^α так же, как цикл $\sigma_\alpha = (i_1^\alpha, \dots, i_{k_\alpha}^\alpha)$. Более того, имеет место равенство $\varphi = \sigma_1 \cdot \dots \cdot \sigma_m$. Порядок сомножителей в этом произведении не важен, поскольку входящие в него циклы попарно независимы.

Таким образом, доказана

Теорема 3.20. *Каждая перестановка разлагается в произведение независимых нетривиальных циклов.*

Упражнение 3.21. *Доказать, что представление перестановки в виде произведения независимых нетривиальных циклов единственно с точностью до порядка следования сомножителей.*

Лекция 4.

Продолжим изучение симметрической группы.

Определение 4.1. Цикл длины 2 называется *транспозицией*.

Рассмотрим следующие транспозиции: $s_1 = (1,2)$, $s_2 = (2,3)$, $\ldots$, $s_{n-1} = (n-1,n)$. Каждая из этих перестановок меняет местами какие-нибудь два соседние элемента, оставляя остальные на местах.

Определение 4.2. *Длиной* $l(\sigma)$ перестановки σ называется число ее инверсий, то есть таких пар (i,j), что $i<j$, но $\sigma(i)>\sigma(j)$.

Теорема 4.3. *Каждая перестановка $\sigma \in S_n$ может быть представлена в виде произведения:*

$$\sigma = s_{i_1}s_{i_2}\ldots s_{i_l},$$

где $l = l(\sigma)$, а $(i_1,\ldots,i_l)$ — некоторая последовательность элементов множества $\{1,\ldots,n-1\}$ (члены последовательности могут повторяться).

Доказательство. Воспользуемся индукцией по $l(\sigma)$.

Если $l(\sigma)=0$, то, очевидно, $\sigma = e$ и доказывать нечего.

Пусть $l(\sigma) = l > 0$ и для всех перестановок длины меньшей l утверждение теоремы верно. Докажем его для σ.

Поскольку $l(\sigma)>0$, то найдутся $i,j\in M$ такие, что $i<j$ и $\sigma(i)>\sigma(j)$. Выберем такую пару (i,j) с минимальной разностью $j-i$. Если $j-i>1$, то либо $\sigma(i+1)>\sigma(i)>\sigma(j)$, но $i+1<j$, либо $\sigma(i)>\sigma(i+1)$ но $i<i+1$. В обоих случаях получаем противоречие с минимальностью $j-i$. Поэтому $j-i=1$, то есть $\sigma(i)>\sigma(i+1)$.

Рассмотрим перестановку $\sigma' = \sigma s_i$. Нетрудно убедиться, что $l(\sigma') = l-1$ (Почему?). По предположению индукции имеется разложение

$$\sigma' = s_{i_1}s_{i_2}\ldots s_{i_{l-1}}.$$

Поскольку $s_i^2 = e$, то $\sigma' s_i = \sigma s_i^2 = \sigma$. Отсюда мы получаем искомое разложение

$$\sigma = s_{i_1}s_{i_2}\ldots s_{i_l},$$

где $i_l = i$. $\square$

Замечание. Разложение, построенное в теореме 4.3, не является однозначным. Рассмотрим, например, перестановку $\sigma = (1,3)\in S_3$. Проверьте, что $l(\sigma) = 3$ и существуют два разложения: $\sigma = s_1s_2s_1$ и $\sigma = s_2s_1s_2$.

Определение 4.4. *Знаком* перестановки σ называется число

$$\varepsilon(\sigma) = (-1)^{l(\sigma)}.$$

Перестановка σ называется *четной*, если $\varepsilon(\sigma)=1$, и *нечетной*, если $\varepsilon(\sigma)=-1$.

Теорема 4.5. *Знак произведения двух перестановок равен произведению их знаков.*

Доказательство. Прежде всего отметим, что для любой перестановки $\sigma\in S_n$ и любого $i\in\{1,\ldots,n-1\}$

$$l(\sigma s_i) = \begin{cases} l(\sigma)+1, & \text{если } \sigma(i)<\sigma(i+1); \\ l(\sigma)-1, & \text{если } \sigma(i)>\sigma(i+1). \end{cases}$$

(Это очевидно из определения длины перестановки как числа инверсий.) Поэтому всегда $\varepsilon(\sigma s_i) = -\varepsilon(\sigma)$. Отсюда следует, что для любого разложения $\sigma = s_{i_1} \cdot \dots \cdot s_{i_m}$, где m не обязано совпадать с $l(\sigma)$, выполнено равенство $\varepsilon(\sigma) = (-1)^m$.

Пусть теперь у нас есть две перестановки σ и σ', длины которых $l(\sigma) = l$ и $l(\sigma') = l'$. По теореме 4.3 существуют разложения $\sigma = s_{i_1} \cdot \dots \cdot s_{i_l}$ и $\sigma' = s_{i'_1} \cdot \dots \cdot s_{i'_{l'}}$. Тогда $\sigma\sigma' = s_{i_1} \cdot \dots \cdot s_{i_l} \cdot s_{i'_1} \cdot \dots \cdot s_{i'_{l'}}$, следовательно, $\varepsilon(\sigma\sigma') = (-1)^{l+l'} = \varepsilon(\sigma)\varepsilon(\sigma')$. $\square$

Определение 4.6. Обозначим через A_n подмножество симметрической группы S_n, состоящее из всех четных перестановок. Из теоремы 4.5 легко следует, что A_n является группой преобразований множества M. Она называется *знакопеременной группой.*

Группы

Определение 4.7. Пусть G — некоторое множество, на котором задана бинарная операция $*$ (то есть правило, сопоставляющее каждой упорядоченной паре элементов $g_1, g_2 \in G$ элемент $g_1 * g_2 \in G$), так, что выполнены следующие аксиомы:

1) Ассоциативность: $(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$ для любых $g_1, g_2, g_3 \in G$;

2) Существование нейтрального элемента: существует такой элемент $e \in G$, что $e * g = g * e = g$ для любого $g \in G$;

3) Существование обратного элемента: для любого $g \in G$ существует такой элемент $h \in G$, что $h * g = g * h = e$.

В этом случае G называется *группой* (относительно операции $*$).

Группа называется *коммутативной* или *абелевой*, если в ней дополнительно выполнена аксиома коммутативности: $g_1 * g_2 = g_2 * g_1$ для любых $g_1, g_2 \in G$.

Из аксиом группы легко следует единственность нейтрального и обратных элементов.

Пример 4.8. Примером группы является произвольная группа преобразований. Примером абелевой группы является произвольное коммутативное кольцо A относительно операции сложения, а также множество $\Bbbk^*$ ненулевых элементов произвольного поля $\Bbbk$ относительно умножения.

Замечание. Как правило, для групп используют либо *мультипликативную* форму записи, либо *аддитивную* форму записи. А именно, в мультипликативном случае вместо $*$ либо не используют вообще никакого знака, либо используют знак умножения. Саму групповую операцию при этом называют умножением, а результат операции $g_1 g_2$ — произведением g_1 и g_2. При этом нейтральный элемент e называют единицей. Обратный элемент к g обозначают через g^{-1}.

В аддитивном случае вместо $*$ пишут $+$, операцию называют сложением, нейтральный элемент называют нулем и обозначают 0, и вообще используют привычную для сложения терминологию. Аддитивную форму записи используют почти исключительно для абелевых групп.

В дальнейшем мы будем следовать этой традиции.

Определение 4.9. Пусть G — группа, а M — произвольное множество. Скажем, что задано *действие группы G на множестве M*, если для каждого $g \in G$ и для каждого $m \in M$ определен элемент $g(m) \in M$, причем $e(m) = m$ для любого m (e — единица группы G) и $g_1 g_2(m) = g_1(g_2(m))$ для любых $g_1, g_2 \in G$ и $m \in M$.

Понятия орбиты, стабилизатора и относящиеся к ним теоремы, доказанные на прошлой лекции, буквально переносятся (вместе с доказательствами) на случай действия абстрактной группы G на множестве M. Единственное изменение, которое нужно сделать в формулировке теоремы Бернсайда, состоит в том, что необходимо потребовать конечность группы G (это уже не следует из конечности множества M).

Действие группы G на множестве M называется *транзитивным*, если всё множество M является G-орбитой. В этом случае для конечной группы G получаем из теоремы, доказанной на предыдущей лекции

$$|G| = |M| \cdot |G_m|, \tag{15}$$

для произвольного элемента $m \in M$.

Определение 4.10. Подмножество $H \subseteq G$ называется подгруппой, если оно непусто и замкнуто относительно умножения и взятия обратного элемента, то есть для любых $h_1, h_2 \in H$ их произведение $h_1 h_2$ и обратные к ним h_1^{-1}, h_2^{-1} лежат в H.

Пример 4.11. Любая группа преобразований множества M является, по определению, подгруппой симметрической группы $S(M)$.

Пример 4.12. Пусть G — любая группа преобразований множества M. Для любого элемента $m \in M$ его стабилизатор G_m является подгруппой группы G.

Определение 4.13. Пусть H — подгруппа группы G. *Левым смежным классом группы G по подгруппе H* называется множество вида $gH = \{gh \mid h \in H\}$, где $g \in G$. Аналогично, *правым смежным классом группы G по подгруппе H* называется множество вида $Hg = \{hg \mid h \in H\}$, где $g \in G$.

Упражнение 4.14. *Пусть H — подгруппа группы G. Определим на G отношение $\sim$, полагая $g_1 \sim g_2$, если $g_1^{-1} g_2 \in H$. Доказать, что это отношение эквивалентности, причем классами эквивалентности являются в точности левые смежные классы G по H. Какому отношению эквивалентности отвечают правые смежные классы?*

Обозначим через G/H множество левых смежных классов G по H. Это фактормножество G по отношению эквивалентности, введенному в упражнении 4.14. Аналогично, через $H\backslash G$ обозначается множество правых смежных классов G по H.

Теорема 4.15 (Лагранжа). *Пусть G — конечная группа и H — ее подгруппа. Тогда*

$$|G| = |H| \cdot |G/H| = |H| \cdot |H\backslash G|.$$

Доказательство. Положим $g(g'H) = gg'H$. Очевидно, что таким образом задается действие группы G на множестве G/H, причем это действие транзитивно. Легко проверить также, что стабилизатором смежного класса $H = eH \in G/H$ является в точности группа H. Применяя формулу (15), получаем первую часть утверждения теоремы.

Вторая часть доказывается аналогично с использованием следующего действия группы G на множестве $H\backslash G$: $g(Hg') = Hg'g^{-1}$. $\square$

В действительности, непосредственное доказательство теоремы Лагранжа спрятано внутри доказательства формулы (15), которое я приводил на прошлой лекции. Советую вам в этом убедиться.

Число элементов группы называется *порядком* группы. В качестве следствия из теоремы Лагранжа мы получаем, что порядок подгруппы всегда делит порядок конечной группы.

Определение 4.16. Пусть H — подгруппа группы G. Число $(G{:}H)$ левых смежных классов G по H называется *индексом* H в G.

Отметим, что индекс $(G{:}H)$ может быть конечен, даже если группа G бесконечна.

Упражнение 4.17. *Найти индекс подгруппы $\mathbb{Q}_+^*$ положительных рациональных чисел в группе $\mathbb{Q}^*$.*

Упражнение 4.18. *Доказать, что число правых смежных классов по подгруппе конечного индекса тоже конечно и равно индексу.*

Определение 4.19. Пусть G — группа, $g_1, \ldots, g_k$ — некоторые ее элементы. *Подгруппой, порожденной элементами* $g_1, \ldots, g_k$ назовем минимальную (по включению) подгруппу H группы G, их содержащую. Такая подгруппа обозначается через $\langle g_1, \ldots, g_k \rangle$. (Слова «минимальная по включению» означают, что любая подгруппа $H' \subset H$, $H' \neq H$ уже не содержит какого-то из элементов $g_1, \ldots, g_k$.)

Подгруппа, порожденная одним элементом, называется *циклической*. *Порядком элемента* $g \in G$ называется порядок порожденной g циклической подгруппы.

Если $G = \langle g_1, \ldots, g_k \rangle$, то элементы $g_1, \ldots, g_k$ называются *образующими* группы G.

Очевидно, что для любых элементов $g_1, \ldots, g_k$ группы G порожденная ими подгруппа содержит всевозможные произведения вида $g_{i_1}^{n_1} g_{i_2}^{n_2} \ldots g_{i_r}^{n_r}$, где $n_1, \ldots, n_r \in \mathbb{Z}$ и $i_1, \ldots, i_r \in \{1, \ldots, k\}$. С другой стороны, множество всех элементов группы G, которые можно представить в виде произведений такого вида, является подгруппой. Поэтому

$$\langle g_1, \ldots, g_k \rangle = \{g_{i_1}^{n_1} \ldots g_{i_r}^{n_r} \mid i_1, \ldots, i_r \in \{1, \ldots, k\}; n_1, \ldots, n_r \in \mathbb{Z}\}$$

Пример 4.20. Элементы $s_1, \ldots, s_{n-1}$ являются образующими симметрической группы S_n (см. теорему 4.3).

Упражнение 4.21. *Доказать, что порядок элемента $g \in G$ равен минимальному натуральному числу k, для которого $g^k = e$.*

Определение 4.22. Пусть G, G' — группы. Отображение $\varphi : G \to G'$ называется *гомоморфизмом*, если $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$ для любых $g_1, g_2 \in G$. Биективный гомоморфизм называется *изоморфизмом*.

Упражнение 4.23. *Доказать, что при любом гомоморфизме $\varphi : G \to H$ образом единицы группы G является единица группы H.*

Пусть $\varphi : G \to H$ — гомоморфизм групп. По определению, $\varphi(gg') = \varphi(g)\varphi(g')$ для любых $g, g' \in G$. Согласно упражнению 4.23, единица группы G отображается в единицу группы H. Отсюда сразу следует, что $\varphi(g^{-1}) = \varphi(g)^{-1}$ для любого $g \in G$. Тем самым образ $\varphi(G)$ гомоморфизма φ является подгруппой в H. Из тех же соображений очевидно, что множество $\operatorname{Ker} \varphi = \{g \in G \mid \varphi(g) = e\}$, называемое *ядром* гомоморфизма φ, является подгруппой в G.

Упражнение 4.24. *Доказать, что при гомоморфизм $\varphi : G \to H$ инъективен тогда и только тогда, когда $\operatorname{Ker} \varphi = \{e\}$.*

Пример 4.25. Пусть задано действие группы G на множестве M. Тогда для любого $g \in G$ определено отображение $m \mapsto g(m)$ множества M в себя. Это отображение имеет обратное: $m \mapsto g^{-1}(m)$, поэтому оно является преобразованием множества M.

Таким образом, каждому элементу группы G отвечает преобразование множества M, то есть мы получаем отображение группы G в симметрическую группу $S(M)$. Очевидно, что это отображение является гомоморфизмом, причем каждый гомоморфизм $G \to S(M)$ связан с некоторым действием группы G на множестве M.

Рассмотрим действие G на себе, определяемое формулой: $g(h) = gh$. Этому действию отвечает некоторый гомоморфизм $\varphi : G \to S(G)$. Обозначим через $\overline{G}$ образ гомоморфизма φ. Очевидно, что $\overline{G}$ является группой преобразований множества G.

Пусть $g_1, g_2 \in G$ таковы, что $g_1 g = g_2 g$ для любого $g \in G$. Тогда $g_1 = g_1 e = g_2 e = g_2$. Отсюда следует, что φ биективно отображает G на $\overline{G}$. Мы получили следующий удивительный результат:

Теорема 4.26 (Кэли). *Каждая группа изоморфна некоторой группе преобразований.*

Таким образом, группы преобразований, которые мы использовали в качестве мотивировки определения абстрактных групп, в действительности являются наиболее общим примером последних.

Определение 4.27. Пусть G — произвольная группа. Преобразование $\varphi \in S(G)$ называется *автоморфизмом*, если оно является изоморфизмом группы G на себя. Множество автоморфизмов группы G обозначается через $\operatorname{Aut} G$.

Упражнение 4.28. *Доказать, что* $\operatorname{Aut} G$ *является подгруппой группы* $S(G)$, *то есть группой преобразований множества* G.

Упражнение 4.29. *Пусть* G — *группа и* $g \in G$. *Доказать, что отображение* $\imath_g : G \to G$, *заданное формулой* $\imath_g(h) = ghg^{-1}$, *является автоморфизмом.*

Обозначим через f отображение G в $\operatorname{Aut} G$, переводящее g в $\imath_g$. Легко видеть, что f является гомоморфизмом. Ядро f называется *центром* группы G; его составляют элементы группы G, коммутирующие со всеми элементами G, то есть такие $g \in G$, что $gh = hg$ для любого $h \in G$. Автоморфизмы, составляющие образ f, называются *внутренними*. Общепринятые обозначения: $Z(G) = \operatorname{Ker} f$, $\operatorname{Int} G = f(G)$.

Отметим, что гомоморфизм f определяет действие группы G на себе; действие элемента $g \in G$ называется *сопряжением с помощью* g. Орбиты этого действия называются *классами сопряженных элементов*.

Упражнение 4.30. *Пусть* $\sigma \in S_n$ — *цикл длины* k, *а* $\tau \in S_n$ — *произвольная перестановка. Доказать, что* $\tau\sigma\tau^{-1}$ — *цикл длины* k. *Какие элементы входят в этот цикл, если* $\sigma = (1, 2, \ldots, k)$?

Задача 4.31. *Найти* $Z(G)$, $\operatorname{Int} G$, $\operatorname{Aut} G$ *и классы сопряженных элементов для* $G = \mu_n$, D_n, S_n, A_n, *где* μ_n — *группа комплексных корней из единицы степени* n, D_n — *группа диэдра,* S_n — *симметрическая, и* A_n — *знакопеременная группы. Постарайтесь решить эту задачу хотя бы для малых* n.

Лекция 5.

Начнем с небольшого добавления к прошлой лекции.

Пусть G — конечное множество. Как задать на G структуру группы? Проще всего составить таблицу такого вида:

$\cdot$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

На пересечении строки, озаглавленной $x \in G$, и столбца, озаглавленного $y \in G$, ставится их произведение xy. В данном случае $G = \{e, a, b\}$. Такая таблица называется *таблицей Кэли*.

Легко проверить, что приведенная нами таблица задает группу, изоморфную группе μ_3 комплексных корней третей степени из единицы (это записывается так: $G \cong \mu_3$).

Упражнение 5.1. *Составьте таблицу Кэли для группы S_3.*

Нормальные подгруппы и факторгруппы

Отметим, что любая подгруппа $K \subseteq H$ является образом некоторого гомоморфизма (в качестве такового можно взять ограничение на K тождественного отображения H в H). Выясним теперь, какие подгруппы $N \subseteq G$ могут являться ядрами гомоморфизмов.

Ядро $\operatorname{Ker}\varphi$ гомоморфизма $\varphi : G \to H$ является слоем отображения φ над единицей группы H. Выберем произвольный элемент $g \in G$ и положим $h = \varphi(g)$. Элемент $g' \in G$ принадлежит слою отображения φ над h тогда и только тогда, когда $\varphi\left(g^{-1}g'\right) = e$, то есть когда g' принадлежит тому же левому смежному классу группы G по подгруппе $N = \operatorname{Ker}\varphi$, что и g. Аналогично проверяется, что $g' \in \varphi^{-1}(h)$ тогда и только тогда, когда g' принадлежит тому же правому смежному классу G по N, что и g. Отсюда следует, что левые смежные классы группы G по подгруппе N совпадают с правыми, являясь в точности слоями отображения φ.

Определение 5.2. Подгруппа $N \subseteq G$ называется *нормальной* (или *инвариантной*, или *нормальным делителем*), если левые смежные классы группы G по подгруппе N совпадают с правыми, то есть если для любого $g \in G$ выполнено равенство $gH = Hg$ или, что равносильно, $gHg^{-1} = H$. То, что N является нормальной подгруппой группы G, часто обозначается так: $N \lhd G$.

Отметим следующее важное, хотя и очевидное, следствие определения;

Утверждение 5.3. *Подгруппа $N \subseteq G$ является нормальной тогда и только тогда, когда она является объединением классов сопряженности группы G.*

Пусть N — нормальная подгруппа группы G. Тогда множество G/N (совпадающее с $N\backslash G$) можно наделить естественной структурой группы. Действительно, $(gN)(g'N) = g(Ng')N = g(g'N)N = gg'N$, то есть произведение двух смежных классов снова является смежным классом. Умножение смежных классов, очевидно, является ассоциативным, $N = eN$ является нейтральным элементом, а $g^{-1}N$ является обратным к gN. Отсюда сразу следует

Теорема 5.4. *Если N — нормальная подгруппа группы G, то операция $(gN)\cdot(g'N) = gg'N$ наделяет фактормножество G/N структурой группы, называемой факторгруппой G по N. При этом каноническая проекция $\pi : G \to G/N$ является гомоморфизмом групп, и $N = \operatorname{Ker}\pi$.*

Пусть $\varphi : G \to H$ — произвольный гомоморфизм групп. Положим $N = \operatorname{Ker}\varphi$. Мы уже проверили, что левые смежные классы группы G по N совпадает с правыми, то есть $N \lhd G$, при этом смежные классы G по N являются в точности слоями отображения φ. По теореме о факторизации отображений существует единственное отображение $\psi : G/N \to H$, делающее диаграмму

$$\begin{tikzcd} G \arrow[rr, "\varphi"] \arrow[dr, "\pi"'] & & H \\ & G/N \arrow[ur, "\psi"'] & \end{tikzcd}$$

коммутативной. Легко проверить, что ψ является гомоморфизмом групп. Таким образом, из теоремы о факторизации отображений следует

Теорема 5.5 (О гомоморфизмах групп). *Пусть $\varphi : G \to H$ — гомоморфизм групп с ядром N. Тогда существует единственный гомоморфизм $\psi : G/N \to H$ такой, что $\varphi = \psi \circ \pi$, где $\pi : G \to G/N$ — каноническая проекция. При этом ψ является изоморфизмом G/N на $\varphi(G)$.*

В частности, если гомоморфизм φ сюръективен, то факторгруппа G/N изоморфна H.

Пример 5.6. Группа $\mathbb{Z}$ — абелева, поэтому любая подгруппа в ней нормальна. Факторгруппа $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ называется *группой классов вычетов по модулю n*. Рассмотрим гомоморфизм $\varphi : \mathbb{Z} \to \mathbb{C}^*$, задаваемый формулой $\varphi(k) = e^{2\pi ik/n}$ ($n \in \mathbb{N}$ — фиксировано). Тогда $\operatorname{Ker}\varphi = n\mathbb{Z}$, $\varphi(\mathbb{Z}) = \mu_n$ и, согласно теореме 5.5, мы имеем изоморфизм групп $\mathbb{Z}_n \cong \mu_n$.

Пример 5.7. Пусть $n > 1$. Функция «знак перестановки» представляет собой гомоморфизм симметрической группы S_n в группу $\mu_2 = \{\pm 1\}$. Знакопеременная группа — ядро этого гомоморфизма, а образом, очевидно, является вся группа μ_2. Мы получаем $S_n/A_n \cong \mu_2$.

Задание групп образующими и соотношениями

Мы уже встречались с понятием системы образующих группы. Например, симметрическая группа S_n порождается образующими $s_1 = (1,2), \ldots, s_{n-1} = (n-1, n)$. Между образующими группы могут быть соотношения. Так, в симметрической группе выполнены соотношения $s_i^2 = e$ ($i = 1, \ldots, n-1$), $s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}$ ($i = 1, \ldots, n-2$), $s_i s_j = s_j s_i$ ($i, j = 1, \ldots, n-1$; $|i-j| > 1$).

Из одних соотношений могут следовать другие; например, из соотношения $s_1^2 = e$ следует соотношение $s_1^{-4} = e$, а из соотношений $s_1^2 = e$, $s_2^2 = e$ и $s_1 s_2 s_1 = s_2 s_1 s_2$ следует соотношение $(s_1 s_2)^3 = e$. Исходя из этого, можно попробовать дать логическое определение группы, порожденной образующими и соотношениями, как группы, имеющей предписанные образующие, между которыми выполняются предписанные соотношения и все их следствия (и только они). При этом встает естественный вопрос: как доказать существование такой группы? Следующая алгебраическая конструкция позволяет как избежать возни со строгим логическим определением следствий заданных соотношений, так и снимает вопрос существования группы, заданной образующими и соотношениями.

Построим сначала группу с заданным множеством образующих, но «без соотношений».

Определение 5.8. Пусть S — произвольное множество. Обозначим через A множество $S \sqcup \{s^{-1} \mid s \in S\}$. Рассмотрим множество всех *слов в алфавите A*, то есть множество всех конечных последовательностей $a_1 \ldots a_k$, где k — неотрицательное целое число (подчеркнем, что среди прочих мы рассматриваем и *пустое слово*). Назовем *элементарным преобразованием* слова w любое слово, получающееся из w вставкой в него в произвольном месте двубуквенного слова вида ss^{-1} или $s^{-1}s$, где $s \in S$, или вычеркиванием двух букв ss^{-1} или $s^{-1}s$, идущих подряд. Два слова называются эквивалентными, если одно можно получить из другого цепочкой элементарных преобразований. *Свободной группой $F(S)$* с множеством образующих S называется множество классов эквивалентности.

Произведением классов эквивалентности, содержащих слова $a_1 \ldots a_k$ и $b_1 \ldots b_l$, называется класс эквивалентности слова $a_1 \ldots a_k b_1 \ldots b_l$. Легко проверить, что это определение является корректным (то есть при замене исходных слов эквивалентными получается в качестве произведения тот же класс эквивалентности). Очевидно, что введенное таким образом произведение является ассоциативным, и класс эквивалентности пустого слова является единичным элементом. Кроме того, класс эквивалентности слова $a_k^{-1}\dots a_1^{-1}$ является обратным к классу эквивалентности слова $a_1\dots a_k$ (мы полагаем $a^{-1}=s$ для $a=s^{-1}$, где $s\in S$).

Положим

$$s^k=\begin{cases}\underbrace{s\dots s}_{k\text{ раз}} & \text{при } k>0,\\ \varnothing & \text{при } k=0,\\ \underbrace{s^{-1}\dots s^{-1}}_{-k\text{ раз}} & \text{при } k<0.\end{cases}$$

Очевидно, что любой элемент свободной группы $F(S)$ можно записать в виде $s_1^{k_1}s_2^{k_2}\dots s_m^{k_m}$, где $m\in\mathbb{N}\cup\{0\}$, $s_i\in S$, $s_i\neq s_{i+1}$, $k_i\in\mathbb{Z}\setminus\{0\}$ $(i=1,\dots,m)$. Такая запись называется несократимой.

Пусть теперь нам задано некоторое подмножество $R\subset F(S)$. Мы хотели бы, говоря неформально, построить группу G, заданную образующими s из множества S и соотношениями $s_1^{k_1}\dots s_m^{k_m}=e$ для всех слов $s_1^{k_1}\dots s_m^{k_m}\in R$. Идея состоит в том, чтобы определить G как некоторую факторгруппу свободной группы $F(S)$.

Подгруппа, порожденная элементами множества R, не обязательно является нормальной, поэтому, вообще говоря, факторизовать по ней нельзя. Обозначим через $N(R)$ пересечение всех нормальных подгрупп группы $F(S)$, содержащих множество R. Подгруппа $N(R)$ уже является нормальной. Действительно, $N(R)=\bigcap N_\alpha$, где все подгруппы N_α нормальны в $F(S)$, то есть если $x\in N_\alpha$, то и $gxg^{-1}\in N_\alpha$ для любого $g\in F(S)$. Поэтому если $x\in\bigcap N_\alpha$, то и $gxg^{-1}\in\bigcap N_\alpha$ для любого $g\in F(S)$. Это означает, что $\bigcap N_\alpha=N(R)\lhd F(S)$.

Определение 5.9. *Группой, заданной образующими $s\in S$ и соотношениями $r=e$, где $r\in R\subset F(S)$*, называется факторгруппа $G=F(S)/N(R)$. Часто используется обозначение $G=\langle s_1,\dots,s_n\mid r_1=e,\dots,r_m=e\rangle$, где $S=\{s_1,\dots,s_n\}$, и $R=\{r_1,\dots,r_m\}$.

Мы будем обозначать образ образующей $s\in S$ при канонической проекции $F(S)\to G$ той же буквой s. Группа G обладает следующим замечательным свойством универсальности:

Теорема 5.10. *Пусть H — любая группа, имеющая образующие $f(s)$, где $s\in S$, и такая, что для любого элемента $s_1^{k_1}\dots s_m^{k_m}\in R$ в группе H выполнено равенство $f(s_1)^{k_1}\dots f(s_m)^{k_m}=e$. Тогда существует сюръективный гомоморфизм $\varphi:G\to H$ такой, что $\varphi(s)=f(s)$.*

Доказательство. Отображение $f:S\to H$ можно, очевидно, продолжить до сюръективного гомоморфизма $f:F(S)\to H$. Условия теоремы означают, что R лежит в ядре этого гомоморфизма. Положим $\tilde N=\operatorname{Ker}f$. Поскольку ядро любого гомоморфизма является нормальной подгруппой, то $N(R)\subseteq\tilde N$. Поэтому формула $\varphi(xN(R))=f(x)$ корректно определяет отображение $\varphi:G\to H$. То, что это отображение является сюръективным гомоморфизмом — очевидно. $\square$

В действительности, конструкция группы, заданной образующими и соотношениями, через свободную группу нужна лишь для того, чтобы доказать существование группы G, обладающей указанным свойством универсальности. Во всех приложениях используется именно это свойство группы, заданной образующими и соотношениями.

Пример 5.11. Пусть $S=\{s\}$ — одноэлементное множество. Тогда $F(S)$ — бесконечная циклическая группа, то есть $F(S)\cong\mathbb{Z}$. Пусть $R=\{s^n\}$ для некоторого натурального n. Тогда $\langle s\mid s^n=e\}=F(S)/N(R)\cong\mathbb{Z}/n\mathbb{Z}=\mathbb{Z}_n$.

Пример 5.12. Пусть $S = \{s, t\}$, $R = \{s^2, t^n, stst\}$. Докажем, что $\langle s, t \mid s^2 = e, t^n = e, stst = e\rangle \cong D_n$, где D_n — группа диэдра (группа симметрий правильного n-угольника).

Докажем сперва, что в группе $G = \langle s, t \mid s^2 = e, t^n = e, stst = e\rangle$ не более $2n$ элементов. Действительно, поскольку $s^2 = e = t^n$ в G, то любой элемент группы G можно записать в виде $t^{k_0}st^{k_1}s\ldots t^{k_{m-1}}st^{k_m}$, где $m \geqslant 0$, $0 \leqslant k_i < n$ $(i = 0, 1, \ldots, m)$ и $k_i > 0$ при $0 < i < n$. Далее, поскольку $stst = e$, то $st = t^{-1}s^{-1} = t^{n-1}s$. Отсюда $st^k = t^{n-k}s$. Поэтому каждый элемент группы G можно записать в виде t^ks^l, где $k \in \{0, 1, \ldots, n-1\}$ и $l \in \{0, 1\}$. Следовательно $|G| \leqslant 2n$.

Заметим, что мы еще не доказали, что $|G| = 2n$ (для этого нам пришлось бы доказать, что из наших соотношений *не следует* никакое соотношение вида $t^{k_1}s^{l_1} = t^{k_2}s^{l_2}$, где $k_1, k_2 \in \{0, 1, \ldots, n-1\}$, $l_1, l_2 \in \{0, 1\}$ и $k_1 \neq k_2$ или $l_1 \neq l_2$). Вот здесь нам и нужно свойство универсальности.

Обозначим через τ поворот правильного n-угольника на угол $2\pi/n$, а через σ — произвольную осевую симметрию, переводящую n-угольник в себя. Легко проверить, что эти преобразования порождают группу D_n, причем выполнены соотношения $\sigma^2 = \tau^n = \sigma\tau\sigma\tau$. Поэтому существует сюръективный гомоморфизм $\varphi : G \to D_n$, переводящий s в σ, а t в τ. Поскольку $|G| \leqslant 2n = |D_n|$, то φ — изоморфизм, то есть $G \cong D_n$.

Отметим, что $D_3 \cong S_3$. Действительно, занумеруем вершины правильного треугольника числами $1, 2, 3$. Каждый элемент группы D_3 переставляет вершины, то есть задает перестановку из S_3. Мы получаем гомоморфизм $D_3 \to S_3$. Легко видеть, что этот гомоморфизм инъективен (движение плоскости, оставляющее все вершины треугольника неподвижными, является тождественным). Кроме того, $|D_3| = 6 = |S_3|$. Поэтому эти группы изоморфны. Следовательно, $S_3 \cong \langle s, t \mid s^2 = e, t^3 = e, stst = e\rangle$.

Подведем некоторые итоги. Мы видели, что группы возникают естественным образом как группы преобразований (группы симметрий). Кроме того, группы можно задавать таблицами Кэли, можно рассматривать подгруппы и факторгруппы уже известных групп и, наконец, можно задавать группы образующими и соотношениями. Я хочу привести еще один рецепт построения новых групп.

Пусть $H_1, \ldots, H_n$ — некоторые группы. Их *прямым произведением* называется группа, элементами которой являются всевозможные строчки вида $(h_1, \ldots, h_n)$, где $h_i \in H_i$, а умножение определяется «покоординатно»: $(g_1, \ldots, g_n)(h_1, \ldots, h_n) = (g_1h_1, \ldots, g_nh_n)$. Эта группа обозначается через $H_1 \times \cdots \times H_n$. В случае, если все группы H_i являются абелевыми и для них используется аддитивная форма записи, их прямое произведение называют *прямой суммой* и обозначают $H_1 \oplus \cdots \oplus H_n$.

Упражнение 5.13. *Доказать, что* $\mathbb{Z}_2 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_6$, *но* $\mathbb{Z}_2 \oplus \mathbb{Z}_4 \ncong \mathbb{Z}_8$.

Лекция 6.

На предыдущих лекциях мы разобрали довольно много примеров групп. Возникает естественная задача: классифицировать все группы с точностью до изоморфизма, то есть предъявить такой список групп, что любая группа изоморфна одной и только одной группе из списка. Эта задача чудовищно сложная. Даже если ограничиться конечными группами, никакой надежды получить полную классификацию нет. Однако для конечных *абелевых групп* существует очень хорошая классификация, которой и посвящена сегодняшняя лекция.

Конечные абелевы группы

Все абелевы группы мы будем записывать аддитивно. Под произведением ng натурального числа n на элемент g абелевой группы мы понимаем сумму

$$\underbrace{g+g+\cdots+g}_{n \text{ раз}}.$$

Мы полагаем также $0g = 0$ (в правой части равенства 0 обозначает целое число, а в левой — нулевой элемент группы) и $(-n)g = -ng$ для натурального n.

Начнем с нескольких простых утверждений об абелевых группах.

Утверждение 6.1. *Пусть G — абелева группа, а n — целое число. Тогда отображение $\varphi_n : G \to G$, переводящее каждый элемент $g \in G$ в ng, является гомоморфизмом.*

Доказательство. Проверим это при натуральном n. Мы имеем

$$n(g+h) = \underbrace{(g+h)+\cdots+(g+h)}_{n \text{ раз}} = \underbrace{g+\cdots+g}_{n \text{ раз}} + \underbrace{h+\cdots+h}_{n \text{ раз}} = ng+nh.$$

Столь же просто разбираются и остальные случаи. □

Определение 6.2. Пусть A и B — подгруппы абелевой группы G. *Суммой* $A+B$ этих подгрупп называется порожденная ими подгруппа группы G. Ясно, что элемент g из G принадлежит $A+B$ тогда и только тогда, когда его можно представить в виде $g = a+b$ для некоторых $a \in A$, $b \in B$. Сумма подгрупп A и B называется прямой, если для любого $g \in A+B$ такое представление единственно.

Утверждение 6.3. *Пусть A и B — подгруппы абелевой группы G. Сумма подгрупп A и B является прямой в том и только в том случае, когда $A \cap B = \{0\}$.*

Доказательство. Пусть $A \cap B = \{0\}$. Предположим, что сумма подгрупп A и B не является прямой, то есть $a_1 + b_1 = a_2 + b_2$ для некоторых $a_1, a_2 \in A$ и $b_1, b_2 \in B$, причем либо $a_1 \neq a_2$, либо $b_1 \neq b_2$ (отсюда, впрочем, следует, что и $a_1 \neq a_2$, и $b_1 \neq b_2$). Тогда $a_1 - a_2 = b_1 - b_2 \in (A \cap B) \setminus \{0\}$. Полученное противоречие доказывает, что сумма подгрупп A и B является прямой.

Пусть теперь сумма подгрупп A и B является прямой. Предположим, что $A \cap B \neq \{0\}$. Выберем $g \in (A \cap B) \setminus \{0\}$. Тогда $g = g+0 = 0+g$ — два различных представления элемента $g \in A+B$ в виде суммы элемента из A и элемента из B. Полученное противоречие доказывает, что $A \cap B = \{0\}$. □

На прошлой лекции мы вводили понятие прямой суммы $A \oplus B$ двух групп A и B как множества пар (a, b), где $a \in A$, $b \in B$. Взаимосвязь этого понятия с понятием прямой суммы подгрупп раскрывается следующим утверждением.

Утверждение 6.4. *Пусть A и B — подгруппы абелевой группы G. Отображение $\varphi : A \oplus B \to A+B$, заданное формулой $\varphi(a,b) = a+b$, является гомоморфизмом групп. Оно является изоморфизмом тогда и только тогда, когда сумма подгрупп A и B является прямой.*

Доказательство. То, что φ является гомоморфизмом — очевидно. Столь же очевидно и то, что этот гомоморфизм сюръективен. Ядро этого гомоморфизма состоит, по определению, из всех пар (a,b), где $a \in A$, $b \in B$, таких, что $a+b=0$. Другими словами, $\operatorname{Ker}\varphi = \{(a,-a) \mid a \in A \cap B\}$. Теперь из утверждения 6.3 вытекает, что гомоморфизм φ инъективен тогда и только тогда, когда сумма подгрупп A и B является прямой. $\square$

Замечание. Доказанное утверждение позволяет отождествить прямую сумму подгрупп $A, B \subseteq G$ (иногда называемую «внутренней прямой суммой» и обозначаемую $A \dotplus B$) с их «внешней прямой суммой» $A \oplus B$.

Определение прямой суммы абелевых групп легко перенести со случая двух групп на случай нескольких групп: прямой суммой $H_1 \oplus \cdots \oplus H_m$ групп $H_1, \ldots, H_m$ называется множество последовательностей вида $(h_1, \ldots, h_m)$, где $h_i \in H_i$, с покомпонентным сложением. Сумма m подгрупп определяется очевидным образом; сумма подгрупп $A_1, \ldots, A_m \subseteq G$ называется прямой («внутренней прямой суммой»), если $A_i \cap \sum\limits_{j \neq i} A_j = \{0\}$. Очевидно, что внешняя прямая сумма $H_1 \oplus \cdots \oplus H_m$ групп $H_1, \ldots, H_m$ равна внутренней прямой сумме своих подгрупп $(H_1, 0, \ldots, 0), \ldots, (0, \ldots, 0, H_m)$.

Упражнение 6.5. *Сформулируйте и докажите аналоги утверждений 6.3 и 6.4 для нескольких подгрупп.*

Займемся теперь следующей задачей: когда абелева группа G изоморфна прямой сумме циклических групп $\mathbb{Z}_{n_1}, \ldots, \mathbb{Z}_{n_m}$?

Утверждение 6.6. *$G \cong \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_m}$ тогда и только тогда, когда в группе G найдутся элементы $g_1, \ldots, g_m$ такие, что порядок g_i равен n_i и любой элемент группы G можно однозначно представить в виде $g = \sum\limits_{i=1}^{m} a_i g_i$, где $0 \leqslant a_i < n_i$.*

Доказательство. Пусть $G \cong \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_m}$. Группа $\mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_m}$ равна внутренней прямой сумме своих циклических подгрупп порядков $n_1, \ldots, n_k$. Следовательно, то же верно и для G. Пусть $G = H_1 \dotplus \cdots \dotplus H_m$, где H_i — циклическая подгруппа порядка n_i, и пусть g_i — образующая подгруппы H_i. Тогда порядок g_i равен n_i и любой элемент группы G можно однозначно представить в виде $g = \sum\limits_{i=1}^{m} a_i g_i$, где $0 \leqslant a_i < n_i$.

С другой стороны, пусть в группе G найдутся элементы $g_1, \ldots, g_m$ такие, что порядок g_i равен n_i и любой элемент группы G можно однозначно представить в виде $g = \sum\limits_{i=1}^{m} a_i g_i$, где $0 \leqslant a_i < n_i$. Тогда группа G равна внутренней прямой сумме подгрупп, порожденных g_i, следовательно, G изоморфна внешней прямой сумме циклических групп порядков $n_1, \ldots, n_k$, то есть $G \cong \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_m}$. $\square$

Займемся теперь подгруппами циклической группы.

Утверждение 6.7. *Все подгруппы группы $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ (число n — натуральное) имеют вид $d\mathbb{Z}_{p^k} = \{da \mid a \in \mathbb{Z}_n\}$, где d — делитель числа n. При этом $d\mathbb{Z}_n = \{x \in \mathbb{Z}_n \mid \frac{n}{d}x = 0\}$.*

Доказательство. Пусть H — подгруппа группы $\mathbb{Z}_n$, и $d \in \mathbb{N}$ — минимальное натуральное число такое, что его образ в $\mathbb{Z}_n$ лежит в H. Тогда d делит n (поскольку образ в $\mathbb{Z}_n$ остатка при делении n на d лежит в H). Поэтому $H = d\mathbb{Z}_n$. То, что $d\mathbb{Z}_n = \{x \in \mathbb{Z}_n \mid \frac{n}{d}x = 0\}$, следует из очевидного равенства $d\mathbb{Z} = \{k \in \mathbb{Z} \mid \frac{n}{d}k \in n\mathbb{Z}\}$. $\square$

Утверждение 6.8. *$\mathbb{Z}_n \cong \mathbb{Z}_{d_1} \oplus \dots \oplus \mathbb{Z}_{d_m}$ тогда и только тогда, когда $n = d_1 d_2 \dots d_m$ и числа $d_1, \dots, d_m$ попарно взаимно просты.*

Доказательство. Число элементов в $\mathbb{Z}_n$ равно n, а число элементов в $\mathbb{Z}_{d_1} \oplus \dots \oplus \mathbb{Z}_{d_m}$ равно $d_1 d_2 \dots d_m$. Отсюда следует необходимость условия $n = d_1 d_2 \dots d_m$.

Пусть это условие выполнено. Заметим, что порядок элемента $(a_1, \dots, a_m) \in \mathbb{Z}_{d_1} \oplus \dots \oplus \mathbb{Z}_{d_m}$ равен наименьшему общему кратному порядков $a_i \in \mathbb{Z}_{n_i}$, что не превосходит наименьшего общего кратного чисел $d_1, \dots, d_m$. Поэтому, если не все из этих чисел попарно взаимно просты, то порядок любого элемента группы $\mathbb{Z}_{d_1} \oplus \dots \oplus \mathbb{Z}_{d_m}$ меньше произведения чисел $d_1, \dots, d_m$, то есть n. В этом случае, очевидно, $\mathbb{Z}_n \ncong \mathbb{Z}_{d_1} \oplus \dots \oplus \mathbb{Z}_{d_m}$.

С другой стороны, если числа $d_1, \dots, d_m$ попарно взаимно просты, то порядок элемента $(1, \dots, 1) \in \mathbb{Z}_{d_1} \oplus \dots \oplus \mathbb{Z}_{d_m}$ равен n. Тогда $\mathbb{Z}_n \cong \mathbb{Z}_{d_1} \oplus \dots \oplus \mathbb{Z}_{d_m}$. $\square$

Теперь мы готовы к тому, чтобы сформулировать и доказать основную теорему сегодняшней лекции.

Теорема 6.9. *Всякая конечная абелева группа изоморфна и притом только одной группе вида*

$$\mathbb{Z}_{p_1^{k_1}} \oplus \dots \oplus \mathbb{Z}_{p_m^{k_m}},$$

где все числа p_i являются простыми, $p_1 \geqslant \ldots \geqslant p_m$ и $k_i \geqslant k_{i+1}$ при $p_i = p_{i+1}$.

Доказательство опирается на следующее утверждение:

Лемма 6.9.1. *Пусть существует такое простое число p, что для любого элемента $g \in G$ найдется такое натуральное число k, что $p^k g = 0$. Тогда G изоморфна группе вида*

$$\mathbb{Z}_{p^{k_1}} \oplus \dots \oplus \mathbb{Z}_{p^{k_m}},$$

где $k_1 \geqslant \ldots \geqslant k_m$, и притом только одной.

Доказательство. Отметим, прежде всего, что порядок каждого элемента из G является степенью p. Действительно, если $g \in G$ и, следовательно, $p^k g = 0$ для некоторого $k \in \mathbb{N}$, то порядок g должен делить p^k, то есть сам являться степенью p.

Воспользуемся индукцией по числу элементов G. При $|G| = 1$ доказывать нечего. Пусть $|G| > 1$. Выберем в G элемент g_1 максимального порядка p^{k_1}. Обозначим через H циклическую подгруппу G, порожденную элементом g_1. Очевидно, что $H \cong \mathbb{Z}_{p^{k_1}}$.

Подгруппа $H \subseteq G$ является нормальной (поскольку группа G абелева). Рассмотрим фактор-группу $\overline{G} = G/H$. Для любого $\overline{g} = g + H \in G/H$ мы имеем $p^{k_1}\overline{g} = p^{k_1}g + H = H = \overline{0}$ (поскольку порядок каждого элемента группы G не превосходит p^{k_1}). По предположению индукции, группа $\overline{G}$ изоморфна группе вида $\mathbb{Z}_{p^{k_2}} \oplus \dots \oplus \mathbb{Z}_{p^{k_m}}$. Это означает, что в ней есть элементы $\overline{g}_2, \overline{g}_3, \dots, \overline{g}_m$ такие, что порядок $\overline{g}_i$ равен p^{k_i} и любой элемент группы $\overline{G}$ однозначно представляется в виде

$$\overline{g} = \sum_{i=2}^{m} a_i \overline{g}_i, \tag{16}$$

где $0 \leqslant a_i \leqslant p^{k_i}$. Докажем, что в G есть такие элементы $g_1, \dots, g_m$, что порядок g_i равен p^{k_i} и любой элемент группы G однозначно представляется в виде

$$g = \sum_{i=1}^{m} a_i g_i, \tag{17}$$

где $0 \leqslant a_i \leqslant p^{k_i}$.

Элемент g_1 порядка p^{k_1} у нас уже есть. Докажем, что среди прообразов элемента $\overline{g}_i$ при канонической проекции $G \to G/H$ найдется элемент порядка p^{k_i} $(i = 2, \dots, m)$.

Пусть g — произвольный прообраз $\overline{g}_i$. Поскольку порядок $\overline{g}_i$ равен p^{k_i}, то $p^{k_i} g \in H$. Поскольку p^{k_1} — максимальный из порядков элементов группы G, то $p^{k_1} g = 0$. Поэтому $p^{k_i} g \in \{x \in H \mid p^{k_1 - k_i} x = 0\} = p^{k_i} H$ (в силу того, что $H \cong \mathbb{Z}_{p^{k_1}}$, и утверждения 6.7), то есть $p^{k_i} g = p^{k_i} h$ для некоторого $h \in H$. Положим $g_i = g - h$. Ясно, что порядок g_i равен p^{k_i} и образ g_i при канонической проекции на $\overline{G}$ равен $\overline{g}_i$.

Докажем теперь, что каждый элемент группы G представляется в виде (17). Действительно, пусть $g \in G$. Рассмотрим его образ $\overline{g}$ в $\overline{G}$ и представим его в виде (16). Тогда

$$g - \sum_{i=2}^{m} a_i g_i \in H.$$

Следовательно, эта разность равна $a_1 g_1$ для некоторого $a_1 \in \{0, \dots, p^{k_1} - 1\}$. Таким образом, g может быть представлен в виде (17).

Докажем, что это представление однозначно. Действительно, если g представлен в виде (17), то для его образа $\overline{g}$ в $\overline{G}$ выполнено равенство (16) и, следовательно, коэффициенты $a_2, \dots, a_m$ определены однозначно. Но тогда и коэффициент a_1 определен однозначно. Поэтому

$$G \cong \mathbb{Z}_{p^{k_1}} \oplus \dots \oplus \mathbb{Z}_{p^{k_m}}.$$

Докажем теперь, что числа $k_1, \dots k_m$ однозначно определяются группой G. Найдем в группе $\mathbb{Z}_{p^{k_1}} \oplus \dots \oplus \mathbb{Z}_{p^{k_m}}$ число $N_l(k_1, \dots, k_m)$ элементов, порядок которых не больше p^l (где $l \in \mathbb{N}$).

Порядок элемента $(a_1, \dots, a_m) \in \mathbb{Z}_{p^{k_1}} \oplus \dots \oplus \mathbb{Z}_{p^{k_m}}$ равен наименьшему общему кратному порядков элементов $a_1 \in \mathbb{Z}_{p^{k_1}}$, ..., $a_m \in \mathbb{Z}_{p^{k_m}}$. Чтобы этот порядок был не больше p^l, необходимо и достаточно, чтобы порядок каждого из a_i был не больше p^l. Число элементов $a_i \in \mathbb{Z}_{p^{k_i}}$ порядка не большего p^l равно p^l, если $l \leqslant k_i$, и p^{k_i}, если $l > k_i$. Пусть $r(l)$ — минимальное натуральное число, для которого $k_{r(l)} \geqslant l$. Тогда $N_l(k_1, \dots, k_m) = p^{C_l(k_1, \dots, k_m)}$, где

$$C_l(k_1, \dots, k_m) = l r(l) + \sum_{s=r(l)+1}^{m} k_s.$$

Отметим, что $C_l(k_1, \dots, k_m) - C_{l-1}(k_1, \dots, k_m) = r(l)$, а набор чисел $r(l)$ для всех $l \in \mathbb{N}$ однозначно определяет набор k_i. Таким образом, числа $k_1, \dots k_m$ однозначно определяются информацией о том, сколько в группе G элементов порядка p^l $(l = 1, 2, \dots)$.

Лемма доказана. $\square$

Вернемся к доказательству теоремы.

Пусть G — произвольная конечная абелева группа и $n = |G|$. Воспользуемся индукцией по n.

Если $n = 1$, то доказывать нечего. Предположим, что $n > 1$ и для всех групп с меньшим числом элементов утверждение теоремы выполняется. Докажем его для группы G.

Пусть p — такое простое число, что в группе G есть элементы порядка p (в качестве p можно взять любой простой делитель порядка произвольного ненулевого элемента группы G). Рассмотрим умножение на p как гомоморфизм группы G в себя. Этот гомоморфизм имеет ненулевое ядро (так как в группе G есть элементы порядка p), поэтому образ этого гомоморфизма не совпадает со всей группой G (по теореме Лагранжа и теореме о гомоморфизмах групп произведение числа элементов в ядре гомоморфизма на число элементов в его образе равно порядку группы G).

Рассмотрим в G последовательность подгрупп $G \supset pG \supseteq p^2 G \supseteq \dots$, и найдем минимальное число k, для которого $p^k G = p^{k+1} G$ (такое число найдется в силу конечности группы G). Умножение на p задает гомоморфизм подгруппы $p^k G$ в себя, образом которого является вся эта подгруппа. Следовательно, ядро этого гомоморфизма $p^k G \to p^k G$ нулевое, то есть в $p^k G$ нет элементов порядка p. Поэтому порядок любого элемента $h \in H$ не делится на p (если бы порядок h был равен lp, то порядок lh равнялся бы p).

Рассмотрим теперь гомоморфизм $\varphi : G \to p^k G$, переводящий каждый элемент $g \in G$ в $p^k g$. Обозначим через H ядро этого гомоморфизма. Мы имеем равенство $|G| = |H| \cdot |p^k G|$ (поскольку $p^k G = \varphi(G)$). Кроме того, $H \cap p^k G = \{0\}$ (поскольку порядок любого элемента из H делит p^k, то есть равен степени числа p). Поэтому сумма подгрупп H и $p^k G$ — прямая, то есть $H + p^k G \cong H \oplus p^k G$. Число элементов в последней группе равно $|H| \cdot |p^k G| = |G|$, поэтому $G = H \dot{+} p^k G$. Согласно лемме 6.9.1, группа H изоморфна прямой сумме вида, требуемого в утверждении теоремы. В группе $p^k G$ элементов меньше, чем в группе G, так что по предположению индукции она тоже изоморфна прямой сумме вида, требуемого в утверждении теоремы. Поэтому то же верно и для группы $G \cong H \oplus p^k G$.

Осталось доказать единственность. Отметим, что число элементов порядка p^l (где p — простое и $l \in \mathbb{N}$) в группе $\mathbb{Z}_{p_1^{k_1}} \oplus \dots \oplus \mathbb{Z}_{p_m^{k_m}}$ равно числу элементов такого порядка в прямой сумме лишь тех из $\mathbb{Z}_{p_i^{k_i}}$, для которых $p_i = p$. А для такой прямой суммы информация о числе элементов порядка p^l позволяет восстановить показатели k_i (смотри доказательство леммы 6.9.1). Поэтому все числа p_i и k_i однозначно определяются группой G. $\square$

Следствие 6.10. *Любая конечная абелева группа G изоморфна группе вида*

$$\mathbb{Z}_{n_1} \oplus \dots \oplus \mathbb{Z}_{n_m},$$

где $n_1, \dots, n_m \in \mathbb{N}$ такие, что n_i делится на n_{i+1} для любого $i = 1, \dots, m-1$.

Доказательство. Представим группу G в виде прямой суммы циклических групп, порядок каждой из которых — степень простого числа (по теореме 6.9). Запишем это представление в виде

$$G \cong \mathbb{Z}_{p_1^{k_1^{(1)}}} \oplus \dots \oplus \mathbb{Z}_{p_1^{k_{m_1}^{(1)}}} \oplus \dots \oplus \mathbb{Z}_{p_l^{k_1^{(l)}}} \oplus \dots \oplus \mathbb{Z}_{p_l^{k_{m_l}^{(l)}}},$$

где все числа p_i являются простыми, $p_1 > \dots > p_l$ и $k_1^{(j)} \geqslant \ldots \geqslant k_{m_j}^{(j)} > 0$ для любого $j = 1, \dots, l$. Пусть $n_i = \prod\limits_{j : m_j \geqslant i} p_j^{k_i^{(j)}}$. Тогда

$$G \cong \mathbb{Z}_{n_1} \oplus \dots \oplus \mathbb{Z}_{n_m},$$

где $m = \max\limits_{1 \leqslant i \leqslant l} m_i$. Ясно, что n_i делится на n_{i+1} для любого $i = 1, \dots, m-1$.

Доказательство единственности я оставляю в качестве упражнения. $\square$

Лекция 7.

Кольца, идеалы и факторкольца

Мы будем рассматривать только ассоциативные кольца.

Подмножество $Q \subseteq R$ кольца R называется *подкольцом*, если оно замкнуто относительно сложения и умножения. Отметим, что подкольцо всегда является кольцом, подкольцо коммутативного кольца является коммутативным, но подкольцо кольца с единицей может не быть кольцом с единицей. Например, в кольце целых чисел $\mathbb{Z}$ любая аддитивная подгруппа (то есть подгруппа $\mathbb{Z}$, как абелевой группы по сложению) является подкольцом, но из них лишь $\mathbb{Z}$ и $\{0\}$ являются кольцами с единицей, причем у последнего единица не совпадает с единицей объемлющего кольца $\mathbb{Z}$.

Пусть R и Q — кольца. Отображение $\varphi : R \to Q$ называется *гомоморфизмом колец*, если $\varphi(a+b) = \varphi(a)+\varphi(b)$ и $\varphi(ab) = \varphi(a)\varphi(b)$ для любых $a, b \in R$. *Ядром* гомоморфизма колец $\varphi : R \to Q$ называется $\varphi^{-1}(0)$, то есть ядро в смысле гомоморфизма абелевых групп по сложению. Очевидно, что ядро и образ гомоморфизма являются подкольцами соответственно в R и Q. Так же, как и для групп, образом гомоморфизма может быть любое подкольцо, но совсем не любое подкольцо может быть ядром гомоморфизма.

Пусть $\varphi : R \to Q$ — гомоморфизм колец, $x \in I = \operatorname{Ker} \varphi$. Тогда $\varphi(ax) = \varphi(a)\varphi(x) = \varphi(a) \cdot 0 = 0$ для любого $a \in R$. Аналогично, $\varphi(xa) = 0$ для любого $a \in R$. Таким образом, $ax \in I$ и $xa \in I$ для любого $a \in R$. Это можно записать так: $RI \subseteq I$ и $IR \subseteq I$. Отметим, что если R — кольцо с единицей, то включения можно заменить на равенства: $RI = I$ и $IR = I$.

Определение 7.1. Пусть R — кольцо. Подкольцо $I \subseteq R$ называется *идеалом*, если $RI \subseteq I$ и $IR \subseteq I$.

Как мы только что проверили, ядро любого гомоморфизма является идеалом. Чуть позже мы убедимся и в обратном — что каждый идеал является ядром некоторого гомоморфизма.

Замечание. Если кольцо R не является коммутативным, то имеет смысл рассматривать подкольца $A \subseteq R$, удовлетворяющие одному условию: $RA \subseteq A$ — *левые идеалы*, или $AR \subseteq A$ — *правые идеалы*. В отличие от правых и левых идеалов, просто идеалы в некоммутативном кольце часто называются *двусторонними идеалами*.

Пусть I — идеал кольца R. Рассмотрим абелеву группу R/I — факторгруппу аддитивной группы поля по подгруппе I. Для каждого $a \in R$ обозначим через $\overline{a}$ смежный класс $a+I$. Положим $\overline{a}\overline{b} = \overline{ab}$. Это определение не зависит от представителей смежных классов $\overline{a}$ и $\overline{b}$. Действительно, $(a + I)(b + I) \subseteq (ab + aI + Ib + II) \subseteq (ab + I)$.

Легко проверить, что введенное таким образом умножение превращает R/I в кольцо. Оно называется *факторкольцом* кольца R по идеалу I. Из определения ясно, что каноническая проекция $\pi : R \to R/I$ является гомоморфизмом колец, причем $I = \operatorname{Ker} \pi$. Очевидно также, что любое факторкольцо коммутативного кольца коммутативно, а любое факторкольцо кольца с единицей является тоже кольцом с единицей.

Если $I = R$, то факторкольцо R/I изоморфно тривиальному кольцу $\{0\}$. Отсюда видно, почему требование $1 \neq 0$ не следует включать в определение кольца с единицей.

Теорема 7.2 (О гомоморфизмах колец). *Пусть $\varphi : R \to Q$ — произвольный гомоморфизм колец. Обозначим через I ядро этого гомоморфизма, через π — каноническую проекцию $R \to R/I$. Тогда существует единственный гомоморфизм колец $\psi : R/I \to Q$, делающий диаграмму*

$$\begin{tikzcd} R \arrow[rr, "\varphi"] \arrow[dr, "\pi"'] & & Q \\ & R/I \arrow[ur, "\psi"'] & \end{tikzcd}$$

коммутативной. При этом ψ является изоморфизмом R/I на $\varphi(R)$.

Доказательство. Отображение ψ существует и единственно по теореме о факторизации отображений. По теореме о гомоморфизмах групп оно является гомоморфизмом аддитивной группы кольца R/I в аддитивную группу кольца Q. То, что ψ — гомоморфизм колец, проверяется столь же просто. Действительно, для любых $a, b \in R$ мы имеем $\psi(\overline{a}\overline{b}) = \psi(\overline{ab}) = \varphi(ab) = \varphi(a)\varphi(b) = \psi(\overline{a})\psi(\overline{b})$. □

Далее в этой лекции мы будем рассматривать только коммутативные кольца.

Пример 7.3. Пусть $R = \mathbb{Z}$ — кольцо целых чисел. Подкольцо $n\mathbb{Z}$ является, очевидно, идеалом кольца $\mathbb{Z}$. Поэтому группу $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ классов вычетов по модулю n можно рассматривать как кольцо.

Название «кольцо классов вычетов» произошло из теории чисел. Два целых числа k и m называются *сравнимыми по модулю* n, если их разность делится на n. Сравнения записываются так:

$$k \equiv m \pmod n.$$

Числа, сравнимые по модулю n, называются (по отношению друг к другу) *вычетами по модулю* n. Соответственно, все числа, сравнимые с данным числом (а, следовательно, сравнимые и друг с другом), образуют *класс вычетов по модулю* n.

Кольца классов вычетов часто используются для доказательства неразрешимости уравнений в целых числах. Рассмотрим, например, уравнение $x^2 - y^2 = 154$. Пусть оно имеет решение в целых числах: $x = a$, $y = b$. Поскольку каноническая проекция $\pi : \mathbb{Z} \to \mathbb{Z}_4$ является гомоморфизмом колец, то из равенства $a^2 - b^2 = 154$ в кольце $\mathbb{Z}$ следует равенство $\overline{a}^2 - \overline{b}^2 = \overline{154}$. Однако в кольце $\mathbb{Z}_4$ лишь $\overline{0}$ и $\overline{1}$ являются квдратами, поэтому $\overline{154} = \overline{2}$ невозможно представить как разность квадратов в $\mathbb{Z}_4$. Следовательно, уравнение $x^2 - y^2 = 154$ неразрешимо в целых числах.

Теорема 7.4. *Пусть p — простое число. Тогда кольцо $\mathbb{Z}_p$ является полем.*

Доказательство. То, что единица в $\mathbb{Z}_p$ не равна нулю, очевидно. Пусть $k \in \mathbb{Z}$ не кратно p, то есть $\overline{k} \in (\mathbb{Z}_p \setminus \{\overline{0}\})$. Обозначим через ν_k отображение $\mathbb{Z}_p \to \mathbb{Z}_p$, задаваемое формулой $\nu_k(\overline{a}) = \overline{k}\overline{a}$. Очевидно, что это групповой гомоморфизм аддитивной группы $\mathbb{Z}_p$ в себя. Если $\overline{a} \neq \overline{0}$, то есть a не делится на p, то и произведение ka не делится на p, поэтому $\overline{k}\overline{a} \neq 0$. Следовательно, $\operatorname{Ker} \nu_k = \{\overline{0}\}$, то есть гомоморфизм ν_k инъективен. Однако инъективное отображение конечного множества в себя является биекцией. Поэтому, в частности, найдется $\overline{a} \in \mathbb{Z}_p$ такое, что $\overline{k}\overline{a} = \overline{1}$. Следовательно, все ненулевые элементы $\mathbb{Z}_p$ обратимы, то есть $\mathbb{Z}_p$ является полем. □

Множество классов вычетов по простому модулю p, рассматриваемое как поле, а не как абелева группа, обычно обозначают через $\mathbb{F}_p$. Вообще, под $\mathbb{F}_q$ понимают конечное поле, состоящее из q элементов. Такие поля бывают не для всех q, а лишь для $q = p^n$, где p — простое, а n — произвольное натуральное число. К этому мы вернемся на следующих лекциях.

Пока же рассмотрим $\mathbb{F}_p^*$ — мультипликативную группу поля $\mathbb{F}_p$. Порядок этой группы равен $p - 1$. По теореме Лагранжа, порядок каждого элемента $\mathbb{F}_p^*$ делит $p - 1$, то есть $\overline{a}^{p-1} = \overline{1}$ для любого $\overline{a} \in \mathbb{F}_p^*$. Домножая обе части равенства на $\overline{a}$, получаем равенство $\overline{a}^p = \overline{a}$, верное уже для любого $\overline{a} \in \mathbb{F}_p$. Получилась

Теорема 7.5 (Малая теорема Ферма). *Пусть p — простое число. Тогда $a^p \equiv a \pmod p$ для любого $a \in \mathbb{Z}$.*

Пример 7.6. Рассмотрим кольцо многочленов $R = \mathbb{R}[x]$, и рассмотрим в нем подмножество I, состоящее из многочленов, делящихся на $x^2 + 1$. Очевидно, что I является идеалом. Рассмотрим факторкольцо $A = R/I$. Поскольку каждый многочлен $f(x) \in R$ сравним по модулю $x^2 + 1$ с единственным линейным многочленом от x (остатком при делении $f(x)$ на $x^2 + 1$), то любой элемент кольца A однозначно записывается в виде $(a\overline{1} + b\overline{x})$, где $a, b \in \mathbb{R}$. Умножение в кольце A устроено так: $(a\overline{1}+b\overline{x})(c\overline{1}+d\overline{x}) = (ac-bd)\overline{1}+(ad+bc)\overline{x})$. Отсюда видно, что существует изоморфизм $A \xrightarrow{\sim} \mathbb{C}$, переводящий $\overline{1}$ в 1, а $\overline{x}$ — в i.

Пример 7.7. Рассмотрим теперь кольцо многочленов $R = \mathbb{F}_3[x]$. Элементы поля $\mathbb{F}_3$ мы будем обозначать через 0, 1 и -1, безо всяких черточек сверху. Обозначим через I идеал в R, состоящий из всех многочленов, делящихся на x^2+1. Как и в предыдущем примере, легко проверить, что любой элемент факторкольца $A = R/I$ однозначно записывается в виде $(a\overline{1}+b\overline{x})$, где $a, b \in \mathbb{F}_3$. Докажем, что A является полем.

Рассмотрим $\overline{f} = a\overline{1}+b\overline{x} \in A$. Мы имеем $(a\overline{1}+b\overline{x})(a\overline{1}-b\overline{x}) = a^2+b^2$. Однако в поле $\mathbb{F}_3$ квадрат любого ненулевого элемента равен 1, поэтому $a^2+b^2 = 0$ тогда и только тогда, когда и $a = 0$, и $b = 0$. Поэтому для любого ненулевого $\overline{f} = a\overline{1}+b\overline{x}$ существует обратный

$$(\overline{f})^{-1} = \frac{a}{a^2+b^2}\overline{1} - \frac{b}{a^2+b^2}\overline{x}.$$

Итак, A является полем. Поскольку аддитивная группа кольца A изоморфна $\mathbb{Z}_3 \oplus \mathbb{Z}_3$, то число элементов A равно 9. Таким образом, мы построили поле $\mathbb{F}_9$.

Евклидовы кольца

Далее слово «кольцо» будет обозначать коммутативное ассоциативное кольцо с единицей.

В действительности, мы будем изучать прежде всего кольцо $\mathbb{Z}$ целых чисел и кольцо $\Bbbk[x]$ многочленов над полем $\Bbbk$. Эти кольца по своим свойствам очень похожи, что позволяет не рассматривать их по отдельности, но вести изложение в более абстрактных терминах, для произвольного кольца R, удовлетворяющего нужным нам свойствам. Дадим необходимые определения.

Определение 7.8. Пусть R — произвольное кольцо. Элемент $a \in R$ называется *обратимым*, если он имеет обратный по умножению. Ненулевой элемент $d \in R$ называется *делителем нуля*, если существует ненулевой элемент $c \in R$ такой, что $cd = 0$.

Легко видеть, что произведение обратимых элементов обратимо, то есть обратимые элементы кольца R образуют группу по умножению. Эта группа обозначается через R^*. Делитель нуля не может быть обратим. Действительно, пусть d обратим и $cd = 0$. Тогда $c = cd \cdot d^{-1} = 0$, то есть d не является делителем нуля.

Упражнение 7.9. *Пусть $R = \mathbb{Z}_{12}$. Проверьте, что элементы $\overline{1}$, $\overline{5}$, $\overline{7}$ и $\overline{11}$ являются обратимыми, а остальные ненулевые элементы кольца R являются делителями нуля. Является ли группа R^* циклической?*

Определение 7.10. Кольцо R называется *целостностным*, или *областью целостности*, если в нем нет делителей нуля и $1 \neq 0$.

Пример 7.11. Кольца $\mathbb{Z}$, $\Bbbk[x]$, а также любое поле $\Bbbk$ являются областями целостности.

Определение 7.12. Область целостности R называется *евклидовым кольцом*, если на $R \setminus \{0\}$ существует такая функция δ со значениями в множестве $\mathbb{N}$ натуральных чисел (мы будем называть $\delta(a)$ *нормой* a), что

1) $\delta(ab) \geqslant \delta(a)$ для любых $a, b \in R \setminus \{0\}$.
2) Для любых $a \in R$ и $b \in R \setminus \{0\}$ найдутся $q, r \in R$ такие, что $a = qb + r$, причем либо $r = 0$, либо $\delta(r) < \delta(b)$ (деление с остатком).

Пример 7.13. Кольцо целых чисел является евклидовым относительно нормы $\delta(a) = |a|$. Кольцо многочленов над полем является евклидовым относительно нормы $\delta(f) = \deg f + 1$.

Евклидовы кольца названы так потому, что в них применим алгоритм Евклида вычисления наибольшего общего делителя.

Определение 7.14. Элемент $k \in R$ называется *делителем* элемента $a \in R$, если $a = ck$ для некоторого $c \in R$. Элемент $d \in R$ называется *наибольшим общим делителем* элементов $a, b \in R$, если d является их общим делителем (то есть делителем как a, так и b), и любой общий делитель a и b является также делителем d. То, что d является наибольшим общим делителем a и b, записывают так: $d = (a, b)$.

В произвольном кольце R наибольший общий делитель совсем не обязан существовать. Однако в евклидовом кольце существование наибольшего общего делителя двух произвольных элементов можно доказать, используя алгоритм Евклида:

Пусть R — евклидово кольцо, $a, b \in R \setminus \{0\}$. Поделим с остатком a на b: $a = q_1 b + r_1$. Далее, поделим с остатком b на r_1: $b = q_2 r_1 + r_2$. Продолжим этот процесс, пока очередной остаток не будет делителем предыдущего (это неизбежно случится, ибо в противном случае мы получили бы бесконечную убывающую последовательность натуральных чисел $\delta(b), \delta(r_1), \delta(r_2), \ldots$). Мы получим последовательность равенств

$$a = q_1 b + r_1, \tag{18}$$
$$b = q_2 r_1 + r_2, \tag{19}$$
$$r_1 = q_3 r_2 + r_3, \tag{20}$$
$$\ldots$$
$$r_{n-2} = q_n r_{n-1} + r_n, \tag{21}$$
$$r_{n-1} = q_{n+1} r_n. \tag{22}$$

Докажем, что r_n является наибольшим общим делителем a и b.

Из равенства (22) следует, что r_n является делителем r_{n-1}. Следовательно, по равенству (21), r_n делит также и r_{n-2}. Поднимаясь вверх по цепочке равенств, мы получаем, что r_n делит b и a, то есть r_n является общим делителем a и b.

Пусть c — произвольный общий делитель a и b. Из равенства (18) следует, что c делит также и r_1. Спускаясь вниз по цепочке равенств, устанавливаем, что c делит все остатки $r_1, r_2, \ldots, r_n$. Следовательно, r_n делится на любой общий делитель a и b, то есть r_n является наибольшим общим делителем a и b.

Важным следствием алгоритма Евклида является следующий факт: если d — наибольший общий делитель ненулевых элементов a и b евклидова кольца R, то $d = ka + lb$ для некоторых $k, l \in R$. Действительно, пусть наибольший общий делитель получается применением алгоритма Евклида. По равенству (18), $r_1 = k_1 a + l_1 b$, где $k_1 = 1, l_1 = -q_1$. Подставляя это выражение вместо r_1 в равенство (19), получаем $r_2 = k_2 a + l_2 b$, где $k_2 = -q_2 k_1, l_2 = 1 - q_2 l_1$. Продолжая этот процесс, получаем искомое выражение $r_n = k_n a + l_n b$.

Заметим теперь, что любой наибольший общий делитель d элементов a и b делится на r_n. Следовательно, $d = e r_n = ka + lb$, где $k = e k_n, l = e l_n$.

Лекция 8.

Теория делимости в кольцах главных идеалов

В этой лекции слово «кольцо» будет обозначать коммутативное ассоциативное кольцо с единицей.

Утверждение 8.1. *Пусть кольцо R евклидово и $d \in R \setminus \{0\}$.*

1) Предположим, что $\delta(da) = \delta(a)$ для некоторого $a \in R \setminus \{0\}$. Тогда элемент d обратим.

2) Элемент d обратим тогда и только тогда, когда $\delta(d) = \delta(1)$.

Доказательство. 1) Разделим a на da с остатком: $a = qda + r$, где $r = 0$ или $\delta(r) < \delta(a)$. Мы имеем $r = (1-qd)a$, поэтому неравенство $\delta(r) < \delta(a)$ невозможно, следовательно, $r = 0$. Поскольку R — область целостности, отсюда следует, что $1 - qd = 0$, то есть $qd = 1$ и d обратим.

2) Из определения евклидова кольца очевидно, что для любого $a \in R\setminus\{0\}$ выполнено неравенство $\delta(a) \geqslant \delta(1)$. Поэтому, если $\delta(d) = \delta(1)$, то 1 делится на d без остатка, то есть d обратим. С другой стороны, если d обратим, то $\delta(1) = \delta(dd^{-1}) \geqslant \delta(d)$, поэтому $\delta(d) = \delta(1)$. □

Определение 8.2. Идеал I в кольце R называется *главным*, если найдется такой элемент $a \in R$, что $I = aR$. Главный идеал aR обозначается также через (a). Кольцо R называется *кольцом главных идеалов*, если оно является областью целостности и любой идеал в нем — главный.

Утверждение 8.3. *Если кольцо R евклидово, то оно является кольцом главных идеалов.*

Доказательство. Пусть I — некоторый идеал в евклидовом кольце R. Если он равен $\{0\}$, то он главный: $I = (0)$. В противном случае рассмотрим непустое множество натуральных чисел $D = \{\delta(x) \mid x \in I, x \neq 0\}$. Любое непустое множество натуральных чисел имеет минимальный элемент. Пусть $b \in I$ таково, что $\delta(b) = \min(D)$. Рассмотрим произвольный элемент $a \in I$. Поделим его на b с остатком: $a = qb + r$, где либо $r = 0$, либо $\delta(r) < \delta(b)$. Однако $r = a - qb \in I$, поэтому $r = 0$, то есть $a = qb$. Следовательно, $I \subseteq (b)$. С другой стороны, I — идеал и $b \in I$, поэтому $(b) \subseteq I$. Таким образом $I = (b)$ — главный идеал. □

Утверждение 8.4. *Пусть R — кольцо главных идеалов. Тогда для любых $a, b \in R$ существует их наибольший общий делитель (a, b).*

Доказательство. Идеал $(a) + (b)$ — главный. Пусть $(a) + (b) = (d)$. Тогда $a = \alpha d$ и $b = \beta d$ для некоторых $\alpha, \beta \in I$, то есть d является общим делителем a и b. С другой стороны, для любого k, являющегося общим делителем a и b, элементы a и b лежат в (k), поэтому $(d) = (a) + (b) \subseteq (k)$, то есть k является делителем d. Следовательно, $d = (a, b)$. □

Как мы видели на прошлой лекции, факторкольцо $\mathbb{Z}/p\mathbb{Z}$ является полем, если p — простое число. Прежде, чем установить подобную взаимосвязь для произвольного кольца главных идеалов, исследуем в общем виде вопрос: при каких условиях на идеал $I \subseteq R$ факторкольцо R/I является полем?

Определение 8.5. Идеал I в кольце R называется *максимальным*, если он не равен всему R, а любой строго содержащий I идеал совпадает с R.

Утверждение 8.6. *1) Идеал I совпадает со всем кольцом тогда и только тогда, когда он содержит единицу.*

2) Факторкольцо R/I является полем тогда и только тогда, когда идеал I максимален.

Доказательство.

1). Ясно, что если I совпадает с R, то он содержит единицу. Пусть наоборот, $1 \in I$. Тогда, поскольку I — идеал, $R \cdot 1 \subseteq I$, но $R \cdot 1 = R$, поэтому $I = R$.

2). Пусть идеал I максимален. Тогда $1 \neq 0$ в факторкольце R/I, поскольку $I \neq R$. Рассмотрим произвольный элемент $a \in R \setminus I$. Идеал $J = aR + I$ строго содержит I, поэтому $J = R$, то есть найдется $b \in R$ такой, что $1 \in ab + I$. Это означает, что образ элемента a при канонической проекции $R \to R/I$ обратим. Поэтому R/I — поле.

В обратную сторону, пусть R/I — поле. Тогда $1 \neq 0$ в R/I, поэтому $I \neq R$. Пусть идеал $J \subseteq R$ строго содержит I. Выберем $a \in J \setminus I$. Образ элемента a при канонической проекции $R \to R/I$ обратим, поэтому найдется $b \in R$ такой, что $1 \in ab + I$. Это означает, что $aR + I = R$, поэтому тем более $J = R$. Следовательно, идеал I максимален. □

Определение 8.7. Пусть R — произвольное кольцо. Необратимый элемент $p \in R$ называется *простым* или *неприводимым*, если из разложения $p = ab$ следует, что либо a, либо b обратим.

Теорема 8.8. *Пусть R — кольцо главных идеалов. Элемент $p \in R$ является неприводимым тогда и только тогда, когда $R/(p)$ — поле.*

Доказательство. По утверждению 8.6 достаточно проверить, что идеал (p) максимален тогда и только тогда, когда p неприводим.

Пусть идеал (p) максимален. Тогда $(p) \neq R$, поэтому p не является обратимым. Предположим, что $p = ab$, причем b — не обратим. Тогда $(b) \neq R$, но $(p) \subseteq (b)$, поэтому $(p) = (b)$ из максимальности (p). Это означает, что найдется $c \in R$ такое, что $b = cp$. Получаем $p = acp$, то есть $(1 - ac)p = 0$. Поскольку R — область целостности, $ac = 1$ и a обратим. Следовательно, p неприводим.

С другой стороны, если p неприводим, то $1 \notin (p)$, то есть $(p) \neq R$. Далее, пусть идеал J строго содержит (p). Поскольку R — кольцо главных идеалов, то существует $a \in R$ такое, что $J = (a)$. Раз $(p) \subset (a)$, то $p = ab$ для некоторого $b \in R$. При этом b не обратим, иначе идеал (p) совпадал бы с (a). Следовательно, a обратим, и $(a) = R$. Таким образом, идеал (p) максимален. □

Определение 8.9. Область целостности R называется *факториальным кольцом*, если любой ненулевой и необратимый элемент $a \in R$ однозначно разлагается в произведение неприводимых, то есть существуют такие неприводимые элементы $p_i \in R$ $(i = 1, \ldots, k)$, что $a = p_1 p_2 \ldots p_k$, и для любого другого разложения на неприводимые множители $a = q_1 q_2 \ldots q_m$ можно утверждать, что $k = m$ и для некоторой перестановки $\sigma \in S_n$ выполнены равенства $p_i = \varepsilon_i q_{\sigma(i)}$ $(i = 1, \ldots, k)$, где элементы ε_i обратимы.

Теорема 8.10. *Пусть R — кольцо главных идеалов. Тогда R — факториальное кольцо.*

Доказательство. Докажем сначала существование разложения. По определению, если ненулевой элемент a необратим и не является неприводимым, то он разложим на необратимые сомножители $a = a_1 a_2$, теперь смотрим на a_1 и a_2, раскладываем те из них, которые не являются неприводимыми, и т. д. Надо лишь убедиться, что процесс оборвется. Если кольцо R евклидово, то это сразу следует из неравенств $\delta(a_1) < \delta(a)$ и $\delta(a_2) < \delta(a)$, поскольку функция δ принимает только натуральные значения. Для произвольного кольца главных идеалов рассуждение ненамного сложнее. Разложение $a = a_1 a_2$ означает, что $(a) \subset (a_1)$ (включение идеалов строгое, иначе a_2 был бы обратим). Если бы процесс разложения мог продолжаться неограниченно, то мы получили бы бесконечную возрастающую цепочку строго вложенных друг в друга идеалов. Докажем, что это невозможно.

Пусть $(d_1) \subset (d_2) \subset \ldots$ — такая цепочка. Обозначим через D объединение идеалов (d_i). Легко видеть, что D — идеал, поэтому $D = (d)$ для некоторого $d \in D$. По определению, $d \in (d_m)$ для некоторого m. Но тогда $(d_{m+1}) \subseteq (d) \subseteq (d_m)$, то есть $(d_m) = (d_{m+1})$, в противоречии с предположением о том, что все включения строгие.

Итак, процесс разложения должен оборваться, и разложение на неприводимые множители существует. Докажем единственность.

Лемма 8.10.1. *Пусть* $p_1, \ldots, p_k$ *и* $q_1, \ldots, q_m$ *— неприводимые элементы кольца* R, *удовлетворяющие условию* $p_1 \ldots p_k = q_1 \ldots q_m$. *Тогда для некоторого* $i_0 \in \{1, \ldots, m\}$ *существует такой обратимый элемент* $\varepsilon \in R$, *что* $p_1 = \varepsilon q_{i_0}$.

Доказательство. Рассмотрим факторкольцо $R/(p_1)$. В нем $\overline{q_1} \cdot \dots \cdot \overline{q_m} = \overline{q_1 \ldots q_m} = 0$. Поскольку $R/(p_1)$ — поле, отсюда следует, что $\overline{q_{i_0}} = 0$ для некоторого $i_0 \in \{1, \ldots, m\}$. Это значит, что $q_{i_0} = \alpha p_1$ для некоторого $\alpha \in R$. Поскольку p_1 и q_{i_0} неприводимы, отсюда следует, что α обратим, то есть для $\varepsilon = \alpha^{-1}$ мы получаем $p_1 = \varepsilon q_{i_0}$. □

С помощью леммы 8.10.1 легко доказать единственность разложения на неприводимые множители. Воспользуемся индукцией по k.

При $k = 1$ по лемме 8.10.1 существует индекс i_0 и обратимый элемент ε, для которых $p_1 = \varepsilon q_{i_0}$. Предположим, что $m > 1$. Тогда $q_{i_0}(\varepsilon - \prod_{i \neq i_0} q_i) = 0$, то есть $\prod_{i \neq i_0} q_i = \varepsilon$, что противоречит необратимости q_i. Отсюда $m = k = 1$ и $q_1 = p_1$.

Пусть теперь для $k < k_0$ утверждение теоремы выполнено и $a = p_1 \ldots p_{k_0} = q_1 \ldots q_m$ — два разложения на неприводимые множители. По лемме 8.10.1 существует индекс i_0 и обратимый элемент ε, для которых $p_1 = \varepsilon q_{i_0}$. Переставив индексы, можем считать, что $i_0 = 1$. Тогда $q_1\left((\varepsilon p_2) p_3 \ldots p_{k_0} - q_2 \ldots q_m\right) = 0$. Кольцо R — область целостности, поэтому $(\varepsilon p_2) p_3 \ldots p_{k_0} = q_2 \ldots q_m$. Доказательство завершается применением к этому равенству предположения индукции при $k = k_0 - 1$. □

Кольцо $\mathbb{Z}$ целых чисел и кольцо $\Bbbk[x]$ многочленов над полем $\Bbbk$ являются евклидовыми, поэтому к ним применимы все теоремы, доказанные на этой лекции. Рассмотрим еще пару примеров.

Пример 8.11. Пусть $R = \mathbb{Z}[i] \subset \mathbb{C}$ — кольцо целых гауссовых чисел (вида $m + in$, где m и n целые). Кольцо R является евклидовым относительно функции $\delta(m + in) = m^2 + n^2$ (Проверьте это!). Отсюда следует, что обратимыми элементами в нем являются только ± 1 и $\pm i$.

Пусть элемент $f = m + in$ неприводим в $\mathbb{Z}[i]$. Возможны два случая:

1) Либо m, либо n равно нулю, тогда $f = i^k p$ для некоторого $k \in \{0, 1, 2, 3\}$ и простого числа p.

2) Ни m, ни n не равно нулю, тогда элемент $\bar{f} = m - in$ тоже неприводим, и $f\bar{f} = m^2 + n^2$ — простое число. Простота $m^2 + n^2$ следует из единственности разложения на простые множители в евклидовом кольце $\mathbb{Z}[i]$.

Мы можем сделать следующий вывод: неприводимые элементы кольца $\mathbb{Z}[i]$ с точностью до умножения на i^k исчерпываются следующими:

1) Простыми числами p, не представимыми в виде суммы двух квадратов, то есть не разложимыми в $\mathbb{Z}[i]$.

2) Элементами вида $m + in$, где $m^2 + n^2$ — простое число. Заметим, что из однозначности разложения на неприводимые множители в кольце $\mathbb{Z}[i]$ следует, что если простое число p представимо в виде суммы двух квадратов, то это представление единственно.

Очевидно, что простые числа вида $4n - 1$ не представляются в виде суммы двух квадратов (рассмотрите вычеты по модулю 4). Для двойки такое представление существует: $2 = (1+i)(1-i) = -i(1 + i)^2$. Рассмотрим теперь простое число $p = 4n + 1$.

Положим $t = (2n)!$. Поскольку $t = (-1)^{2n} t = (-1)(-2) \ldots (-2n) \equiv (p - 1)(p - 2) \ldots ((p + 1)/2) \pmod p$, то $t^2 \equiv (p - 1)! \pmod p$. Однако для любого простого числа p выполнено сравнение

$$(p - 1)! + 1 \equiv 0 \pmod p.$$

Это утверждение, известное как теорема Вильсона, легко следует из того, что в поле $\mathbb{Z}/p\mathbb{Z}$ только 1 и -1 совпадают со своими обратными. Поэтому $t^2 + 1 \equiv 0 \pmod p$, то есть $(t + i)(t - i) = lp$

для некоторого натурального числа l. Кольцо $\mathbb{Z}[i]$ факториально, так что любой неприводимый делитель произведения делит хотя бы один из сомножителей. Таким образом, число p не может быть неприводимым элементом $\mathbb{Z}[i]$, иначе $t \pm i$ делилось бы на p, что невозможно.

Мы доказали, что неприводимыми в кольце $\mathbb{Z}[i]$ остаются только простые числа вида $p = 4n-1$. Отсюда следует

Теорема 8.12. *Натуральное число N представимо в виде суммы квадратов целых чисел m и n тогда и только тогда, когда в разложение N в произведение простых чисел каждое простое число вида $4n-1$ входит в четной степени.*

Доказательство. Представление натурального числа в виде суммы двух квадратов — то же самое, что представление его в виде $N = f\bar{f}$, где $f \in \mathbb{Z}[i]$. Простые числа, не имеющие вид $4n-1$, допускают такое представление. Пусть в разложение N в произведение простых чисел каждое простое число вида $4n-1$ входит в четной степени. Это разложение можно записать так:

$$N = p_1 \dots p_k q_1^2 \dots q_m^2,$$

где простые числа p_i допускают разложение $p_i = f_i \bar{f}_i$. Положим $f = f_1 \dots f_k q_1 \dots q_m$. Тогда $N = f\bar{f}$.

С другой стороны, пусть $N = f\bar{f}$. Разложим f на неприводимые множители в $\mathbb{Z}[i]$: $f = f_1 f_2 \dots f_k$. Тогда, очевидно, $\bar{f} = \bar{f}_1 \bar{f}_2 \dots \bar{f}_k$ — разложение $\bar{f}$ на неприводимые множители. Отсюда $N = (f_1\bar{f}_1) \cdot \dots \cdot (f_k\bar{f}_k)$, где $f_i\bar{f}_i$ — либо простое число, не имеющее вид $4n-1$, либо квадрат простого числа, имеющего вид $4n-1$. $\square$

Пример 8.13. Пусть $R = \mathbb{Z}[\sqrt{-5}] \subset \mathbb{C}$. Элементами кольца R являются комплексные числа вида $m + \sqrt{-5}n$, где m и n целые. Проверьте, что в R число 9 имеет два существенно различных разложения на неприводимые множители:

$$9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5})$$

(Кострикин, гл. 5, § 3).

Разумеется, это возможно потому, что R не является кольцом главных идеалов. Проверьте, что идеал $3R + (2 + \sqrt{-5})R$ не является главным.

Лекция 9.

Конечные поля

Как и на прошлой лекции, слово «кольцо» будет обозначать коммутативное ассоциативное кольцо с единицей.

Поскольку на этой лекции мы будем заниматься в основном полями, я бы хотел подчеркнуть следующий важный, хотя и простой, факт.

Утверждение 9.1. *В произвольном поле $\mathbb{F}$ есть только два идеала: $\mathbb{F}$ и $\{0\}$. Соответственно, кольцевой гомоморфизм поля $\mathbb{F}$ в кольцо R либо тривиален (то есть переводит все поле в 0), либо инъективен.*

Доказательство этого я оставляю в качестве упражнения.

На первой лекции мы убедились, что в любом кольце R однозначно определены элементы $\overline{n}$ для всех целых чисел n такие, что $\overline{m}+\overline{n}=\overline{m+n}$, $\overline{m}\cdot\overline{n}=\overline{mn}$, причем $\overline{0}$ — нуль, а $\overline{1}$ — единица кольца R. Кроме того, для любых $n\in\mathbb{N}$ и $a\in R$

$$\overline{n}a=\underbrace{a+a+\cdots+a}_{n\text{ раз}}.$$

Далее мы не будем ставить черту над n, когда из контекста ясно, имеется ли в виду целое число, или элемент кольца. Приведенные равенства показывают, что такая вольность в обозначениях оправдана.

Говоря более научно, существует канонический гомоморфизм $\mathbb{Z}\to R$, переводящий n в $\overline{n}$. Его образ — подкольцо кольца R, изоморфное либо $\mathbb{Z}$, либо $\mathbb{Z}/m\mathbb{Z}$ для некоторого $m\in\mathbb{Z}$.

Пусть $\mathbb{F}$ — конечное поле. Напомню, что характеристикой $\operatorname{char}\mathbb{F}$ поля $\mathbb{F}$ называется минимальное натуральное число p, для которого $\overline{p}=\overline{0}$ в поле $\mathbb{F}$. Поскольку поле конечно, то такое натуральное число существует. Из определения ясно, что канонический образ $\mathbb{Z}$ в $\mathbb{F}$ изоморфен $\mathbb{Z}/p\mathbb{Z}$. Число p — простое, поскольку в поле не может быть делителей нуля.

Определение 9.2. Пусть $\mathbb{F}$ — поле. Подмножество $A\subseteq\mathbb{F}$ называется *подполем* поля $\mathbb{F}$, если A является подкольцом $\mathbb{F}$ и вместе с каждым ненулевым элементом содержит обратный к нему. Если $\Bbbk$ — подполе поля $\mathbb{F}$, то поле $\mathbb{F}$ называется *расширением* поля $\Bbbk$.

Упражнение 9.3. *Пусть поле $\mathbb{F}$ конечно. Доказать, что если его подмножество $\Bbbk$ замкнуто относительно сложения и умножения, то $\Bbbk$ является подполем поля $\mathbb{F}$.*

Как мы видели, любое конечное поле $\mathbb{F}$ является расширением поля, изоморфного $\mathbb{F}_p$ для некоторого простого числа p, то есть $\mathbb{F}$ изоморфно расширению $\mathbb{F}_p$. То же относится, очевидно, ко всем полям положительной характеристики: любое поле $\mathbb{F}$ характеристики p изоморфно расширению поля $\mathbb{F}_p$.

Упражнение 9.4. *Доказать, что любое поле $\mathbb{F}$ характеристики 0 изоморфно расширению поля $\mathbb{Q}$.*

Утверждение 9.5. *Пусть $\mathbb{F}$ — конечное поле характеристики p. Тогда число элементов поля $\mathbb{F}$ равно p^k, где k — некоторое натуральное число.*

Доказательство. Элементы вида $\overline{n}\in\mathbb{F}$ образуют подполе поля $\mathbb{F}$, изоморфное $\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z}$ для некоторого простого $p\in\mathbb{N}$. Рассмотрим аддитивную группу поля $\mathbb{F}$. Для любого $a\in\mathbb{F}$ мы имеем $pa=\overline{p}a=0$. Следовательно, по теореме о строении конечных абелевых групп, аддитивная группа поля $\mathbb{F}$ изоморфна

$$\underbrace{\mathbb{Z}_p\oplus\cdots\oplus\mathbb{Z}_p}_{k\text{ раз}}$$

для некоторого натурального числа k. Отсюда следует, что $|\mathbb{F}|=p^k$. $\square$

Теорема 9.6. *Всякая конечная подгруппа мультипликативной группы любого поля является циклической. В частности, мультипликативная группа любого конечного поля — циклическая.*

Доказательство. Пусть G — конечная подгруппа мультипликативной группы поля $\mathbb{F}$, и $|G| = n$. По теореме о строении конечных абелевых групп, группа G изоморфна $\mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_m}$, где $n_1 \vdots n_2 \vdots \ldots \vdots n_m$ и $n_1 \cdot \cdots \cdot n_m = n$. Отсюда следует, что для любого $g \in G$ мы имеем $g^{n_1} = 1$. Однако многочлен $x^{n_1} - 1$ не может иметь более чем n_1 корней в поле $\mathbb{F}$, поэтому $n_1 = n$ и группа G является циклической. $\square$

Определение 9.7. Элемент a поля $\mathbb{F}$ называется *примитивным корнем степени n из* 1, если $a^n = 1$ и $a^k \neq 1$ при $0 < k < n$.

Мы видим, что каждый ненулевой элемент поля $\mathbb{F}_q$ является корнем степени $q-1$ из единицы, причем существует примитивный корень, то есть такой элемент $a \in \mathbb{F}_q$, что все ненулевые элементы поля $\mathbb{F}_q$ имеют вид a^k для некоторого $k \in \{1, \ldots, q-1\}$.

Упражнение 9.8. *Доказать, что число примитивных корней из* 1 *степени n в поле комплексных чисел $\mathbb{C}$ равно $\varphi(n)$, где $\varphi(n)$ — функция Эйлера: количество натуральных чисел m таких, что $m \leqslant n$ и $(m, n) = 1$.*

Теорема 9.9. *Для любого поля $\Bbbk$ и любого многочлена $f(x) \in \Bbbk[x]$, не равного константе, существует расширение $\mathbb{F}$ поля $\Bbbk$, над которым многочлен $f(x)$ раскладывается на линейные множители.*

Доказательство. Воспользуемся индукцией по степени многочлена $f(x)$.

Если $\deg f(x) = 1$, то доказывать нечего. Пусть $\deg f(x) > 1$, и для всех многочленов меньшей степени (над любым полем) утверждение теоремы верно. Докажем его для многочлена $f(x)$.

Разложим $f(x)$ на неприводимые множители. Если хотя бы один из них имеет степень 1, то $f(x) = (x - a)g(x)$ для некоторого $a \in \Bbbk$ и некоторого многочлена $g(x) \in \Bbbk[x]$, не равного константе. Применяя предположение индукции к многочлену $g(x)$, находим расширение $\mathbb{F}$ поля $\Bbbk$, над которым многочлен $g(x)$, а, следовательно, и многочлен $f(x)$, раскладывается на линейные множители.

Пусть все неприводимые множители многочлена $f(x)$ имеют степень, большую 1, и пусть $g(x)$ — один из этих множителей. Рассмотрим факторкольцо $\Bbbk[x]/(g(x))$. Оно является полем, так как многочлен $g(x)$ неприводим. Обозначим это поле через $\Bbbk_1$. Поле $\Bbbk$ естественно вкладывается в кольцо многочленов $\Bbbk[x]$, следовательно, существует естественное отображение $\Bbbk \to \Bbbk_1$. Ясно, что это отображение ненулевое, поэтому оно является инъективным. Отождествим поле $\Bbbk$ с его образом в $\Bbbk_1$ (чтобы рассматривать $\Bbbk_1$ как расширение поля $\Bbbk$). Образ $\overline{x}$ переменной x в факторкольце $\Bbbk[x]/(g(x)) = \Bbbk_1$ удовлетворяет, очевидно, уравнению $g(\overline{x}) = 0$ (ибо $g(\overline{x}) = \overline{g(x)}$). Поэтому многочлен $g(x)$ (который мы можем теперь рассматривать и как многочлен над полем $\Bbbk_1$) имеет в поле $\Bbbk_1$ корень $\overline{x}$, то есть делится на $(x - \overline{x})$ в кольце $\Bbbk_1[x]$. поэтому и многочлен $f(x)$ делится на $(x - \overline{x})$ в кольце $\Bbbk_1[x]$. Применяя к частному предположение индукции, получаем расширение $\mathbb{F}$ поля $\Bbbk_1$ (а, следовательно, и поля $\Bbbk \subset \Bbbk_1$), над которым многочлен $f(x)$ раскладывается на линейные множители. $\square$

Теорема 9.10. *Для любого простого числа p и любого натурального числа k существует поле $\mathbb{F}_q$ из $q = p^k$ элементов.*

Доказательство. Если $k = 1$, то $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ является полем из $q = p$ элементов. Пусть $k > 1$. Мы знаем, что поле из q элементов должно содержать подполе, изоморфное $\mathbb{F}_p$. Кроме того, каждый ненулевой элемент поля $\mathbb{F}_q$ должен быть корнем многочлена $x^{q-1} - 1$. Чтобы не выделять нуль, домножим этот многочлен на x. Тогда все q элементов поля $\mathbb{F}_q$ должны быть корнями многочлена $x^q - x$. Поэтому наша задача — присоединить к полю $\mathbb{F}_p$ все корни этого многочлена.

Итак, пусть $\mathbb{F}$ — такое расширение поля $\mathbb{F}_p$, что многочлен $x^q - x$ раскладывается в $\mathbb{F}[x]$ на линейные множители (такое расширение существует по теореме 9.9), то есть

$$x^q - x = (x - a_1) \cdot (x - a_q)$$

для некоторых $a_1, \ldots, a_q \in \mathbb{F}$.

Лемма 9.10.1. *Все элементы $a_1, \ldots, a_q \in \mathbb{F}$ попарно различны.*

Доказательство. Если многочлен $x^q - x$ делится на $(x-b)^2$ для некоторого $b \in \mathbb{F}$, то производная многочлена $x^q - x$ делится на $x - b$, то есть b является одновременно корнем многочленов $x^q - x$ и $(x^q - x)' = qx^{q-1} - 1 = -1$ (поскольку $q = p \cdot p^{k-1} = 0$ в поле $\mathbb{F}_p$). Однако многочлен -1, очевидно, не имеет корней. Следовательно, многочлен $x^q - x$ не имеет кратных корней. □

Лемма 9.10.2. *Элементы $a_1, \ldots, a_q \in \mathbb{F}$ образуют подполе поля $\mathbb{F}$.*

Доказательство. Очевидно, достаточно проверить, что сумма и произведение корней многочлена $x^q - x$ снова является его корнем (см. упражнение 9.3).

Для произведения это очевидно: если $a^q = a$ и $b^q = b$, то $(ab)^q = a^q b^q = ab$. Чтобы доказать то же для суммы, проверим сначала равенство $(a+b)^p = a^p + b^p$, верное для любых элементов любого поля характеристики p.

По формуле бинома

$$(a+b)^p = \sum_{l=0}^{p} \binom{p}{l} a^l b^{p-l}.$$

При $0 < l < p$ биномиальный коэффициент $\binom{p}{l} = \frac{p!}{l!(p-l)!}$ делится на p, поэтому над полем характеристики p от формулы бинома остаются лишь два крайних члена: $(a+b)^p = a^p + b^p$.

С помощью индукции по k отсюда легко вывести, что при $q = p^k$ над полем характеристики p верно равенство $(a+b)^q = a^q + b^q$. В нашем случае, если $a^q = a$ и $b^q = b$, то $(a+b)^q = a^q + b^q = a + b$.
□

Итак, $\mathbb{F}_q = \{a_1, \ldots, a_q\}$ является полем из q элементов. □

Теорема 9.11. *Любые два поля из $q = p^k$ элементов изоморфны.*

Доказательство. Пусть $\mathbb{F}$, $\mathbb{F}'$ — два поля из q элементов. Мы можем считать, что оба этих поля являются расширениями поля $\mathbb{F}_p$.

Мы знаем, что мультипликативная группа поля $\mathbb{F}$ — циклическая. Пусть $a \in \mathbb{F}^*$ — образующая этой группы, то есть a является примитивным корнем степени $q-1$ из единицы. Поскольку a является корнем многочлена $x^{q-1} - 1$, то a — корень одного из неприводимых над $\mathbb{F}_p$ многочленов, входящего в разложение многочлена $x^{q-1} - 1$ на неприводимые множители в $\mathbb{F}_p[x]$. Обозначим этот многочлен через $f_a(x)$.

Рассмотрим гомоморфизм колец $\varphi_a : \mathbb{F}_p[x] \to \mathbb{F}$, переводящий произвольный многочлен $f(x)$ в $f(a) \in \mathbb{F}$. Образ этого гомоморфизма содержит 0 и все натуральные степени a. Поскольку a является образующей группы $\mathbb{F}^*$, образ гомоморфизма φ_a совпадает с $\mathbb{F}$.

Ядро $\operatorname{Ker} \varphi_a$ содержит многочлен $f_a(x)$. Поэтому $(f_a(x)) \subseteq \operatorname{Ker} \varphi_a$. Многочлен $f_a(x)$ неприводим, поэтому главный идеал $(f_a(x))$ максимален, но $\operatorname{Ker} \varphi_a \neq \mathbb{F}_p[x]$, так что $\operatorname{Ker} \varphi_a = (f_a(x))$. По теореме о гомоморфизмах колец $\mathbb{F} \cong \mathbb{F}_p[x]/(f_a(x))$.

Рассмотрим теперь поле $\mathbb{F}'$. Докажем, что многочлен $f_a(x)$ разлагается в $\mathbb{F}'[x]$ на линейные множители. Действительно, пусть неприводимый многочлен $g(x)$ входит в разложение $f_a(x)$ на неприводимые множители в $\mathbb{F}'[x]$. Поскольку многочлен $x^{q-1} - 1$ делится на многочлен $f_a(x)$, мы можем заключить, что $x^{q-1} - 1$ делится на $g(x)$. Однако многочлен $x^{q-1} - 1$ разлагается в $\mathbb{F}'[x]$ на линейные множители. Из однозначности разложения на неприводимые множители в кольце $\mathbb{F}'[x]$ получаем, что многочлен $g(x)$ является линейным.

Итак, многочлен $f_a(x)$ разлагается в $\mathbb{F}'[x]$ на линейные множители и, следовательно, имеет в $\mathbb{F}'$ хотя бы один корень. Пусть $a' \in \mathbb{F}'$ — корень многочлена $f_a(x)$. Определим гомоморфизм колец $\varphi'_a : \mathbb{F}_p[x] \to \mathbb{F}'$ формулой $\varphi'_a(f(x)) = f(a')$. Ядро этого гомоморфизма содержит главный идеал $(f_a(x))$ и не совпадает со всем кольцом $\mathbb{F}_p[x]$, поскольку $\varphi'_a(1)$ — единица поля $\mathbb{F}'$, не равная нулю. Идеал $(f_a(x))$ максимален, поэтому $\operatorname{Ker}\varphi'_a = (f_a(x))$. По теореме о гомоморфизмах колец существует инъективный гомоморфизм $\psi'_a : \mathbb{F}_p[x]/(f_a(x)) \to \mathbb{F}'$. Однако $\mathbb{F}_p[x]/(f_a(x)) \cong \mathbb{F}$, так что число элементов в $\mathbb{F}_p[x]/(f_a(x))$ и в $\mathbb{F}'$ одинаково. Следовательно, ψ'_a — изоморфизм, то есть поля $\mathbb{F}$ и $\mathbb{F}'$ изоморфны. $\square$

В доказательстве теоремы 9.10 нам уже встретился следующий замечательный факт: если поле $\mathbb{F}$ имеет характеристику p, то для любых $a, b \in \mathbb{F}$ имеет место равенство $(a+b)^p = a^p + b^p$. Отсюда и из того, что $(ab)^p = a^p b^p$, легко следует, что отображение $F : \mathbb{F} \to \mathbb{F}$, заданное формулой $F(a) = a^p$, является гомоморфизмом. Ядро этого гомоморфизма не содержит 1, поэтому оно равно $\{0\}$ (поскольку в поле $\mathbb{F}$ лишь два идеала: $\mathbb{F}$ и $\{0\}$). Поэтому гомоморфизм F инъективен. В частности, если поле $\mathbb{F}$ конечно, то F обратим, то есть F является автоморфизмом. Он называется *автоморфизмом Фробениуса.*

Задача 9.12. *Доказать, что группа автоморфизмов конечного поля* $\mathbb{F}$ *циклическая и порождена автоморфизмом Фробениуса.*

Лекция 10.

Арифметические линейные пространства и матрицы

Пусть $\Bbbk$ — произвольное поле. *Арифметическим линейным пространством размерности m над полем* $\Bbbk$ называется множество $\Bbbk^m$ m-элементных наборов $\mathbf{x} = (\mathbf{x^1}, \dots, \mathbf{x^m})$, где $x^i \in \Bbbk$. Как прямая сумма абелевых групп, $\Bbbk^m$ естественно само обладает структурой абелевой группы. Кроме этого, элементы $\Bbbk^m$ можно умножать на элементы поля: $\alpha\mathbf{x} = (\alpha\mathbf{x^1}, \dots, \alpha\mathbf{x^m})$, где $\alpha \in \Bbbk$. Элементы пространства $\Bbbk^m$ называются *векторами*, а числа $x^1, \dots, x^m$ —*координатами* вектора $\mathbf{x}$.

Обозначим через $\mathbf{e_j}$ вектор, у которого j-тая координата равна 1, а остальные — 0. Любой вектор $\mathbf{x} = (\mathbf{x^1}, \dots, \mathbf{x^m})$ из $\Bbbk^m$ может быть выражен через векторы $\mathbf{e_j}$ по формуле

$$\mathbf{x} = \sum_{\mathbf{i=1}}^{\mathbf{m}} \mathbf{x^i e_i},$$

причем, как легко видеть, такое выражение однозначно. Набор векторов $(\mathbf{e_j})$ называют *стандартным базисом* пространства $\Bbbk^m$.

Рассмотрим отображение $\varphi : \Bbbk^m \to \Bbbk^n$, для которого координаты вектора $\mathbf{y} = \varphi(\mathbf{x})$ выражаются линейно через координаты вектора $\mathbf{x}$, то есть $y^i = \sum\limits_{i=1}^{m} a^i_j x^j$ для всех $i \in \{1, \dots, n\}$, где $a^i_j \in \Bbbk$ при $i \in \{1, \dots, n\}$, $j \in \{1, \dots, m\}$. Такое отображение называется *линейным*, а набор $A = (a^i_j)$ называется *матрицей линейного отображения* φ, при этом a^i_j называются *матричными элементами* матрицы A. Матрицы принято записывать следующим образом:

$$A = \begin{pmatrix} a^1_1 & a^1_2 & \dots & a^1_m \\ a^2_1 & a^2_2 & \dots & a^2_m \\ \vdots & \vdots & \ddots & \vdots \\ a^n_1 & a^n_2 & \dots & a^n_m \end{pmatrix}.$$

Говорят, что матрица A имеет n строк и m столбцов, или что A является матрицей размера $n \times m$. Множество всех матриц размера $n \times m$ обозначается через $M_{n\times m}(\Bbbk)$, или просто $M_{n\times m}$, если ясно, о каком поле идет речь. Для множества квадратных матриц вместо $M_{n\times n}$ используется обозначение M_n.

Отметим, что не только отображение φ однозначно определяется матрицей A, но и матрица A определяется линейным отображением φ однозначно. Действительно, вектор $(a^1_j, \dots, a^n_j)$, координаты которого составляют j-тый столбец матрицы A, является образом базисного вектора $\mathbf{e_j}$.

Рассмотрим теперь композицию $\varphi\circ\psi$ линейных отображений $\psi : \Bbbk^l \to \Bbbk^m$ и $\varphi : \Bbbk^m \to \Bbbk^n$. Пусть отображению φ отвечает матрица A (размера $n \times m$), а отображению ψ — матрица B (размера $m \times l$). Выберем произвольный вектор $\mathbf{x} = (\mathbf{x^1}, \dots, \mathbf{x^l}) \in \Bbbk^\mathbf{l}$ и положим $\mathbf{y} = (\mathbf{y^1}, \dots, \mathbf{y^m}) = \psi(\mathbf{x})$, $\mathbf{z} = (\mathbf{z^1}, \dots, \mathbf{z^n}) = \varphi(\mathbf{y}) = \varphi\circ\psi(\mathbf{x})$. Согласно определению матрицы линейного отображения, мы имеем

$$z^i = \sum_{j=1}^{m} a^i_j y^j = \sum_{j=1}^{m} a^i_j \Big(\sum_{k=1}^{l} b^j_k x^k\Big) = \sum_{k=1}^{l}\Big(\sum_{j=1}^{m} a^i_j b^j_k\Big) x^k = \sum_{k=1}^{l} c^i_k x^k,$$

где

$$c^i_k = \sum_{j=1}^{m} a^i_j b^j_k.$$

Мы видим, что композиция линейных отображений является снова линейным отображением. Матрица $C = (c^i_k)$, отвечающая отображению $\varphi\circ\psi$, называется *произведением* матриц A и B и обозначается через AB. Чтобы вычислить элемент произведения матриц A и B, стоящий на пересечении i-той строки и k-того столбца, надо взять i-тую строку матрицы A, k-тый столбец матрицы B, покоординатно их перемножить и сложить полученные произведения.

Применение линейного отображения $\varphi : \Bbbk^m \to \Bbbk^n$ с матрицей A к вектору $\mathbf{x} = (\mathbf{x^1}, \dots, \mathbf{x^m})$ из $\Bbbk^m$ можно рассматривать как частный случай умножения матриц. А именно, поставим в соответствие каждому вектору $\mathbf{x} \in \Bbbk^{\mathbf{m}}$ матрицу X размера $m \times 1$, у которой в i-той строке стоит x^i. Таким образом мы получим отождествление пространства $\Bbbk^m$ с множеством $M_{m\times 1}(\Bbbk)$. Аналогично, пространство $\Bbbk^n$ отождествляется с $M_{n\times 1}(\Bbbk)$. После такого отождествления отображение φ есть просто левое умножение на матрицу A, то есть $\varphi(X) = AX$. Далее мы будем записывать линейные отображения именно так.

Поскольку матрицы находятся во взаимно однозначном соответствии с линейными отображениями, причем умножение матриц соответствует композиции отображений, а композиция отображений является ассоциативной операцией, то умножение матриц тоже ассоциативно. Таким образом, $A(BC) = (AB)C$ для любых $A \in M_{n\times m}$, $B \in M_{m\times l}$, $C \in M_{l\times k}$.

Тождественное отображение $\Bbbk^n \to \Bbbk^n$ является, очевидно, линейным с матрицей

$$E_n = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}.$$

Эта матрица называется *единичной*. Для матричных элементов единичной матрицы существует специальное обозначение δ^i_j и название — *символ Кронекера*. По определению символа Кронекера

$$\delta^i_j = \begin{cases} 1, & \text{при } i = j; \\ 0, & \text{при } i \neq j. \end{cases}$$

Пусть $A \in M_{n\times m}$. При фиксированном $Y \in \Bbbk^n$ матричное уравнение $AX = Y$ представляет собой не что иное, как систему линейных уравнений

$$\begin{cases} a^1_1 x^1 + a^1_2 x^2 + \dots + a^1_m x^m &= y^1, \\ a^2_1 x^1 + a^2_2 x^2 + \dots + a^2_m x^m &= y^2, \\ \dots\dots\dots\dots\dots\dots\dots \\ a^n_1 x^1 + a^n_2 x^2 + \dots + a^n_m x^m &= y^n \end{cases}$$

на неизвестные $x^1, \dots, x^m$.

Как мы знаем, существование у такой системы решений при любом $Y \in \Bbbk^n$, то есть сюръективность отображения $X \mapsto AX$, эквивалентно наличию у этого отображения правого обратного. Аналогично, наличие у такой системы не более одного решения при любом $Y \in \Bbbk^n$, то есть инъективность отображения $X \mapsto AX$, эквивалентно наличию у него левого обратного. В связи с этим встает естественный вопрос: когда у отображения $X \mapsto AX$ есть правое (или левое) обратное в классе *линейных* отображений, то есть когда матрица A обратима справа (слева)?

Отметим, что если матрица A обратима и справа, и слева, то есть просто *обратима*, то правая и левая обратная матрицы равны между собой, тем самым обратная матрица определена однозначно.

Утверждение 10.1. *Пусть матрица D обратима и размеры матрицы A таковы, что определено произведение матриц DA. Тогда*

1) *матрица DA обратима слева в том и только в том случае, если матрица A обратима слева;*

2) *матрица DA обратима справа в том и только в том случае, если матрица A обратима справа.*

Доказательство. Пусть матрица DA обратима слева. Тогда найдется матрица B такая, что $BDA = E$, следовательно, A тоже обратима слева. Применяя то же рассуждение к матрице D^{-1}

вместо D и к матрице DA вместо A, получаем, что если A обратима слева, то и DA обратима слева.

Пусть теперь матрица DA обратима справа. Тогда найдется матрица B такая, что $DAB = E$. Сопряжем это равенство с помощью D^{-1}. Получим $D^{-1}DABD = D^{-1}ED$, то есть $ABD = E$, следовательно, A тоже обратима справа. Аналогично, если $AC = E$, то $DACD^{-1} = E$. Таким образом, если A обратима справа, то и DA обратима справа. $\square$

Чтобы использовать утверждение 10.1 для анализа левой и правой обратимости матриц, нам нужен достаточный запас обратимых матриц.

Обозначим через $D(i,j;\alpha) = (d^k_l)$ квадратную матрицу размера $n \times n$, у которой все матичные элементы, кроме d^i_j, такие же, как у единичной матрицы, а $d^i_j = \alpha$.

Пусть $i \neq j$. Тогда матрица $D(i,j;\alpha)$ имеет следующий вид:

$$\begin{array}{cc} & \begin{array}{ccccccc} & & i & & j & & \end{array} \\ \begin{array}{c} \\ \\ i \\ \\ j \\ \\ \\ \end{array} & \begin{pmatrix} 1 & \dots & 0 & \dots & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & 1 & \dots & \alpha & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & \dots & 1 & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & \dots & 0 & \dots & 1 \end{pmatrix} \end{array}$$

Пусть $A = (a^r_s)$ — произвольная матрица размера $n \times m$. Тогда $D(i,j;\alpha)A = (b^r_s)$, где $b^r_s = a^r_s + \alpha\delta^r_i a^j_s$, то есть при умножении матрицы A слева на $D(i,j;\alpha)$ все ее строчки, кроме i-той, не меняются, а к i-той строчке прибавляется j-тая, умноженная на α. Такое преобразование строк матрицы A называется *элементарным преобразованием первого типа*.

Заметим, что, применив такое преобразование к матрице $D(i,j;-\alpha)$, мы получим единичную матрицу. Поэтому $D(i,j;\alpha)D(i,j;-\alpha) = E$. Аналогично, $D(i,j;-\alpha)D(i,j;\alpha) = E$. Следовательно, матрица $D(i,j;\alpha)$ обратима.

Пусть теперь $\beta \in \Bbbk^*$ и $i \in \{1,\dots,n\}$. Рассмотрим матрицу $D(i,i;\beta)$. Эта матрица имеет следующий вид:

$$\begin{array}{cc} & \begin{array}{ccccc} & & i & & \end{array} \\ \begin{array}{c} \\ \\ i \\ \\ \\ \end{array} & \begin{pmatrix} 1 & \dots & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & \beta & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & \dots & 1 \end{pmatrix} \end{array}$$

Пусть $A = (a^r_s)$ — произвольная матрица размера $n \times m$. Тогда $D(i,i;\beta)A = (b^r_s)$, где $b^r_s = a^r_s \cdot \beta^{\delta^r_i}$, то есть при умножении матрицы A слева на $D(i,i;\beta)$ все ее строчки, кроме i-той, не меняются, а i-тая строчка умножается на β. Такое преобразование строк матрицы A называется *элементарным преобразованием второго типа*.

Применив такое преобразование к матрице $D(i,i;\beta^{-1})$, мы получим единичную матрицу. Поэтому $D(i,i;\beta)D(i,i;\beta^{-1}) = E$. Аналогично, $D(i,i;\beta^{-1})D(i,i;\beta) = E$. Следовательно, матрица $D(i,i;\beta)$ обратима.

Назовем *допустимыми* преобразования строк матрицы A размера $n \times m$, которые могут быть получены композицией элементарных преобразований первого и второго типов. Каждое допустимое преобразование сводится к умножению матрицы A слева на некоторое произведение обратимых матриц вида $D(i,j;\alpha)$, то есть на некоторую обратимую матрицу. Поэтому допустимые преобразования сохраняют свойства левой и правой обратимости.

Упражнение 10.2. *Доказать, что перестановки строк матрицы A являются допустимыми преобразованиями. На какую обратимую матрицу нужно умножить матрицу A слева, чтобы строки с номерами i и j поменялись местами? Представить эту матрицу как произведение матриц вида $D(i,j;\alpha)$.*

Говорят, что матрица A имеет *ступенчатый вид*, если каждая ее строка, кроме, быть может, первой, начинается нулями, причем количество начальных нулей в каждой следующей строке больше, чем в предыдущей.

Легко проверить, что любую матрицу A можно допустимым преобразованием привести к ступенчатому виду. Действительно, найдем первый ненулевой столбец матрицы A, то есть такой, в котором не все элементы равны нулю. Переставим строки матрицы так, чтобы ненулевой элемент этого столбца оказался наверху. Теперь, вычитая первую строку получившейся матрицы, умноженную на подходящие элементы поля, из остальных строк, получим матрицу, у которой в первой строке начальных нулей меньше, чем в любой другой. «Забудем» теперь о первой строке и повторим тот же процесс для оставшейся части полученной матрицы. После этого первая строка не изменится, во второй начальных нулей будет больше чем в первой, но меньше, чем во всех остальных. Повторяя этот процесс, пока остаются ненулевые строки в «обрабатываемой части» матрицы, мы получим, в конце концов, матрицу ступенчатого вида.

Заметим, что допустимыми преобразованиями мы можем добиться большего. А именно, каждую матрицу можно привести допустимым преобразованием к матрице ступенчатого вида, у которой первый ненулевой элемент в каждой строке равен единице, а все остальные элементы того же столбца равны нулю. Такие матрицы имеют вид:

$$\begin{pmatrix} 0 & \dots & 1 & * & \dots & * & 0 & * & \dots & 0 & * & \dots & * \\ 0 & \dots & 0 & 0 & \dots & 0 & 1 & * & \dots & 0 & * & \dots & * \\ \multicolumn{13}{c}{\dotfill} \\ 0 & \dots & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 1 & * & \dots & * \\ \multicolumn{13}{c}{\dotfill} \\ 0 & \dots & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & \dots & 0 \end{pmatrix}$$

(нулевых столбцов в начале и нулевых строк в конце может, разумеется, и не быть). Такие матрицы иногда называются матрицами *главного ступенчатого вида*.

Приведение матрицы к главному ступенчатому виду используется в *методе Гаусса* решения систем линейных уравнений. Об этом можно прочитать в учебнике Кострикина (или в любом другом).

Квадратная матрица главного ступенчатого вида либо имеет нулевую строку, либо совпадает с единичной. В первом случае она, очевидно, не может быть обратима справа, а во втором случае она обратима и слева и справа. Поскольку каждая матрица может быть приведена допустимым преобразованием к главному ступенчатому виду, а такие преобразования сохраняют левую и правую обратимость, то имеет место

Утверждение 10.3. *Квадратная матрица обратима тогда и только тогда, когда она обратима справа.*

Следствие 10.4. *Квадратная матрица обратима тогда и только тогда, когда она обратима слева.*

Доказательство. Пусть матрица A обратима слева, то есть найдется матрица B, для которой $BA = E$. Тогда матрица B обратима справа, следовательно, обратима. При этом $A = B^{-1}$, поэтому матрица A тоже обратима. $\square$

Итак, квадратная матрица A обратима тогда и только тогда, когда она приводится допустимым преобразованием к единичной матрице. Поскольку допустимое преобразование состоит в умножении матрицы A слева на некоторую обратимую матрицу D, являющуюся произведением матриц вида $D(i,j;\alpha)$, то мы имеем $DA = E$, то есть $D = A^{-1}$. Матрицу A^{-1} можно вычислить одновременно с приведением матрицы A элементарными преобразованиями к единичной. А именно, припишем справа к матрице A единичную матрицу. Запишем полученную матрицу размера $n \times 2n$ как $(A \mid E)$ в знак того, что она состоит из двух блоков размера $n \times n$. После применения к этой матрице допустимого преобразования, отвечающего матрице D, мы получим матрицу $D(A \mid E) = (DA \mid D)$. Таким образом, как только в первом блоке окажется единичная матрица, во втором будет матрица A^{-1}.

Множество всех обратимых матриц размера $n \times n$ над полем $\Bbbk$ обозначается через $GL_n(\Bbbk)$. Очевидно, что $GL_n(\Bbbk)$ является группой.

Упражнение 10.5. *Доказать, что группа $GL_n(\Bbbk)$ порождается матрицами $D(i,j;\alpha)$ с $i \neq j$ и матрицами $D(i,i;\beta)$ с $\beta \neq 0$.*

Заметим, что матрица ступенчатого вида размера $n \times m$ при $n > m$ обязательно имеет нулевую строку, поэтому она не может быть обратима справа. Поскольку свойство обратимости слева при допустимых преобразованиях сохраняется, то же верно для любой матрицы размера $n \times m$. Отсюда следует, что никакая матрица $m \times n$ не может быть обратима слева. Поэтому, если матрица обратима, то она квадратная.

Упражнение 10.6. *Доказать, что свойства инъективности и сюръективности линейных отображений сохраняются при элементарных преобразованиях матриц.*

Упражнение 10.7. *Доказать, что линейное отображение является инъективным тогда и только тогда, когда его матрица обратима слева.*

Упражнение 10.8. *Доказать, что линейное отображение является сюръективным тогда и только тогда, когда его матрица обратима справа.*

Определение 10.9. *Линейным пространством над полем* $\Bbbk$ называется множество V, на котором заданы операция сложения, относительно которой V является абелевой группой, и операция умножения элементов поля $\Bbbk$ на элементы множества V, то есть отображение $\Bbbk \times V \to V$, удовлетворяющие следующим аксиомам:

1) $1 \cdot v = v$, где 1 — единица поля $\Bbbk$, а v — произвольный элемент множества V;

2) $a(bv) = (ab)v$ для любых $a, b \in \Bbbk$, $v \in V$;

3) $(a+b)v = av + bv$ для любых $a, b \in \Bbbk$, $v \in V$;

4) $a(v+w) = av + aw$ для любых $a \in \Bbbk$, $v, w \in V$.

Линейное пространство V называется *конечномерным*, если в нем существует такой конечный набор элементов $v_1, \ldots, v_n$, что для любого $v \in V$ найдутся такие $\alpha^1, \ldots, \alpha^n \in \Bbbk$, что $v = \sum\limits_{i=1}^{n} \alpha^i v_i$. Если при этом $\alpha^1, \ldots, \alpha^n$ определены однозначно, то набор (v_i) называется *базисом* пространства V.

Легко видеть, что арифметическое линейное пространство является примером линейного пространства, а стандартный базис арифметического линейного пространства является примером базиса.

Утверждение 10.10. *Любое конечномерное линейное пространство имеет конечный базис.*

Доказательство. Пусть $v_1, \dots, v_n$ такие, как в определении конечномерного пространства. Мы можем считать, что все они отличны от нуля. Положим $w_1 = v_1$. Если $v_2 \neq \alpha w_1$ ни при каком $\alpha \in \Bbbk$, то положим $w_2 = v_2$. Если же $v_2 = \beta w_1$ для некоторого $\beta \in \Bbbk$, то найдем минимальное $j = j(2)$ такое, что $v_j \neq \alpha w_1$ ни при каком $\alpha \in \Bbbk$, и положим $w_2 = v_j$. Аналогично, на k-том шаге найдем минимальное $j = j(k)$ такое, что

$$v_j \neq \sum_{i=1}^{k-1} \alpha^i w_i$$

ни при каких $\alpha^i \in \Bbbk$, и положим $w_k = v_j$. Очевидно, что последовательность $(1, j(2), j(3), \dots)$ возрастает, поэтому в какой-то момент процесс оборвется. Полученный к этому моменту набор $(w_1, \dots, w_l)$ будет базисом.

Действительно, каждый элемент пространства V линейно выражается через набор (v_j), а элементы этого набора линейно выражаются через набор (w_i), поэтому каждый элемент пространства V линейно выражается через набор (w_i). Предположим, что однозначность не имеет места, то есть для некоторого $v \in V$ найдутся $\alpha^i, \beta^i \in \Bbbk$ такие, что

$$v = \sum_{i=1}^{l} \alpha^i w_i = \sum_{i=1}^{l} \beta^i w_i,$$

причем $\alpha^i \neq \beta^i$ хотя бы для одного $i \in \{1, \dots, l\}$. Тогда $\gamma^i = \alpha^i - \beta^i$ не все равны нулю, но

$$\sum_{i=1}^{l} \gamma^i w_i = 0.$$

Пусть k — максимальное, для которого $\gamma^k \neq 0$. Тогда

$$w_k = \sum_{i=1}^{k-1} \frac{(-\gamma^i)}{\gamma^k} w_i,$$

что противоречит выбору w_k. Поэтому любой элемент пространства V выражается через w_i однозначно. $\square$

Теорема 10.11. *Пусть $(v_1, \dots, v_m)$ и $(w_1, \dots, w_n)$ — два базиса линейного пространства V. Тогда $n = m$.*

Доказательство. Выразим элементы базисов друг через друга:

$$v_j = \sum_{i=1}^{n} a_j^i w_i; \qquad w_l = \sum_{k=1}^{m} b_l^k v_k.$$

Подставим эти выражения друг в друга, поменяв порядок суммирования:

$$v_j = \sum_{k=1}^{m} \sum_{i=1}^{n} a_j^i b_i^k v_k; \qquad w_l = \sum_{i=1}^{n} \sum_{k=1}^{m} b_l^k a_k^i w_i.$$

Поскольку разложение $v_j \in V$ по базису $(v_1, \dots, v_m)$ однозначно, мы получаем из первого из этих равенств

$$\sum_{i=1}^{n} a_j^i b_i^k = \delta_j^k.$$

Аналогично,

$$\sum_{k=1}^{m} b_l^k a_k^i = \delta_l^i.$$

Таким образом, для матриц $A = (a_j^i)$ и $B = (b_l^k)$ выполнены равенства $BA = E$ и $AB = E$, то есть обе они обратимы. Поскольку обратимой может быть только квадратная матрица, то мы и получаем $n = m$. $\square$

Определение 10.12. Пусть V — конечномерное линейное пространство. *Размерностью* пространства V называется число элементов базиса V. Размерность пространства V обозначается через $\dim V$.

Поскольку любое конечномерное линейное пространство имеет конечный базис и любые два его базиса имеют одно и то же число элементов, то определение размерности корректно (не зависит от выбора базиса).

Пусть V — линейное пространство над полем $\Bbbk$. Подмножество $W \subseteq V$ называется *подпространством* пространства V, если оно замкнуто относительно сложения и умножения на произвольные элементы поля $\Bbbk$.

Пусть V — линейное пространство над полем $\Bbbk$, $W \subseteq V$ — подпространство. Рассмотрим факторгруппу $U = V/W$. Введем на U умножение на элементы поля $\Bbbk$, полагая $\alpha\cdot(v+W) = \alpha v+W$. Проверьте, что таким образом U приобретает структуру линейного пространства над полем $\Bbbk$. Оно называется *факторпространством* пространства V по подпространству W.

Упражнение 10.13. *Пусть V — конечномерное линейное пространство над полем $\Bbbk$, $W \subseteq V$ — подпространство, $U = V/W$ — факторпространство. Доказать, что W и U конечномерны, причем* $\dim W + \dim U = \dim V$.

Мы обсудили умножение матриц. На самом деле, матрицы можно еще и складывать. Разумеется, матрицы можно складывать далеко не всегда, а лишь тогда, когда они имеют одинаковый размер. В то время как призведение матриц отвечает композиции линейных отображений, их сумма отвечает сумме отображений (значение на векторе $v \in V$ суммы двух отображений φ и ψ пространства V в пространство W равно сумме значений $\varphi(v) + \psi(v)$).

Легко проверить, что для умножения и сложения матриц выполнены свойства левой и правой дистрибутивности:

1) Для любой матрицы A размера $n\times m$ и любых двух матриц B и C размера $m\times l$ выполнено равенство
$$A(B + C) = AB + AC.$$

2) Для любых двух матриц A и B размера $n\times m$ и любой матрицы C размера $m\times l$ выполнено равенство
$$(A + B)C = AC + BC.$$

Рассмотрим теперь множество $M_n(\Bbbk)$ квадратных матриц размера $n \times n$. Легко понять, что $M_n(\Bbbk)$ является ассоциативным кольцом с единицей (но не коммутативным при $n > 1$).

Упражнение 10.14. *Доказать, что в кольце $M_n(\Bbbk)$ только два двусторонних идеала: $M_n(\Bbbk)$ и* $\{0\}$.

Лекция 11.

Алгебры

Определение 11.1. *Алгеброй над полем* $\Bbbk$ называется кольцо A, являющееся одновременно линейным пространством над полем $\Bbbk$, в котором кольцевые операции согласованы со структурой линейного пространства, то есть сложение – общее и $\alpha(ab) = (\alpha a)b = a(\alpha b)$ для любых $a, b \in A$ и $\alpha \in \Bbbk$.

Пример 11.2. Поле комплексных чисел $\mathbb{C}$ является алгеброй размерности два над полем вещественных чисел $\mathbb{R}$. Любое поле характеристики p является алгеброй над полем $\mathbb{F}_p$ (по существу, мы уже пользовались этим, когда доказывали, что любое конечное поле характеристики p имеет p^k элементов). Кольцо многочленов $\Bbbk[x]$ является бесконечномерной алгеброй над полем $\Bbbk$.

Упражнение 11.3. *Доказать, что кольцо $n \times n$ матриц над полем $\Bbbk$ является алгеброй размерности n^2 над полем $\Bbbk$.*

На первой лекции мы определяли кольцо многочленов не только над полем, но и над произвольным коммутативным кольцом. В частности, можно рассмотреть кольцо многочленов над $\Bbbk[x]$. Получается $\Bbbk[x, y] = \Bbbk[x][y]$ — *кольцо многочленов от двух переменных*. Легко видеть, что $\Bbbk[x, y]$ является алгеброй над $\Bbbk$ с базисом, состоящем из *мономов* $x^k y^l$, где $k, l \in \mathbb{N} \cup \{0\}$.

Аналогично определяется алгебра $\Bbbk[x_1, \dots, x_n]$ многочленов от n переменных; базис ее над $\Bbbk$ составляют мономы $x_1^{k_1} \dots x_n^{k_n}$.

Утверждение 11.4. *Кольцо многочленов $A[x]$ над целостным кольцом A является целостным.*

Доказательство. Пусть $f(x), g(x)$ — ненулевые многочлены из $A[x]$. Положим $m = \deg f(x)$, $n = \deg g(x)$. Тогда $f(x) = a_0 + \dots + a_m x^m$, $g(x) = b_0 + \dots + b_n x^n$, причем $a_m \neq 0$ и $b_n \neq 0$. По определению произведения многочленов,

$$f(x)g(x) = \sum_{k=0}^{m+n} c_k x^k,$$

где $c_k = \sum\limits_{i+j=k} a_i b_j$. В частности, $c_{m+n} = a_m b_n$, но $a_m b_n \neq 0$, поскольку A — область целостности. Следовательно, $f(x)g(x) \neq 0$. □

Из утверждения 11.4 следует, что кольцо многочленов от нескольких переменных над полем является целостным.

Не все свойства кольца многочленов от одного переменного переносятся на кольцо многочленов от нескольких переменных. Так, кольцо $\Bbbk[x_1, \dots, x_n]$ является кольцом главных идеалов лишь при $n = 1$. Например, идеал $(x) + (y)$ в кольце $\Bbbk[x, y]$ не является главным (Докажите это!).

Тем не менее кольцо $\Bbbk[x_1, \dots, x_n]$ является факториальным. Доказательство этого есть в учебнике Кострикина, гл. 9, § 2.

Пусть $(a_1, \dots, a_n)$ — базис алгебры A над полем $\Bbbk$ как линейного пространства. Из определения ясно, что структура алгебры однозначно определяется произведениями базисных элементов $a_i a_j$ для всех $i, j \in \{1, \dots, n\}$. Поскольку $(a_1, \dots, a_n)$ — базис, эти произведения можно по нему разложить:

$$a_i a_j = \sum_{k=1}^{n} c_{ij}^k a_k.$$

Элементы $c_{ij}^k \in \Bbbk$ называются *структурными константами* алгебры A. Отметим, что произвольный выбор структурных констант определяет на линейном пространстве A структуру алгебры, которая, вообще говоря, не будет ни коммутативной, ни ассоциативной.

Упражнение 11.5. *При каком условии на структурные константы c_{ij}^k алгебра A является коммутативной? Ассоциативной?*

Пример 11.6. Определим алгебру кватернионов $\mathbb{H}$ как линейное пространство над $\mathbb{R}$ с базисом $(1, i, j, k)$, где произведения базисных векторов определяются так:

$$\begin{aligned} 1\cdot 1 = -i\cdot i = -j\cdot j = -k\cdot k &= 1;\\ 1\cdot i = i\cdot 1 = j\cdot k = -k\cdot j &= i;\\ 1\cdot j = j\cdot 1 = k\cdot i = -i\cdot k &= j;\\ 1\cdot k = k\cdot 1 = i\cdot j = -j\cdot i &= k. \end{aligned}$$

Алгебра $\mathbb{H}$, очевидно, не является коммутативной.

Утверждение 11.7. *Алгебра $\mathbb{H}$ является ассоциативной.*

Доказательство. Доказать ассоциативность алгебры $\mathbb{H}$ можно прямой проверкой. Мы поступим чуть-чуть иначе.

Рассмотрим в алгебре матриц $M_4(\mathbb{R})$ линейное подпространство H, состоящее из матриц вида

$$\begin{pmatrix} a & -b & -c & -d\\ b & a & -d & c\\ c & d & a & -b\\ d & -c & b & a \end{pmatrix}.$$

Базис H составляют матрицы

$$E = \begin{pmatrix} 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1 \end{pmatrix}, \qquad I = \begin{pmatrix} 0 & -1 & 0 & 0\\ 1 & 0 & 0 & 0\\ 0 & 0 & 0 & -1\\ 0 & 0 & 1 & 0 \end{pmatrix},$$

$$J = \begin{pmatrix} 0 & 0 & -1 & 0\\ 0 & 0 & 0 & 1\\ 1 & 0 & 0 & 0\\ 0 & -1 & 0 & 0 \end{pmatrix} \quad \text{и} \quad K = \begin{pmatrix} 0 & 0 & 0 & -1\\ 0 & 0 & -1 & 0\\ 0 & 1 & 0 & 0\\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

Непосредственно проверяется, что эти матрицы удовлетворяют соотношениям

$$\begin{aligned} E\cdot E = -I\cdot I = -J\cdot J = -K\cdot K &= E;\\ E\cdot I = I\cdot E = J\cdot K = -K\cdot J &= I;\\ E\cdot J = J\cdot E = K\cdot I = -I\cdot K &= J;\\ E\cdot K = K\cdot E = I\cdot J = -J\cdot I &= K. \end{aligned}$$

Отсюда следует, что, во-первых, H замкнуто относительно умножения, то есть является подалгеброй алгебры $M_4(\mathbb{R})$, и, во-вторых, алгебра H изоморфна алгебре кватернионов $\mathbb{H}$. Ассоциативность алгебры $\mathbb{H}$ следует теперь из ассоциативности умножения матриц. □

Определение 11.8. В произвольном ассоциативном кольце R с единицей элемент $a \in R$ называется *обратимым*, если существует $b \in R$, для которого $ab = ba = 1$.

Ассоциативное кольцо R с единицей называется *телом*, если каждый ненулевой элемент $a \in R$ обратим.

Легко видеть, что обратимые элементы произвольного ассоциативного кольца с единицей образуют группу по умножению.

Утверждение 11.9. *Алгебра $\mathbb{H}$ является телом.*

Доказательство. Пусть $h = a + bi + cj + dk \in \mathbb{H}$. Положим $\overline{h} = a - bi - cj - dk \in \mathbb{H}$. Тогда $h\overline{h} = \overline{h}h = a^2 + b^2 + c^2 + d^2$ и если $h \neq 0$, то $\overline{h}/(a^2 + b^2 + c^2 + d^2)$ является обратным к h. □

Алгебра Грассмана

Алгебра Грассмана от n переменных над полем $\Bbbk$, построение которой будет изложено далее, является ассоциативной алгеброй с единицей. Она почти столь же важна в математике, как и кольцо многочленов от нескольких переменных, и во многом аналогична ему. Кольцо многочленов $\Bbbk[x_1,\ldots,x_n]$ порождено набором коммутирующих переменных $(x_1,\ldots,x_n)$, между которыми нет других соотношений. Алгебра Грассмана $\Lambda^\bullet(\xi^1,\ldots,\xi^n)$ порождена набором *антикоммутирующих* переменных $\xi^1,\ldots,\xi^n$, между которыми также нет других соотношений.

Слово «антикоммутирующие» означает следующее: $\xi^i\wedge\xi^j=-\xi^j\wedge\xi^i$ для любых $i,j\in[1,n]$, а также $\xi^i\wedge\xi^i=0$ для любого $i\in[1,n]$ (где $[1,n]$ обозначает множество целых чисел от 1 до n). При $\operatorname{char}\Bbbk\neq 2$ второе условие следует из первого. Знак $\wedge$ в алгебре Грассмана традиционно используется для обозначения произведения. Умножение в алгебре Грассмана называется *внешним умножением*.

Условие антикоммутативности умножения на первый взгляд сильно отличается от коммутативности, но на самом деле ничем не хуже — оно позволяет переставлять в любом произведении $\xi^{i_1}\wedge\cdots\wedge\xi^{i_k}$ соседние сомножители местами, при этом произведение просто меняет знак. Отсюда следует, что в алгебре Грассмана любое произведение образующих либо равно нулю, либо равно, с точностью до знака, произведению образующих со строго возрастающими номерами. Поэтому каждый элемент алгебры Грассмана линейно выражается через такие произведения.

Все вышесказанное представляет собой только наводящие соображения — алгебру Грассмана еще предстоит построить. Дадим точные определения.

Зафиксируем набор *грассмановых переменных* $\xi^1,\ldots,\xi^n$. *Грассмановым мономом* от $\xi^1,\ldots,\xi^n$ называется выражение вида $\xi^{i_1}\wedge\cdots\wedge\xi^{i_k}$, где $1\leqslant i_1<i_2<\cdots<i_k\leqslant n$. Обозначим такой моном через ξ^I, где $I=\{i^1,\ldots,i^k\}$. Таким образом, грассмановы мономы находятся во взаимно однозначном соответствии с подмножествами множества $\{1,\ldots,n\}$. Пустому множеству при этом соответствует произведение пустого множества образующих, то есть 1.

Положим $\xi^{i_{\sigma(1)}}\wedge\cdots\wedge\xi^{i_{\sigma(k)}}=\varepsilon(\sigma)\xi^{i_1}\wedge\cdots\wedge\xi^{i_k}$ для любой перестановки $\sigma\in S_k$ (напомню, что через $\varepsilon(\sigma)$ обозначается знак перестановки σ). Произведение $\xi^{j_1}\wedge\cdots\wedge\xi^{j_m}$, где среди набора индексов $(j_1,\ldots,j_m)$ есть повторяющиеся, положим равным нулю.

Теперь легко определить произведение $\xi^I\wedge\xi^J$ грассмановых мономов ξ^I и ξ^J. Оно получается просто приписыванием одного монома к другому через знак $\wedge$ и преобразованием получившегося выражения по изложенным выше правилам. Результат можно описать так:

$$\xi^I\wedge\xi^J=\begin{cases}0, & \text{если } I\cap J\neq\varnothing,\\ (-1)^{c(I,J)}\xi^{I\cup J}, & \text{если } I\cap J=\varnothing,\end{cases}$$

где

$$c(I,J)=\#\{(i,j)\in I\times J\mid i>j\}.$$

(Знак $\#$ обозначает число элементов множества.)

Упражнение 11.10. *Доказать, что введенное умножение мономов является ассоциативным.*

Обозначим через $\Lambda^\bullet(\xi^1,\ldots,\xi^n)$, или просто через $\Lambda^\bullet$, линейное пространство над полем $\Bbbk$ с базисом (ξ^I), то есть пространство всех выражений вида

$$\sum_{I\subseteq[1,n]}a_I\xi^I,$$

где $a_I\in\Bbbk$. Введенное на базисе этого пространства умножение задает структуру алгебры на $\Lambda^\bullet$. По построению это алгебра с единицей. Легко видеть, что ассоциативность умножения в алгебре достаточно проверять на базисе (см. упражнение 11.5). Из упражнения 11.10 получаем, что алгебра $\Lambda^\bullet$ является ассоциативной. Она и называется алгеброй Грассмана.

Размерность алгебры Грассмана равна числу всех подмножеств множества $[1,n]$, то есть $\dim\Lambda^\bullet=2^n$. Назовем *степенью* монома $\xi^{i_1}\wedge\cdots\wedge\xi^{i_k}$ число k. Грассмановы мономы степени

k образуют базис подпространства $\Lambda^k \subseteq \Lambda^\bullet$. Ясно, что $\dim \Lambda^k = \binom{n}{k}$ и $\Lambda^\bullet = \bigoplus\limits_{k=0}^{n} \Lambda^k$. Отметим также, что при перемножении степени мономов складываются.

Пусть $\alpha, \beta \in \Lambda^1$, то есть $\alpha = \sum\limits_{i=1}^{n} a_i \xi^i$ и $\beta = \sum\limits_{i=1}^{n} b_i \xi^i$. Тогда, как легко убедиться, $\alpha \wedge \alpha = 0$ и $\alpha \wedge \beta = -\beta \wedge \alpha$. Эти равенства понадобятся нам на следующей лекции.

Упражнение 11.11. *Доказать, что если $\zeta \in \Lambda^p$ и $\eta \in \Lambda^q$, то*

$$\zeta \wedge \eta = (-1)^{pq} \eta \wedge \zeta.$$

Лекция 12.

Определители матриц

Мы будем строить теорию определителей с помощью алгебры Грассмана.

Определение 12.1. *Определителем* $\det A$ матрицы $A = (a^i_j) \in M_n(\Bbbk)$ называется коэффициент при $\xi^1 \wedge \dots \wedge \xi^n$ в произведении n грассмановых полиномов первой степени

$$\Big(\sum_{j=1}^n a^1_j \xi^j\Big) \wedge \Big(\sum_{j=1}^n a^2_j \xi^j\Big) \wedge \dots \wedge \Big(\sum_{j=1}^n a^n_j \xi^j\Big) = (\det A)\xi^1 \wedge \dots \wedge \xi^n.$$

Определитель матрицы A обозначается также через $|A|$ (чаще всего такое обозначение используется для матриц, выписанных в явном виде).

Пример 12.2.

$$(a\xi^1 + b\xi^2) \wedge (c\xi^1 + d\xi^2) = ac\xi^1 \wedge \xi^1 + ad\xi^1 \wedge \xi^2 + bc\xi^2 \wedge \xi^1 + bd\xi^2 \wedge \xi^2 = \\ = ad\xi^1 \wedge \xi^2 - bc\xi^1 \wedge \xi^2 = (ad - bc)\xi^1 \wedge \xi^2,$$

то есть

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc.$$

Утверждение 12.3. *Определитель матрицы A задается формулой*

$$\det A = \sum_{\sigma \in S_n} \varepsilon(\sigma) a^1_{\sigma(1)} a^2_{\sigma(2)} \cdots a^n_{\sigma(n)}.$$

Доказательство. Непосредственно следует из определения умножения в алгебре Грассмана. □

Определение 12.4. *Транспонированной* матрицей к матрице $A = (a^i_j)$ размера $m \times n$ называется матрица $A^t = (b^k_l)$ размера $n \times m$, где $b^k_l = a^l_k$.

Упражнение 12.5. *Доказать, что для любой квадратной матрицы A выполнено равенство $\det A^t = \det A$.*

Утверждение 12.6. *Функция $\det : M_n(\Bbbk) \to \Bbbk$ обладает следующими свойствами:*

1) При умножении строки матрицы на элемент поля значение функции умножается на этот элемент поля.

2) Если некоторая строка матрицы представлена в виде суммы двух строк, то значение функции на этой матрице равно сумме значений ее на матрицах, полученных из первоначальной заменой выделенной строки на строки — слагаемые.

3) Если у матрицы две соседние строки равны между собой, то функция от нее равна нулю.

4) Функция от единичной матрицы равна 1.

Доказательство. Непосредственно следует из свойств умножения в алгебре Грассмана. □

Теорема 12.7. *Свойствами 1–4 функция на $M_n(\Bbbk)$ определяется однозначно.*

Доказательство. Пусть функция $f(A)$ имеет свойства 1–4.

Лемма 12.7.1. *Из свойств 2 и 3 следует, что функция $f(A)$ умножается на -1 при перемене двух соседних строк матрицы A местами.*

Доказательство. Заменим каждую из двух соседних строк их суммой. Тогда

$$f\begin{pmatrix} a_1^1 & a_2^1 & \cdots & a_n^1 \\ \cdots & \cdots & \cdots & \cdots \\ a_1^i + a_1^{i+1} & a_2^i + a_2^{i+1} & \cdots & a_n^i + a_n^{i+1} \\ a_1^i + a_1^{i+1} & a_2^i + a_2^{i+1} & \cdots & a_n^i + a_n^{i+1} \\ \cdots & \cdots & \cdots & \cdots \\ a_1^n & a_2^n & \cdots & a_n^n \end{pmatrix} = 0$$

по свойству 3. С другой стороны, применяя к обеим строкам полученной матрицы последовательно свойство 2 и пользуясь вновь свойством 3, получаем

$$f\begin{pmatrix} a_1^1 & a_2^1 & \cdots & a_n^1 \\ \cdots & \cdots & \cdots & \cdots \\ a_1^i + a_1^{i+1} & a_2^i + a_2^{i+1} & \cdots & a_n^i + a_n^{i+1} \\ a_1^i + a_1^{i+1} & a_2^i + a_2^{i+1} & \cdots & a_n^i + a_n^{i+1} \\ \cdots & \cdots & \cdots & \cdots \\ a_1^n & a_2^n & \cdots & a_n^n \end{pmatrix} =$$

$$= f\begin{pmatrix} a_1^1 & a_2^1 & \cdots & a_n^1 \\ \cdots & \cdots & \cdots & \cdots \\ a_1^i & a_2^i & \cdots & a_n^i \\ a_1^i & a_2^i & \cdots & a_n^i \\ \cdots & \cdots & \cdots & \cdots \\ a_1^n & a_2^n & \cdots & a_n^n \end{pmatrix} + f\begin{pmatrix} a_1^1 & a_2^1 & \cdots & a_n^1 \\ \cdots & \cdots & \cdots & \cdots \\ a_1^i & a_2^i & \cdots & a_n^i \\ a_1^{i+1} & a_2^{i+1} & \cdots & a_n^{i+1} \\ \cdots & \cdots & \cdots & \cdots \\ a_1^n & a_2^n & \cdots & a_n^n \end{pmatrix} +$$

$$+ f\begin{pmatrix} a_1^1 & a_2^1 & \cdots & a_n^1 \\ \cdots & \cdots & \cdots & \cdots \\ a_1^{i+1} & a_2^{i+1} & \cdots & a_n^{i+1} \\ a_1^i & a_2^i & \cdots & a_n^i \\ \cdots & \cdots & \cdots & \cdots \\ a_1^n & a_2^n & \cdots & a_n^n \end{pmatrix} + f\begin{pmatrix} a_1^1 & a_2^1 & \cdots & a_n^1 \\ \cdots & \cdots & \cdots & \cdots \\ a_1^{i+1} & a_2^{i+1} & \cdots & a_n^{i+1} \\ a_1^{i+1} & a_2^{i+1} & \cdots & a_n^{i+1} \\ \cdots & \cdots & \cdots & \cdots \\ a_1^n & a_2^n & \cdots & a_n^n \end{pmatrix} =$$

$$= f\begin{pmatrix} a_1^1 & a_2^1 & \cdots & a_n^1 \\ \cdots & \cdots & \cdots & \cdots \\ a_1^i & a_2^i & \cdots & a_n^i \\ a_1^{i+1} & a_2^{i+1} & \cdots & a_n^{i+1} \\ \cdots & \cdots & \cdots & \cdots \\ a_1^n & a_2^n & \cdots & a_n^n \end{pmatrix} + f\begin{pmatrix} a_1^1 & a_2^1 & \cdots & a_n^1 \\ \cdots & \cdots & \cdots & \cdots \\ a_1^{i+1} & a_2^{i+1} & \cdots & a_n^{i+1} \\ a_1^i & a_2^i & \cdots & a_n^i \\ \cdots & \cdots & \cdots & \cdots \\ a_1^n & a_2^n & \cdots & a_n^n \end{pmatrix}.$$

Таким образом, сумма значений функции на исходной матрице и на матрице с переставленными соседними строками равна нулю. □

Лемма 12.7.2. *Из свойств 2 и 3 следует, что функция $f(A)$ равна нулю, если у матрицы A какие-то две строки равны.*

Доказательство. С помощью леммы 12.7.1 все сводится к случаю, когда равны соседние строки, а тогда $f(A) = 0$ по свойству 3. □

Лемма 12.7.3. *Из свойств 1, 2 и 3 следует, что функция не изменяется при элементарном преобразовании первого типа строк матрицы A.*

Доказательство. Пусть j-тая строка матрицы A пропорциональна i-той, то есть существует $d \in \Bbbk$ такое, что $a_k^j = da_k^i$ для любого $k \in [1, n]$. Тогда $f(A) = 0$ по свойству 1 и лемме 12.7.2.

Пусть теперь A — произвольная квадратная матрица. По свойству 2

$$f\begin{pmatrix} a_1^1 & a_2^1 & \cdots & a_n^1 \\ \multicolumn{4}{c}{\dotfill} \\ a_1^i & a_2^i & \cdots & a_n^i \\ \multicolumn{4}{c}{\dotfill} \\ a_1^j + da_1^i & a_2^j + da_2^i & \cdots & a_n^j + da_n^i \\ \multicolumn{4}{c}{\dotfill} \\ a_1^n & a_2^n & \cdots & a_n^n \end{pmatrix} =$$

$$= f\begin{pmatrix} a_1^1 & a_2^1 & \cdots & a_n^1 \\ \multicolumn{4}{c}{\dotfill} \\ a_1^i & a_2^i & \cdots & a_n^i \\ \multicolumn{4}{c}{\dotfill} \\ a_1^j & a_2^j & \cdots & a_n^j \\ \multicolumn{4}{c}{\dotfill} \\ a_1^n & a_2^n & \cdots & a_n^n \end{pmatrix} + f\begin{pmatrix} a_1^1 & a_2^1 & \cdots & a_n^1 \\ \multicolumn{4}{c}{\dotfill} \\ a_1^i & a_2^i & \cdots & a_n^i \\ \multicolumn{4}{c}{\dotfill} \\ da_1^i & da_2^i & \cdots & da_n^i \\ \multicolumn{4}{c}{\dotfill} \\ a_1^n & a_2^n & \cdots & a_n^n \end{pmatrix} =$$

$$= f\begin{pmatrix} a_1^1 & a_2^1 & \cdots & a_n^1 \\ \multicolumn{4}{c}{\dotfill} \\ a_1^i & a_2^i & \cdots & a_n^i \\ \multicolumn{4}{c}{\dotfill} \\ a_1^j & a_2^j & \cdots & a_n^j \\ \multicolumn{4}{c}{\dotfill} \\ a_1^n & a_2^n & \cdots & a_n^n \end{pmatrix}.$$

□

Мы знаем, что любую квадратную матрицу можно привести последовательностью элементарных преобразований либо к единичной матрице, либо к матрице с нулевой строкой. Элементарные преобразования обратимы, поэтому каждую матрицу можно получить последовательностью элементарных преобразований либо из единичной матрицы, либо из матрицы с нулевой строкой. По свойству 1 и лемме 12.7.3 отсюда следует, что функция f определяется однозначно своими значениями на единичной матрице и на матрицах с нулевой строкой. По свойству 1 значение функции f на матрице с нулевой строкой равно нулю, а свойство 4 фиксирует ее значение на единичной матрице. Поэтому функция $f(A)$ определена однозначно. □

Следствие 12.8 (доказательства). *Матрица A обратима тогда и только тогда, когда ее определитель отличен от нуля.*

□

Из утверждения 12.6 и теоремы 12.7 следует, что свойства 1–4 можно рассматривать как *аксиоматическое определение* определителя матрицы. Утверждение 12.6 при этом можно воспринимать как доказательство существования определителя, а теорему 12.7 — как доказательство его единственности.

Пусть $\beta^1, \ldots, \beta^k \in \Lambda^1$ — произвольный набор грассмановых многочленов первой степени. Для их внешнего произведения $\beta^1 \wedge \cdots \wedge \beta^k$ мы будем использовать символ $\bigwedge\limits_{i=1}^{k} \beta^i$ (по аналогии с краткой записью суммы).

Утверждение 12.9. *Если $C = (c_j^i)$ — матрица размера $k \times k$, то*

$$\bigwedge_{i=1}^{k} \Big(\sum_{j=1}^{k} c_j^i \beta^j\Big) = (\det C) \bigwedge_{i=1}^{k} \beta^i. \tag{23}$$

Доказательство. Раскроем скобки в левой части (23), пользуясь дистрибутивностью внешнего умножения относительно сложения и ассоциативностью алгебры Грассмана. Мы получим сумму некоторых мономов степени k от $\beta_1, \dots, \beta_k$ с коэффициентами из поля $\Bbbk$. Воспользуемся упоминавшимися на прошлой лекции свойствами внешнего произведения грассмановых многочленов первой степени: $\beta^i \wedge \beta^i = 0$ и $\beta^i \wedge \beta^j = -\beta^j \wedge \beta^i$. Из этих свойств следует, что каждый ненулевой моном степени k от $\beta_1, \dots, \beta_k$ равен, с точностью до знака, $\bigwedge\limits_{i=1}^{k} \beta^i$. Если и этот моном равен нулю, то обе части равенства (23) равны нулю, то есть оно выполнено.

Пусть $\bigwedge\limits_{i=1}^{k} \beta^i \neq 0$. При раскрытии скобок в левой части (23) мы получим $\bigwedge\limits_{i=1}^{k} \beta^i$ с некоторым коэффициентом, зависящим от матрицы C. Этот коэффициент удовлетворяет свойствам 1–4 и, следовательно, совпадает с определителем матрицы C. □

Следствие 12.10. *Пусть A и B — две квадратные матрицы размера $n \times n$. Тогда* $\det(AB) = \det A \cdot \det B$.

Доказательство. Положим $\beta^i = \sum\limits_{j=1}^{n} b^i_j \xi^j$. По формуле (23)

$$\bigwedge_{i=1}^{n} \Big(\sum_{j=1}^{n} a^i_j \beta^j\Big) = (\det A) \bigwedge_{i=1}^{n} \beta^i.$$

В то же время

$$\bigwedge_{i=1}^{n} \beta^i = (\det B) \bigwedge_{i=1}^{n} \xi^i.$$

С другой стороны,

$$\sum_{j=1}^{n} a^i_j \beta^j = \sum_{j=1}^{n} a^i_j \Big(\sum_{k=1}^{n} b^j_k \xi^k\Big) = \sum_{k=1}^{n} \Big(\sum_{j=1}^{n} a^i_j b^j_k\Big) \xi^k,$$

поэтому

$$\bigwedge_{i=1}^{n} \Big(\sum_{j=1}^{n} a^i_j \beta^j\Big) = (\det AB) \bigwedge_{i=1}^{n} \xi^i,$$

откуда и следует равенство $\det(AB) = \det A \cdot \det B$. □

Мы знаем, что определитель обратимой матрицы отличен от нуля, то есть имеется отображение $\det : GL_n(\Bbbk) \to \Bbbk^*$. Доказанное нами равенство означает, что это отображение — гомоморфизм. Ядро этого гомоморфизма называется *специальной линейной группой* и обозначается через $SL_n(\Bbbk)$. Другими словами, специальную линейную группу образуют матрицы с определителем 1.

Задача 12.11. *Доказать, что матрицы вида $D(i, j; \alpha)$, отвечающие элементарным преобразованиям строк первого типа ($i \neq j$; см. лекцию 5), порождают группу $SL_n(\Bbbk)$.*

Обозначим множество $[1, n]$ через N. Для любого подмножества $I = \{i_1, \dots, i_k\} \subseteq N$ положим $\|I\| = i_1 + \dots + i_k$ (не путать с обозначением $|I| = \#I = k$).

Утверждение 12.12. *Пусть $I, J \subseteq N$, причем $|I| + |J| = n$. Тогда*

$$\xi^I \wedge \xi^J = \begin{cases} 0, & \text{если } I \cup J \neq N, \\ (-1)^{s(I)} \xi^N, & \text{если } I \cup J = N, \end{cases}$$

где

$$s(I) = \|I\| - \binom{|I| + 1}{2}.$$

Доказательство. По определению умножения в алгебре Грассмана

$$\xi^I \wedge \xi^J = \begin{cases} 0, & \text{если } I \cap J \neq \varnothing, \\ (-1)^{c(I,J)}\xi^{I\cup J}, & \text{если } I \cap J = \varnothing, \end{cases}$$

где

$$c(I,J) = \#\{(i,j) \in I \times J \mid i > j\}.$$

Ясно, что раз $|I| + |J| = n$, то $I \cap J = \varnothing$ тогда и только тогда, когда $I \cup J = N$. Поэтому надо только доказать, что $s(I) = c(I,J)$ при $J = N \setminus I$.

Пусть $|I| = k$. Перенумеруем элементы множества I в порядке возрастания: $I = \{i_1, \ldots, i_k\}$, $i_1 < \cdots < i_k$. Легко видеть, что для любого $t \in \{1, \ldots, k\}$ число элементов $j \in J$ таких, что $i_t > j$, равно $i_t - t$. Поэтому

$$c(I,J) = \sum_{t=1}^{k}(i_t - t) = \|I\| - \frac{k(k+1)}{2} = \|I\| - \binom{|I|+1}{2} = s(I).$$

□

Обозначим множество $[1,m]$ через M.

Определение 12.13. Пусть $B = (b^i_j)$ — матрица $m \times n$. Для любых подмножеств $I \subseteq M$ и $J \subseteq N$ обозначим через B^I_J подматрицу, составленную из элементов B, номера строк которых принадлежат I, а номера столбцов — J, то есть $B^I_J = (b^i_j)_{i \in I, j \in J}$. (Мы считаем, что строки и столбцы в подматрице расположены в порядке возрастания их номеров в матрице B.) *Минором* b^I_J порядка k, задаваемым k-элементными подмножествами $I \subseteq M$ и $J \subseteq N$, называется определитель подматрицы B^I_J.

Утверждение 12.14. *Пусть $B = (b^i_j)$ — матрица $m \times n$. Положим*

$$\beta^i = \sum_{j=1}^{n} b^i_j \xi^j \in \Lambda^1.$$

Тогда для любого подмножества $I = \{i_1, \ldots, i_k\} \subseteq M$, где $i_1 < \cdots < i_k$, выполнено равенство

$$\beta^I = \sum_{\substack{J \subseteq N, \\ |J| = k}} b^I_J \xi^J,$$

где

$$\beta^I = \bigwedge_{t=1}^{k} \beta^{i_k}.$$

Доказательство. Чтобы вычислить коэффициент при ξ^J в разложении β^I по стандартному базису алгебру Грассмана, можно заменить на 0 коэффициенты при ξ^j для $j \notin J$ в каждом из β^i. Тогда получается внешнее произведение грассмановых полиномов первой степени, отвечающих строкам матрицы B^I_J, равное, по определению минора, $b^I_J \xi^J$. □

Теорема 12.15 (Лапласа). *Пусть B — матрица $n \times n$. Фиксируем k-элементное подмножество $I \subseteq N$. Тогда имеет место формула:*

$$\det B = \sum_{\substack{J \subseteq N, \\ |J| = k}} (-1)^{\|J\| - \|I\|} b^I_J b^{N \setminus I}_{N \setminus J}.$$

Доказательство. Мы имеем

$$\bigwedge_{i=1}^{k}\beta^i = (-1)^{\binom{k+1}{2}-\|I\|}\beta^I\wedge\beta^{N\setminus I} =$$

$$= (-1)^{\binom{k+1}{2}-\|I\|}\Big(\sum_{|J|=k} b^I_J\xi^J\Big)\wedge\Big(\sum_{|J'|=n-k} b^{N\setminus I}_{J'}\xi^{J'}\Big) =$$

$$= (-1)^{\binom{k+1}{2}-\|I\|}\Big(\sum_{\substack{|J|=k,\\ |J'|=n-k}} b^I_J b^{N\setminus I}_{J'}\xi^J\wedge\xi^{J'}\Big).$$

Но внешнее произведение $\xi^J\wedge\xi^{J'}$ отлично от нуля лишь при $J' = N\setminus J$, когда

$$\xi^J\wedge\xi^{J'} = (-1)^{\|J\|-\binom{k+1}{2}}\bigwedge_{i=1}^{n}\xi^i.$$

Поэтому получаем, что

$$\bigwedge_{i=1}^{k}\beta^i = \sum_{|J|=k}(-1)^{\|J\|-\|I\|} b^I_J b^{N\setminus I}_{N\setminus J}\bigwedge_{i=1}^{n}\xi^i.$$

Остается сравнить это равенство с определением определителя матрицы B. □

Множитель $(-1)^{\|J\|-\|I\|}b^{N\setminus I}_{N\setminus J}$ при миноре b^I_J, входящем в разложение определителя матрицы B по теореме Лапласа, называется *алгебраическим дополнением* этого минора.

Следствие 12.16. *Пусть* $d = \det B \neq 0$. *Обозначим через* a^i_j *алгебраическое дополнение элемента* b^i_j, *рассматриваемого как минор порядка* 1, *то есть* $a^i_j = (-1)^{j-i}\det B^{N\setminus\{i\}}_{N\setminus\{j\}}$. *Положим* $C = (c^i_j)$, *где* $c^i_j = d^{-1}a^j_i$. *Тогда* $C = B^{-1}$.

Доказательство. Из теоремы Лапласа в частном случае $I = \{i\}$ получаем *формулу разложения определителя по i-той строке*

$$\det B = \sum_{j=1}^{n} b^i_j a^i_j. \tag{24}$$

Изменим теперь матрицу B, заменив в ней k-тую строку на i-тую. При $k\neq i$ полученная матрица имеет две одинаковые строки и, следовательно, определитель ее равен нулю. Разлагая его по k-той строке, получаем

$$\delta^i_k\det B = \sum_{j=1}^{n} b^i_j a^k_j.$$

Разделим обе части этого равенства на d:

$$\delta^i_k = \sum_{j=1}^{n} b^i_j c^j_k,$$

то есть $E = BC$. Матрица B обратима (как имеющая ненулевой определитель), поэтому $B^{-1} = C$.
□

Задача 12.17. *Пусть* $A = (a^i_j)$ — *матрица* $m\times n$, *а* $B = (b^j_i)$ — *матрица* $n\times m$, *причем* $n\geqslant m$. *Выразить* $\det(AB)$ *через миноры (размера* $m\times m$*) матриц* A *и* B.

Напоследок несколько слов о практическом вычислении определителей. Раскрывать произведение грассмановых полиномов или вычислять знакопеременную сумму по симметрической группе (как в утверждении 12.3) — занятие, как правило, неблагодарное. Гораздо полезнее оказываются обычно лемма 12.7.3 (об инвариантности определителя относительно элементарных преобразований первого типа) и теорема Лапласа, особенно разложение определителя по строке. Равенство $\det A^t = \det A$ позволяет перенести эти утверждения на столбцы матрицы A.

Рассмотрим пару примеров.

Пример 12.18 (Определитель Вандермонда). Положим

$$\Delta_n(x_1,\dots,x_n) = \begin{vmatrix} 1 & 1 & \dots & 1 \\ x_1 & x_2 & \dots & x_n \\ (x_1)^2 & (x_2)^2 & \dots & (x_n)^2 \\ \vdots & \vdots & \ddots & \vdots \\ (x_1)^{n-1} & (x_2)^{n-1} & \dots & (x_n)^{n-1} \end{vmatrix}.$$

Применим к этой матрице следующую последовательность элементарных преобразований первого типа: вычтем из n-ой строки $(n-1)$-ую, умноженную на x_1, затем вычтем из $(n-1)$-ой строки $(n-2)$-ую, умноженную на x_1 и т. д. Получиттся

$$\Delta_n(x_1,\dots,x_n) = \begin{vmatrix} 1 & 1 & \dots & 1 \\ 0 & x_2 - x_1 & \dots & x_n - x_1 \\ 0 & (x_2)^2 - x_1 x_2 & \dots & (x_n)^2 - x_1 x_2 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & (x_2)^{n-1} - x_1 (x_2)^{n-2} & \dots & (x_n)^{n-1} - x_1 (x_n)^{n-2} \end{vmatrix}.$$

Разложим теперь определитель по первому столбцу:

$$\Delta_n(x_1,\dots,x_n) = \begin{vmatrix} x_2 - x_1 & \dots & x_n - x_1 \\ (x_2)^2 - x_1 x_2 & \dots & (x_n)^2 - x_1 x_2 \\ \vdots & \ddots & \vdots \\ (x_2)^{n-1} - x_1 (x_2)^{n-2} & \dots & (x_n)^{n-1} - x_1 (x_n)^{n-2} \end{vmatrix}$$

и в полученном определителе вынесем из j-го столбца общий множитель $x_{j+1} - x_1$ $(j = 1,\dots,n-1)$. Мы получим выражение определителя Вандермонда n-го порядка через определитель Вандермонда $(n-1)$-го порядка:

$$\Delta_n(x_1,\dots,x_n) = \Big(\prod_{j=2}^{n}(x_j - x_1)\Big)\Delta_{n-1}(x_2,\dots,x_n).$$

С помощью индукции по n из этого выражения получается окончательный ответ:

$$\Delta_n(x_1,\dots,x_n) = \prod_{i<j}(x_j - x_i).$$

Пример 12.19 (Числа Фибоначчи). Положим $f_1 = 1$ и

$$f_{n+1} = \begin{vmatrix} 1 & 1 & 0 & \cdots & 0 & 0 & 0 \\ -1 & 1 & 1 & \ddots & 0 & 0 & 0 \\ 0 & -1 & 1 & \ddots & 0 & 0 & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \ddots & 1 & 1 & 0 \\ 0 & 0 & 0 & \ddots & -1 & 1 & 1 \\ 0 & 0 & 0 & \cdots & 0 & -1 & 1 \end{vmatrix}$$

— определитель порядка n. Разложим этот пределитель по первой строке

$$f_{n+1} = \begin{vmatrix} 1 & 1 & \ddots & 0 & 0 & 0 \\ -1 & 1 & \ddots & 0 & 0 & 0 \\ \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \ddots & 1 & 1 & 0 \\ 0 & 0 & \ddots & -1 & 1 & 1 \\ 0 & 0 & \cdots & 0 & -1 & 1 \end{vmatrix} - \begin{vmatrix} -1 & 1 & \ddots & 0 & 0 & 0 \\ 0 & 1 & \ddots & 0 & 0 & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \ddots & 1 & 1 & 0 \\ 0 & 0 & \ddots & -1 & 1 & 1 \\ 0 & 0 & \cdots & 0 & -1 & 1 \end{vmatrix}$$

Разложив второй из этих определителей по первому столбцу, получим рекуррентную формулу

$$f_{n+1} = f_n + f_{n-1},$$

причем $f_2 = f_1 = 1$. Последовательность (f_n) этими формулами определена однозначно. Как вы уже знаете, она называется *последовательностью Фибоначчи*.

Задачи

Листок №1.

1) Найти модуль и аргумент следующих комплексных чисел:

$$-4, \quad 1+i, \quad 1-i\sqrt{3}, \quad \sin\alpha + i\cos\alpha, \quad \frac{1+i\operatorname{tg}\alpha}{1-i\operatorname{tg}\alpha}, \quad 1+\cos\alpha + i\sin\alpha.$$

2) Вычислить

$$\frac{(5+i)(7-6i)}{3+i}; \quad \frac{(1+i)^5}{(1-i)^3}; \quad \frac{(1+3i)(8-i)}{(2+i)^2}.$$

3) Найти x и y, считая их вещественными:

$$(1+2i)x + (3-5i)y = 1-3i.$$

4) Решить уравнения:

$$z^2 = i; \qquad z^2 = 5-12i; \qquad z^2 + (2i-7)z + 13 - i = 0.$$

5) Найти все z:

$$\bar{z} = z^2; \qquad \bar{z} = z^3.$$

6) Вычислить

$$(1+i\sqrt{3})^{150}; \qquad \left(\frac{\sqrt{3}+i}{1-i}\right)^{30}; \qquad (1+\cos\alpha + i\sin\alpha)^k.$$

7) Есть 4 попарно различных чашки и 4 одинаковых стакана. Имеется также 10 одинаковых кусков сахара и 10 попарно различных ложечек. Сколькими способами можно разложить

   а) ложки по чашкам;
   б) сахар по чашкам;
   в) сахар по чашкам так, чтобы пустых чашек не осталось;
   г) сахар по стаканам;
   д) ложки по стаканам?

8) Раскройте скобки у $(a_1 + \dots + a_m)^2$ и $(a+b+c)^3$.

9) Чему равен коэффициент при $a_1^{k_1} \dots a_m^{k_m}$ после раскрытия скобок и приведения подобных членов в выражении $(a_1 + \dots + a_m)^n$?

10) Вычислить:

   а) $$\binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{n};$$

   б) $$\binom{n}{0} - \binom{n}{1} + \dots + (-1)^n\binom{n}{n};$$

   в) $$\binom{n}{0}^2 + \binom{n}{1}^2 + \dots + \binom{n}{n}^2;$$

г) $$\binom{n}{0}-\binom{n}{2}+\binom{n}{4}-\binom{n}{6}+\ldots;$$

д) $$\binom{n}{0}-\binom{n}{4}+\binom{n}{8}+\ldots.$$

11) Выразить $\sin^4 x$ и $\cos^5 x$ через первые степени $\sin$ и $\cos$ от кратных аргументов.

12) Выразить $\cos nx$ и $\sin nx$ через $\cos x$ и $\sin x$.

13) Вычислить:

а) $$\sin x+\sin 2x+\cdots+\sin nx;$$

б) $$\sin^2 x+\sin^2 3x+\cdots+\sin^2(2n-1)x;$$

в) $$\cos x+2\cos 2x+\cdots+n\cos nx.$$

Листок №1. Дополнительные задачи.

1) Вычислить:

а) $$\binom{2n}{0}^2-\binom{2n}{1}^2+\binom{2n}{2}^2-\cdots+\binom{2n}{2n}^2;$$

б) $$\binom{n}{1}+\binom{n}{5}+\binom{n}{9}+\ldots;$$

в) $$\binom{n}{1}-\frac{1}{3}\binom{n}{5}+\frac{1}{9}\binom{n}{9}-\ldots.$$

2) Вычислить:

а) Сумму и произведение всех корней степени n из 1.

б) Сумму и произведение s-х степеней всех корней степени n из 1.

в) $1+2\varepsilon+3\varepsilon^2+\cdots+n\varepsilon^{n-1}$, где $\varepsilon^n=1$.

3) Доказать, что всякое комплексное число z, $|z|=1$, $z\neq -1$, может быть представлено в виде
$$z=\frac{1+ti}{1-ti},\qquad t\in\mathbb{R}.$$

4) Доказать, что если $z+1/z=2\cos\theta$, то $z^m+1/z^m=2\cos m\theta$.

5) Доказать, что вещественная и мнимая части любого корня квадратного уравнения с комплексными коэффициентами выражаются в радикалах через вещественные и мнимые части коэффициентов уравнения.

6) Выразить в радикалах $\cos\dfrac{2\pi}{5}$ и $\sin\dfrac{4\pi}{5}$.

Листок № 2.

1) Пусть $f(x)=\sum\limits_{k=0}^{n} a_k x^k$ — многочлен над полем $\Bbbk$. Производной этого многочлена называется многочлен $f'(x)=\sum\limits_{k=1}^{n} k a_k x^{k-1}$. Предположим, что характеристика поля $\Bbbk$ равна нулю.

   а) Доказать, что $x_0\in\Bbbk$ является корнем кратности m многочлена $f(x)$ в том и только том случае, когда $f(x_0)=f'(x_0)=\dots=f^{(m-1)}(x_0)=0$, но $f^{(m)}(x_0)\neq 0$.

   б) Доказать, что для любого многочлена степени n и любого $x_0\in\Bbbk$ имеет место формула Тейлора:
$$f(x)=\sum_{k=0}^{n}\frac{f^{(k)}(x_0)}{k!}(x-x_0)^k.$$

   в) Верно ли утверждение из пункта а), если $\operatorname{char}\Bbbk\neq 0$?

2) Определить $a\in\mathbb{C}$ и $b\in\mathbb{C}$ так, чтобы многочлен $ax^{n+1}+bx^n+1$ делился на $(x-1)^2$.

3) а) Доказать, что многочлен над полем $\Bbbk$ характеристики нуль делится на свою производную тогда и только тогда, когда он равен $a_0(x-x_0)^n$ для некоторых $a_0,x_0\in\Bbbk$ и $n\in\mathbb{N}$.

   б) Верно ли это при $\operatorname{char}\Bbbk\neq 0$?

4) Пусть характеристика поля $\Bbbk$ равна нулю. Определим в кольце формальных степенных рядов $\Bbbk[[t]]$ элементы $e^{\alpha t}=\sum\limits_{k=0}^{\infty}\frac{\alpha^k}{k!}t^k$ для всех $\alpha\in\Bbbk$. Доказать, что для любых $\alpha,\beta\in\Bbbk$ выполнено равенство $e^{\alpha t}e^{\beta t}=e^{(\alpha+\beta)t}$.

5) Пусть в кольце $\mathbb{Q}[[t]]$ формальных степенных рядов с рациональными коэффициентами задано такое семейство рядов $F_a(t)$ для всех $a\in\mathbb{Q}$, что $F_1(t)=1+t$ и $F_a(t)F_b(t)=F_{a+b}(t)$ для любых $a,b\in\mathbb{Q}$. Доказать, что $F_a(t)$ определяются этими условиями однозначно, т. е. $F_a(t)=(1+t)^a$. Верно ли это, если поле $\mathbb{Q}$ заменить на поле $\mathbb{Q}\left[\sqrt{2}\right]$?

6) Для числа способов разложить k кусков сахара по n стаканам написать

   а) рекуррентную формулу;

   б) производящую функцию (при фиксированном числе стаканов n).

7) Рассмотрим пути на вещественной прямой, состоящие из отрезков длины 1 вправо или влево, начинающиеся в 0 и не заходящие в отрицательную сторону. Найти производящую функцию для числа таких путей длины k, кончающихся

   а) в 0;

   б) в точке $n>0$.

8) Рассмотрим пути на плоскости, состоящие из отрезков длины 1, идущих на север, восток или запад (на юг идти нельзя). Найти производящую функцию для числа таких путей длины k, начинающихся в 0 и не самопересекающихся.

9) Доказать, что каждое натуральное число можно представить в виде суммы различных натуральных чисел столькими же способами, сколькими его можно представить в виде суммы нечетных натуральных чисел (некоторые из которых могут совпадать).

10) Пусть M и N — конечные множества, $|M|=m$ и $|N|=n$. Найти

   а) число всех отображений $M\to N$;

   б) число инъективных отображений $M\to N$;

   в) число сюръективных отображений $M\to N$.

Листок № 3.

1) Доказать, что

   а) Отображение множества M в множество N является инъективным тогда и только тогда, когда оно имеет левое обратное отображение.

   б) Отображение множества M в множество N является сюръективным тогда и только тогда, когда оно имеет правое обратное отображение.

2) Пусть на плоскости заданы два отрезка:

$$X = [(0,0),(3,1)] \qquad \text{и} \qquad Y = [(0,0),(1,-4)].$$

   Сколько точек пересечения имеют их образы при канонической проекции на тор?

3) Пусть G — группа движений ромба (не являющегося квадратом).

   а) Найти порядок группы G.

   б) Найти орбиты вершин ромба и их стационарные подгруппы.

4) Пусть G — группа движений правильного шестиугольника.

   а) Найти порядок группы G.

   б) Найти все точки плоскости, для которых порядок стабилизатора в группе G больше 1.

5) Найти порядок стационарной группы вершины для группы вращений

   а) диэдра;

   б) тетраэдра;

   в) куба;

   г) октаэдра;

   д) икосаэдра;

   е) додекаэдра.

6) Под группой многогранника мы будем понимать группу *вращений* многогранника. Найти порядок

   а) группы диэдра;

   б) группы тетраэдра;

   в) группы куба;

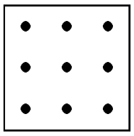
   г) группы икосаэдра.

7) Пусть группа G преобразований множества M коммутативна, то есть $ab = ba$ для любых $a, b \in G$. Доказать, что если для некоторых $g \in G$ и $m_0 \in M$ справедливо равенство $gm_0 = m_0$, то $gm = m$ для любой точки m, лежащей в одной орбите с точкой m_0.

8) Сколько существует различных ожерелий из 6 бусин, каждая из которых может быть красного, синего или желтого цвета?

   (Указание: использовать теорему Бернсайда).

9) В городе N талоны на автобус имеют форму квадрата, а компостер пробивает от одной до девяти из возможных дырочек, показанных на рисунке



По пробитому талончику невозможно узнать, как он был вставлен (лицом или изнанкой, и как повернут). Известно, что по талончику, пробитому в одном автобусе, нельзя проехать на другом автобусе. Каково максимальное число автобусов в городе N?

Листок № 4.

1) Доказать, что если порядок любого нееденичного элемента группы G равен двум, то группа G — абелева. Привести пример такой группы более чем из двух элементов.

2) Пусть G — произвольная группа, $a, b \in G$, причем порядок их произведения ab равен n. Каким может быть порядок элемента ba?

3) Найти знак перестановки $\begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ n & n-1 & n-2 & \dots & 2 & 1 \end{pmatrix}$.

4) Пусть $\sigma \in S_n$ — нечетная перестановка и N — ее порядок в группе S_n. Что можно сказать про четность N?

5) Рассмотрим перестановку $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix} \in S_5$. Найти σ^{100}.

6) Доказать, что непустое подмножество H конечной группы G является подгруппой, если H замкнуто относительно умножения (т. е. в данном случае требование существования в H обратных элементов излишне). Верно ли это для бесконечной группы G?

7) Какие подгруппы имеет группа S_3? Найти для них левые и правые смежные классы.

8) Любое коммутативное кольцо можно рассматривать как группу по сложению; если $\Bbbk$ — поле, то множество его ненулевых элементов образует группу по умножению, которая обозначается через $\Bbbk^*$. Через $\mathbb{R}_+^*$ обозначается группа положительных вещественных чисел по умножению. Доказать, что а) группы $\mathbb{R}$ и $\mathbb{R}_+^*$ изоморфны; б) группы $\mathbb{Z}$ и $\mathbb{Q}$ неизоморфны; в) группы $\mathbb{Q}$ и $\mathbb{Q}^*$ неизоморфны.

9) Пусть $\sigma \in S_n$ — цикл длины k, а $\tau \in S_n$ — произвольная перестановка. Доказать, что $\tau\sigma\tau^{-1}$ — цикл длины k. Какие элементы входят в этот цикл, если $\sigma = (1, 2, \dots, k)$?

10) Найти классы сопряженных элементов для а) группы диэдра D_n; б) симметрической группы S_n.

Листок № 4. Дополнительные задачи

1) Пусть $\{1, \dots, n\} = I_1 \sqcup I_2 \sqcup \dots \sqcup I_k$ — разбиение множества $\{1, \dots, n\}$ на орбиты перестановки $\sigma \in S_n$. Определим *декремент* перестановки формулой

$$d(\sigma) = \sum_{l=1}^{k} (|I_l| - 1) = n - k.$$

а) Доказать, что знак перестановки σ равен $(-1)^{d(\sigma)}$.

б) Доказать, что перестановку σ можно представить в виде произведения $d(\sigma)$ транспозиций.

в) Доказать, что перестановку σ нельзя представить в виде произведения менее чем $d(\sigma)$ транспозиций.

2) Доказать, что

а) группа диэдра D_3 изоморфна симметрической группе S_3;

б) группа тетраэдра T изоморфна знакопеременной группе A_4;

в) группа куба C изоморфна симметрической группе S_4;

г) группа икосаэдра I изоморфна знакопеременной группе A_5.

3) Доказать, что симметрическая группа S_n порождена транспозицией (12) и циклом $(123\ldots n)$.

4) Доказать, что знакопеременная группа A_n, $n \geqslant 3$, порождается циклами длины 3, причем на самом деле

$$A_n = \langle (123), (124), \ldots, (12n) \rangle.$$

Листок № 5.

1) Доказать, что если подгруппа $H \subset G$ имеет индекс 2, то она нормальна.

2) Какие подгруппы группы S_3 являются нормальными?

3) Доказать, что группа S_4 имеет, кроме себя самой и единичной подгруппы, лишь следующие нормальные подгруппы:

а) знакопеременная группа A_4;

б) «четверная группа Клейна» V_4, состоящая из перестановок:

$$e, \quad (12)(34), \quad (13)(24), \quad (14)(23).$$

Показать, что последняя группа абелева.

4) Доказать, что $S_4/V_4 \cong S_3$.

5) Доказать, что если A — циклическая группа порядка n и d — делитель n, то A содержит ровно одну подгруппу порядка d, причем эта подгруппа циклическая.

6) Доказать, что любая группа четного порядка содержит хотя бы один элемент порядка 2.

7) Всегда ли а) инъективный гомоморфизм групп имеет левый обратный гомоморфизм? б) сюръективный гомоморфизм групп имеет правый обратный гомоморфизм?

8) Найти $Z(G)$, $\operatorname{Int} G$, $\operatorname{Aut} G$ для а) группы μ_n комплексных корней из единицы степени n при $n = 2,3,4,5,6$; б) группы диэдра D_n при $n = 3,4$; в)* симметрической группы S_4; г)* знакопеременной группы A_4.

9) Доказать, что

а) симметрическая группа S_3 изоморфна группе, заданной образующими s_1, s_2 и соотношениями $s_1^2 = e, s_2^2 = e$, $(s_1 s_2)^3 = e$;

б)* симметрическая группа S_4 изоморфна группе, заданной образующими s_1, s_2, s_3 и соотношениями $s_1^2 = e, s_2^2 = e, s_3^2 = e$, $(s_1 s_2)^3 = e$, $(s_1 s_3)^2 = e$, $(s_2 s_3)^3 = e$.

Листок № 6.

1) Доказать, что в конечной абелевой группе порядка n для любого $d \mid n$ существует хотя бы одна подгруппа порядка d.

2) Изоморфны ли группы $\mathbb{Z}_{12} \oplus \mathbb{Z}_{72}$ и $\mathbb{Z}_{18} \oplus \mathbb{Z}_{48}$?

3) Описать все гомоморфизмы $S_3 \to S_3$.

4) Сколько элементов симметрической группы S_4 остаются неподвижными при сопряжении перестановкой $(1,2)(3,4)$?

5) Группа G задана образующими a, b и соотношениями $ab^2 = ba$, $ba^2 = ab$. Каков порядок группы G?

6) Обозначим через C группу вращений куба с вершинами в точках $(\pm 1, \pm 1, \pm 1)$. Пусть T — группа вращений тетраэдра с вершинами в точках $(-1,-1,-1)$, $(1,1,-1)$, $(1,-1,1)$ и $(-1,1,1)$. Доказать, что T — нормальная подгруппа группы C.

7) Пусть N и M — две нормальные подгруппы группы G, причем $N \cap M = \{e\}$. Доказать, что $ab = ba$ для любых $a \in N$, $b \in M$.

8) Доказать, что если произведение двух любых левых смежных классов группы G по подгруппе H снова является левым смежным классом, то H — нормальная подгруппа в G.

9) Перечислить все группы порядка $\leqslant 6$ с точностью до изоморфизма.

10) Сколько подгрупп конечного индекса в группе $\mathbb{R}^*$ ненулевых действительных чисел по умножению?

11) Доказать, что для любой группы G группа ее внутренних автоморфизмов $\operatorname{Int} G$ является нормальной подгруппой группы всех автоморфизмов $\operatorname{Aut} G$.

12)* Пусть p — наименьшее простое число, делящее порядок конечной группы G, $H \subset G$ — подгруппа индекса p. Доказать, что H — нормальная подгруппа в G.

Листок № 7.

1) Найти инвариантные множители группы $\mathbb{Z}_{18} \oplus \mathbb{Z}_{15} \oplus \mathbb{Z}_{20}$.

2) Докажите, что уравнение $15x^2 - 7y^2 = 9$ не имеет решений в целых числах.

3) Доказать, что длина хотя бы одной стороны пифагорова треугольника (прямоугольного треугольника с целыми длинами сторон) делится на 5.

4) Докажите, что

   а) класс вычетов $[k]_m$ обратим в $\mathbb{Z}_m$ $\Leftrightarrow$ $[k]_m$ не является делителем нуля в $\mathbb{Z}_m$ $\Leftrightarrow$ $(k, m) = 1$.

   б) Кольцо $\mathbb{Z}_m$ является полем $\Leftrightarrow$ m — простое.

5) а) Найти все такие $x \in \mathbb{Z}_p$ (p — простое), что $x^2 = 1$.

   б) Чему равно произведение всех ненулевых чисел в $\mathbb{Z}_p$ (p — простое)?

   в) Доказать терему Вильсона: Число p является простым тогда и только тогда, когда $(p-1)! + 1 \equiv 0 \pmod{p}$.

6) Доказать, что ровно половина чисел в $\mathbb{Z}_p^*$ является квадратами (p — простое, $p > 2$, $\mathbb{Z}_p^* = \{x \in \mathbb{Z}_p \mid x \neq 0\}$).

7) Доказать, что уравнение $x^2 + y^2 = -1$ всегда разрешимо в кольце $\mathbb{Z}_p$ (p — простое).

8) Найти остаток 3^{1000} по модулю 13.

9) а) Доказать, что если $m_1, \ldots, m_k$ — попарно взаимно простые модули, а $a_1, \ldots, a_k$ — произвольные целые числа, то найдется такое $x \in \mathbb{Z}$, что $x \equiv a_i \pmod{m_i}$, причем x определен однозначно по модулю $m_1 \cdot \cdots \cdot m_k$ (китайская теорема об остатках).

б) Найти все $x \in \mathbb{Z}$ такие, что

$$\begin{cases} x \equiv 2 \pmod{7}, \\ x \equiv 3 \pmod{18}, \\ x \equiv 3 \pmod{13}. \end{cases}$$

10)* Решить сравнение: $2^n \equiv n \pmod{p}$ (p — простое).

Листок № 7. Дополнительные задачи.

1) Обозначим через $\varphi(m)$ число обратимых элементов в кольце $\mathbb{Z}_m$ (то есть количество натуральных чисел, меньших m и взаимно простых с m). Эта функция называется функцией Эйлера. Доказать теорему Эйлера:

Если класс вычетов $[a]_m$ обратим, то $a^{\varphi(m)} \equiv 1 \pmod{m}$.

2) Доказать, что если $m = p_1^{k_1} \cdot \cdots \cdot p_n^{k_n}$ (p_i — различные простые числа), то $\mathbb{Z}_m \cong \mathbb{Z}_{p_1^{k_1}} \times \cdots \times \mathbb{Z}_{p_n^{k_n}}$.

3) Доказать, что если кольцо $A \cong A_1 \times \cdots \times A_n$, то $A^* \cong A_1^* \times \cdots \times A_n^*$. Вывести отсюда, что функция Эйлера мультипликативна, т. е. если $(k, l) = 1$, то $\varphi(kl) = \varphi(k)\varphi(l)$.

4) Доказать, что если $m = p_1^{k_1} \cdot \cdots \cdot p_n^{k_n}$ (p_i — различные простые числа), то

$$\varphi(m) = m \cdot (1 - \frac{1}{p_1}) \cdot \cdots \cdot (1 - \frac{1}{p_n}).$$

5) Найти все m такие, что $\varphi(m) = 10$.

6) Доказать, что $\sum\limits_{d|m} \varphi(d) = m$.

7) а) Пусть $[a] \in \mathbb{Z}_m^*$. Назовем порядком вычета a наименьшее натуральное число k такое, что $[a]^k = [1]$. Доказать, что если порядки k_i вычетов a_i попарно взаимно просты, то порядок вычета $a = a_1 \cdot \cdots \cdot a_n$ равен $k = k_1 \cdot \cdots \cdot k_n$.

б) Если существуют вычеты порядков k и l, то существует вычет порядка НОК(k, l) (наименьшее общее кратное k и l).

в) Назовем первообразным корнем такой обратимый вычет, что любой другой обратимый вычет является его степенью. Доказать, что существует первообразный корень по модулю p (p — простое).

8)* а) Пусть g — первообразный корень по модулю p (p — простое, $p > 2$). Доказать, что для некоторого натурального числа t число u, определенное равенством $(g + pt)^{p-1} = 1 + pu$, не делится на p. Доказать, что тогда $g + pt$ будет первообразным корнем по модулю p^k для любого $k \in \mathbb{N}$.

б) Доказать, что существует первообразный корень по модулю $2 \cdot p^k$.

9) Существует ли первообразный корень по модулю 21?

Листок № 8.

1) Для многочленов $a(t)=t^5-1$ и $b(t)=t^4+t^2+1$

   а) найти их наибольший общий делитель $d(t)$;

   б) найти такие многочлены $x(t)$ и $y(t)$, что $a(t)x(t)+b(t)y(t)=d(t)$.

2) Привести примеры делителей нуля в кольце непрерывных функций на $[0,1]$.

3) Доказать, что кольцо $\Bbbk[x,y]$ многочленов от двух переменных не является кольцом главных идеалов.

4) Сколько корней имеет уравнение $x^7=35$ в $\mathbb{Z}_{601}$?

5) Решить уравнение

   а) $x^3=10$ в $\mathbb{Z}_{37}$;

   б) $6x^3+27x^2+17x+20=0$ в $\mathbb{Z}_{30}$.

6) Рассмотрим многочлен $f(x)=x^2-a^2\in\mathbb{F}_q[x]$, где $a\in\mathbb{F}_q$. Сколько может быть обратимых элементов в кольце $\mathbb{F}_q[x]/(f(x))$?

7) Рассмотрим многочлен $f(x)=x^2+1$ над полем $\mathbb{F}_3$. Доказать, что факторкольцо $\mathbb{F}_3[x]/(f(x))$ является полем. Указать какой-нибудь многочлен, образ которого при канонической проекции $\mathbb{F}_3[x]\to\mathbb{F}_3[x]/(f(x))$ является образующей мультипликативной группы этого поля.

8) Будет ли факторкольцо $\mathbb{R}[x]/(f(x))$ полем, если

   а) $f(x)=x^4+1$?

   б) $f(x)=x^2+3$?

9) Пусть $f(x)=x^3+b\in\mathbb{F}_7[x]$. Для каких $b\in\mathbb{F}_7$ существует ненулевой гомоморфизм колец $\mathbb{F}_7[x]/(f(x))\to\mathbb{F}_7$?

10) Описать все идеалы в кольце $\Bbbk[[x]]$ формальных степенных рядов над полем $\Bbbk$. Какие из них являются максимальными?

Листок № 9.

1) Пусть p — простое число. Найти в поле $\mathbb{F}_p$ все решения уравнения $y^2=x^p-x+1$.

2) Доказать, что число примитивных корней из 1 степени n в произвольном поле $\mathbb{F}$ либо равно нулю, либо равно $\varphi(n)$, где $\varphi(n)$ — функция Эйлера: количество натуральных чисел m таких, что $m\leqslant n$ и $(m,n)=1$.

3) а) Для каких натуральных k и n число p^n-1 делится на p^k-1 (число p — простое)?

   б) Для каких q_1 и q_2 существует нетривиальный гомоморфизм $\mathbb{F}_{q_1}\to\mathbb{F}_{q_2}$?

4) Доказать, что в кольце $\Bbbk[x]$, где $\Bbbk$ — поле, бесконечно много неприводимых многочленов.

5) Доказать, что множество решений уравнения $x^{p^k}-x=0$ в поле характеристики p образует подполе.

6) Какова максимальная степень неприводимого многочлена над $\mathbb{F}_p$, делящего $x^{p^k}-x$?

7) Сколько неприводимых многочленов степеней 2 и 3 над полем $\mathbb{F}_q$?

8) Пусть $R=\{m+ni\in\mathbb{C}\mid m,n\in\mathbb{Z}\}$ — кольцо целых гауссовых чисел.

а) Существует ли такой идеал $J \subseteq R$, что факторкольцо R/J является полем характеристики 2? Если да, то сколько элементов в нем может быть?

б) Существует ли такой идеал $J \subseteq R$, что факторкольцо R/J является полем характеристики 3? Если да, то сколько элементов в нем может быть?

9) Доказать, что группа автоморфизмов конечного поля $\mathbb{F}_q$ порождена автоморфизмом Фробениуса $a \mapsto a^p$, где p — простое число и $q = p^k$. Каков порядок этой группы?

10) Доказать, что любой неприводимый многочлен $f(x) \in \mathbb{F}_p[x]$, имеющий корень в $\mathbb{F}_{p^k}$, разлагается в $\mathbb{F}_{p^k}[x]$ на линейные множители.

Листок № 10.

1) Вычислить $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n$, $\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}^n$, $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}^n$, $\begin{pmatrix} a & 1 \\ 0 & b \end{pmatrix}^n$;

2) Доказать, что если $A^n = 0$ (т. е. матрица A нильпотентна), то матрицы $(E \pm A)$ обратимы.

3) Найти: $\begin{pmatrix} 1 & 1 \\ 1 & a+1 \end{pmatrix}^{-1}$, $\begin{pmatrix} 1 & a & 0 \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}^{-1}$, $\begin{pmatrix} 1 & a & 0 \\ 0 & 1 & 0 \\ 0 & b & 1 \end{pmatrix}^{-1}$, $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1}$.

4) Найти все матрицы, коммутирующие с матрицей $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & a \end{pmatrix}$.

5) Найти все квадратные матрицы размера $n \times n$, коммутирующие с любой матрицей того же размера.

6) а) Пусть $A, B, \ldots, D_1$ — квадратные матрицы одного порядка. Выразить произведение матриц $\begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix}$ через заданные матрицы.

б) Придумать и доказать аналогичную формулу для прямоугольных матриц.

7) а) В кольце $M_2(\mathbb{R})$ найти подкольцо, изоморфное полю $\mathbb{C}$.

б) В кольце $M_2(\mathbb{C})$ найти подкольцо, изоморфное телу кватернионов.

8) Сколько элементов в группе $GL_2(\mathbb{F}_q)$?

9) Сколько в пространстве $\mathbb{F}_q^n$ а) элементов? б) одномерных линейных подпространств? в) двумерных линейных подпространств?

10) Доказать, что $GL_2(\mathbb{F}_2) \cong S_3$.

11) Найти все (с точностью до изоморфизма) двумерные ассоциативные алгебры с единицей над полем вещественных чисел.

12) Доказать, что любая конечномерная ассоциативная алгебра с единицей над полем $\Bbbk$ изоморфна подалгебре алгебры матриц $M_n(\Bbbk)$ (для некоторого $n \in \mathbb{N}$).

Листок № 11.

1) Пусть E_{ij} — матрица из алгебры M_n, у которой элемент, стоящий на пересечении i-й строки с j-м столбцом, равен 1, а остальные элементы равны нулю. Доказать, что матрицы E_{12}, E_{23}, E_{31} составляют систему образующих в M_3. Обобщить этот факт для любого n.

2) Вычислить определители:

а)

$$\begin{vmatrix} a_1 & 0 & \dots & 0 & b_1 \\ 0 & a_2 & \dots & b_2 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & b_{2n-1} & \dots & a_{2n-1} & 0 \\ b_{2n} & 0 & \dots & 0 & a_{2n} \end{vmatrix};$$

б)

$$\begin{vmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-2} & x_1^n \\ 1 & x_2 & x_2^2 & \dots & x_2^{n-2} & x_2^n \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & x_n & x_n^2 & \dots & x_n^{n-2} & x_n^n \end{vmatrix}.$$

3) Пусть $\Lambda^\bullet = \Lambda^\bullet(\xi^1, \xi^2, \xi^3, \xi^4)$ — алгебра Грассмана над полем $\Bbbk$. Элемент $\omega \in \Lambda^2$ называется разложимым, если найдутся $\beta^1, \beta^2 \in \Lambda^1$ такие, что $\omega = \beta^1 \wedge \beta^2$. Для произвольных $a, b, c, d, x \in \Bbbk$ рассмотрим следующий элемент из Λ^2:

$$\omega = \xi^1 \wedge \xi^2 + a\xi^1 \wedge \xi^3 + b\xi^1 \wedge \xi^4 + c\xi^2 \wedge \xi^3 + d\xi^2 \wedge \xi^4 + x\xi^3 \wedge \xi^4.$$

Пусть a, b, c, d — фиксированы. При каких x элемент ω является разложимым?

4) Рассмотрим в грассмановой алгебре $\Lambda^\bullet(\xi^1, \xi^2, \xi^3)$ над полем $\Bbbk$ следующие элементы: $\beta^1 = \xi^1 + \xi^2$, $\beta^2 = \xi^2 + \xi^3$ и $\beta^3 = \xi^1 + a\xi^3$. При каких значениях a моном $\xi^1 \wedge \xi^2$ принадлежит подалгебре, порожденной β^1, β^2 и β^3?

Программа зачета и задачи экзамена

Отображения и группы

1) Отображения множеств. Теорема о факторизации отображения.

2) Преобразования множества, симметрическая группа. Разложение перестановки в произведение независимых циклов.

3) Инверсии, знак перестановки. Знакопеременная группа.

4) Группы преобразований. Орбита, стабилизатор, неподвижные точки. Теорема Бернсайда.

5) Группы, абелевы группы. Подгруппы, смежные классы. Теорема Лагранжа. Циклические группы. Порядок элемента группы.

6) Гомоморфизмы групп. Действие группы на множестве. Теорема Кэли. Автоморфизмы, внутренние автоморфизмы.

7) Классы сопряженных элементов. Описание классов сопряженных элементов в симметрической группе.

8) Нормальные подгруппы, факторгруппы. Теорема о гомоморфизмах групп.

9) Свободные группы, задание групп образующими и соотношениями. Универсальность группы, заданной образующими и соотношениями.

10) Прямые суммы абелевых групп. Классификация конечных абелевых групп. Инвариантные множители.

Коммутативные кольца и поля

1) Определения кольца и поля. Поле комплексных чисел. Его геометрическая интерпретация. Формула Муавра.

2) Биномиальные коэффициенты. Кольцо многочленов. Теорема Безу.

3) Кольцо формальных степенных рядов. Общая формула бинома Ньютона.

4) Формальные степенные ряды как производящие функции. Число разбиений. Формула Эйлера.

5) Гомоморфизмы колец. Идеалы. Теорема о гомоморфизмах колец. Кольца классов вычетов.

6) Кольца главных идеалов. Максимальные идеалы. Теорема о факторкольце по идеалу, порожденному неприводимым элементом.

7) Евклидовы кольца. Факториальность евклидовых колец.

8) Целые гауссовы числа. Представление натурального числа в виде суммы двух квадратов.

9) Характеристика поля. Число элементов конечного поля. Мультипликативная группа конечного поля. Единственность конечного поля с заданным числом элементов с точностью до изоморфизма.

10) Существование конечного поля из p^k элементов (p — простое).

Линейные пространства и матрицы

1) Арифметические линейные пространства. Линейные отображения. Матрицы. Умножение матриц. Алгебра $M_n(\Bbbk)$.
2) Исследование обратимости матриц с помощью элементарных преобразований. Полная линейная группа $GL_n(\Bbbk)$.
3) Линейные пространства. Базис. Размерность.
4) Алгебры. Тело кватернионов.
5) Алгебра Грассмана. Ее ассоциативность.
6) Определитель матрицы (аксиоматическое определение). Построение определителя с помощью алгебры Грассмана и его единственность.
7) Определитель произведения матриц. Специальная линейная группа $SL_n(\Bbbk)$.
8) Миноры и их алгебраические дополнения. Теорема Лапласа.

Задачи к зачету по алгебре.

1) Группой Гамильтона называется следующая подгруппа мультипликативной группы алгебры кватернионов: $\Gamma = \{\pm 1, \pm i, \ \pm j, \pm k\}$, где $(1, i, j, k)$ — базис алгебры кватернионов. Является ли в ней нормальной подгруппой
   а) подгруппа, порожденная i?
   б) подгруппа, порожденная -1?
2) Изоморфны ли группа диэдра D_4 и группа Гамильтона $\Gamma = \{\pm 1, \pm i, \ \pm j, \pm k\}$, где $(1, i, j, k)$ — базис алгебры кватернионов?
3) Найти классы сопряженных элементов в группе Гамильтона $\Gamma = \{\pm 1, \pm i, \ \pm j, \pm k\}$, где $(1, i, j, k)$ — базис алгебры кватернионов.
4) При каких n группа диэдра D_4 (группа симметрий квадрата) может действовать на множестве из n элементов без неподвижных точек?
5) Пусть a_k — число разбиений k не более чем на m натуральных слагаемых (порядок слагаемых несуществен). Написать производящую функцию для последовательности (a_k).
6) Описать все гомоморфизмы колец $\mathbb{Z} \to \mathbb{F}_2[x]/(f(x))$, где
   а) $f(x) = x^2 + x + 1$;
   б) $f(x) = x^2 + 1$;
   в) $f(x) = x^2 + x$.
7) Найти все целочисленные решения системы сравнений
$$\begin{cases} x \equiv 3 \pmod 5, \\ x \equiv 4 \pmod 6, \\ x \equiv 5 \pmod 7. \end{cases}$$
8) Описать все идеалы и все подкольца колец $\mathbb{Z}/6\mathbb{Z}$ и $\mathbb{Z}/9\mathbb{Z}$.

9) Обозначим символом $[A, B]$ коммутатор $AB - BA$. Доказать, что для любых квадратных матриц A, B, C выполняются равенства:

   а) $[A, BC] = [A, B]C + B[A, C]$;

   б) $[[A, B], C] = [A, [B, C]] + [B, [C, A]]$.

10) Обозначим через $B_n(\Bbbk)$ множество верхнетреугольных матриц над полем $\Bbbk$ размера $n \times n$ с ненулевыми элементами на диагонали, то есть матриц вида

$$B = \begin{pmatrix} b_1^1 & b_2^1 & \dots & b_n^1 \\ 0 & b_2^2 & \dots & b_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & b_n^n \end{pmatrix},$$

где $b_i^i \in \Bbbk^*$ для всех $i = 1, \dots, n$. Обозначим через $U_n(\Bbbk)$ подмножество множества $B_n(\Bbbk)$, состоящее из верхнетреугольных матриц с единицами на диагонали. Доказать, что $B_n(\Bbbk)$ и $U_n(\Bbbk)$ — подгруппы в $GL_n(\Bbbk)$, причем подгруппа $U_n(\Bbbk)$ нормальна в $B_n(\Bbbk)$. Нормальна ли подгруппа $U_n(\Bbbk)$ в $GL_n(\Bbbk)$?

11) Пусть $W \subset M_n(\Bbbk)$ — множество матриц размера $n \times n$, у которых в каждом столбце и в каждой строке $n-1$ раз встречается ноль и один раз — единица. Доказать, что W — подгруппа группы $GL_n(\Bbbk)$, изоморфная симметрической группе S_n.

12) Вычислить значение многочлена $f(x) = a_0 + a_1 x + \dots + a_n x^n$ от матрицы X, где

   а) $X = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$;

   б) $X = \begin{pmatrix} a & 1 \\ 0 & b \end{pmatrix}$;

   в) $X = \begin{pmatrix} a & 1 & 0 \\ 0 & b & 1 \\ 0 & 0 & c \end{pmatrix}$.

Экзамен по алгебре за 1 семестр I курса. 12 декабря 1995 г.

1) Для какого максимального n существует сюръективный гомоморфизм группы диэдра D_6 в симметрическую группу S_n?

2) Является ли циклической группа обратимых элементов кольца

   а) $\mathbb{Z}_3[x]/(x^2)$?

   б) $\mathbb{Z}_4[x]/(x^2)$?

3) В линейном пространстве $V = \Bbbk^6$ со стандартным базисом $(e_1, \ldots, e_6)$ рассмотрим следующие векторы: $v_1 = e_1 - e_2$, $v_2 = e_2 - e_3$, $v_3 = e_3 - e_4$, $v_4 = e_4 - e_5$, $v_5 = e_5 - e_6$, и $v_6 = e_1 + e_2 + e_3 + e_4 + e_5 + e_6$.

   а) Образуют ли векторы $v_1, \ldots, v_6$ базис пространства V, если $\Bbbk = \mathbb{R}$ — поле вещественных чисел?

   б) Пусть $\operatorname{char} \Bbbk = p > 0$. При каких p векторы $v_1, \ldots, v_6$ образуют базис пространства V?

4) а) Описать все классы сопряженности в S_n, содержащие вместе с каждым элементом его квадрат.

   б) Обозначим через a_n число таких классов сопряженности. Написать производящую функцию для последовательности (a_n).

5) Для каких простых чисел p существует ненулевой гомоморфизм кольца целых гауссовых чисел $\mathbb{Z}[i]$ в кольцо вычетов $\mathbb{Z}_p$?

6) Пусть $\Lambda^\bullet = \Lambda^\bullet(\xi^1, \ldots, \xi^n)$ — алгебра Грассмана над полем $\mathbb{R}$, и пусть J — двусторонний идеал в алгебре $\Lambda^\bullet$. При каких J факторалгебра $\Lambda^\bullet/J$ является телом?