Теория чисел

Чуркин Валерий Авдеевич

21 января 2006 г.

Оглавление

Глава 1

Теория групп

1.1 Группы преобразований

ОПР 1.1.1 (Абстрактной группы)**.**

Абстрактной группой *называется непустое множество G с одной бинарной операцией (назовём её умножением и обозначим $\cdot$[1]) $(a, b) \to ab$ со свойствами:*

1. $\forall\, a, b, c \in G\colon (ab)c = a(bc)$ *— ассоциативность;*
2. $\exists\, e \in G \,|\, \forall\, a \in G\colon ae = ea = a$ *— существование единицы;*
3. $\forall\, a \in G\colon \exists\, a^{-1} \in G \,|\, aa^{-1} = a^{-1}a = e$ *— существование обратного.*

Коммутативность не предполагается. Например: как правило, не коммутативны группы преобразований.

ОПР 1.1.2 (Преобразований)**.**

Преобразованием *множества X называется взаимнооднозначное отображение X на себя. Таким будет* тождественное *(или* единичное*) преобразование $e\colon X \to X \,|\, e(x) = x - \forall\, x \in X$.*

Если f — преобразование X, то определено преобразование f^{-1} и если $f(x) = y$, то $f^{-1}(y) = x$. Ясно, что f^{-1} тоже преобразование X:

$$\forall\, x_1, x_2\colon \begin{array}{ccc} x_1 & \xrightarrow{f} & y_1 \\ \nparallel & & \nparallel \\ x_2 & \underset{f}{\longrightarrow} & y_2 \end{array} \quad \Rightarrow \quad \begin{array}{ccc} x_1 & \xleftarrow{f^{-1}} & y_1 \\ \nparallel & & \nparallel \\ x_2 & \underset{f^{-1}}{\longleftarrow} & y_2 \end{array}.$$

Кроме того, композиция преобразований X — снова преобразование $X \,|\, (fg)(x) \overset{def}{=} f(g(x))$:

$$\begin{array}{ccccc} x_1 & \xrightarrow{g} & y_1 & \xrightarrow{f} & z_1 \\ \nparallel & & \nparallel & & \nparallel \\ x_2 & \underset{g}{\longrightarrow} & y_2 & \underset{f}{\longrightarrow} & z_2 \end{array}.$$

ОПР 1.1.3 (Группы преобразований)**.**

Множество G преобразований множества X называется группой преобразований X*, если $\forall f, g \in G$:*

1. $e_x \in G$;
2. $f \in G \Rightarrow f^{-1} \in G$;
3. $f, g \in G \Rightarrow fg \in G$.

Теорема 1.1.4 (О преобразованиях)**.**

[1] А для сокращения будем писать вообще без ничего - прим. ред.

▷ Группа преобразований всегда является абстрактной группой в смысле определения группы[2].

▷ **Доказательство**.

- Пусть G — группа преобразований множества X, тогда на множестве G определена операция умножения $(f,\, g) \to fg$ (композиция).
- Проверим аксиомы групп:
  1. Ассоциативность:
     $\forall\, f, g, h \in G$: $(fg)h = f(gh)$, действительно:
     $$\forall x \in X - \begin{cases} ((fg)h)(x) = f(g(h(x))); \\ (f(gh))(x) = f(g(h(x))). \end{cases} .$$
  2. Существование единицы:
     Пусть $e = e_x \in G$ и $f \in G$, тогда $ef = fe = f$, т.к. $f(x) = e(f(x)) = (ef)(x) = (fe)(x) = f(e(x)) = f(x)$.
  3. Существование обратного:
     Если $f \in G$, то f^{-1} — обратное отображение $\Big|\, f^{-1} \in G,\ ff^{-1} = f^{-1}f = e_x$.

□

Пример 1.1.4.1 (Групп преобразований)**.**

▷ Пусть $S(X)$ — множество всех преобразований множества X, тогда $S(X)$ — группа преобразований, она называется *симметрической группой преобразований* множества X; если X — бесконечное множество, то $S(X)$ — *большая группа*; если X — конечно, то обычно полагают $X = \{1, 2, \dots n\}$ и $S(X) = S_n$ называют *группой всех подстановок n-элементного множества* (или *симметрической группой*).

▷ Пусть $X = V$, где V — векторное пространство[3] размерности n над полем K, тогда следующие множества будут группами преобразований:

- $GL(V) = \{$все невырожденные линейные операторы[4] пространства $V\}$;
- $SL(V) = \{$все линейные операторы пространства V с определителем $1\}$;

---

[2] Кому интересно: определение мультипликативной (абелевой) группы из первого семестра — абелева группа, где сложение заменено умножением: $(A; \cdot)$:

У1. $\forall a,\, b,\, c \in A$: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ — ассоциативность;

У2. $\forall a,\, b \in A$: $a \cdot b = b \cdot a$ — коммутативность;

У3. $\exists 1 \in A \Big|\, a \cdot 1 = 1 \cdot a = a$ — существование единицы;

У4. $\forall a \in A$: $\exists a^{-1} \in A \Big|\, a \cdot a^{-1} = a^{-1} \cdot a = 1$ — существование обратного элемента.

Алгебраические операции на множестве M — это отображение $M \times M \to M$, т.е. некоторое правило, сопоставляющее всякой паре $(a,\, b)$ из $M \times M$ элемент $c \in M$.

Алгебраическая структура (система) — это не пустое множество с заданным на нём семейством алгебраических операций.

[3] Определение из первого семестра: это алгебраическая структура $(V; +, (a \mapsto \lambda a,\ a \in K))$, удовлетворяющая следующим аксиомам:

1. $(V; +)$ — аддитивная абелева группа;
2. $\lambda \cdot (a + b) = \lambda \cdot a + \lambda \cdot b$;
3. $(\lambda + \mu) \cdot a = \lambda \cdot a + \mu \cdot a$;
4. $(\lambda \cdot \mu) \cdot a = \lambda \cdot (\mu \cdot a)$ — дистрибутивности;
5. $1 \cdot a = a$ — существование единицы.

Аддитивная (абелева) группа — это алгебраическая структура $(A; +)$, операция которой удовлетворяет следующим свойствам:

С1. $\forall a,\, b,\, c \in A$: $(a + b) + c = a + (b + c)$ — ассоциативность;

С2. $\forall a,\, b \in A$: $a + b = b + a$ — коммутативность;

С3. $\exists 0 \in A \Big|\, \forall a \in A$: $a + 0 = 0 + a = a$ — существование нуля (нулевого элемента);

С4. $\forall a \in A$: $\exists (-a) \in A \Big|\, a + (-a) = (-a) + a = 0$ — существование противоположного элемента.

[4] Это определение было в теореме из первого семестра: это такой линейный оператор A векторного пространства V над полем K, для которого следующие утверждения равносильны:

1. $\ker A = \{0\}$;
2. $\operatorname{Im} A = V$;
3. A — взаимнооднозначное отображение V на V;
4. A^{-1} — существует и линейно;
5. A-образ всякого базиса V — базис V;
6. A-образ некоторого базиса V — базис V;
7. Матрица $\mathtt{A}$ — невырожденная в некотором базисе;
8. Матрица $\mathtt{A}$ — невырожденная во всяком базисе.

Пусть W и V — векторные пространства над полем K, отображение $A\colon V \to W$ — называется *линейным*, если $A(x + y) = A(x) + B(y)$, $A(\alpha \cdot x) = \alpha \cdot (Ax) - \forall x,\, y \in V$, $\forall \alpha \in K$. При $W = V$: A — называется *линейный оператором* пространства V.

Вещественная (комплексная) матрица называется ортогональной (унитарной), если $\mathtt{A}^{-1} = \mathtt{A}^T$ $(\mathtt{A}^{-1} = \overline{\mathtt{A}^T})$.

- $O(V) = \{$все ортогональные операторы евклидова пространства $V\}$;
- $U(V) = \{$все унитарные операторы эрмитова пространства $V\}$;
- $GA(V) = \{$все афинные преобразования векторного пространства V$\}$ (т.е. отображения вида $f(x) = \mathtt{A}x + b$, где $\det \mathtt{A} \neq 0$);
- $Is(V) = \{$все изометрии евклидова пространства $V\}$ (т.е. отображения вида $f(x) = \mathtt{A}x + b$, $\mathtt{A}$ — ортогональный оператор).

Они изоморфны следующим группам матриц:

$$GL_n(K) = \{\mathtt{A} \in M_n(K)^{5} \big| \det \mathtt{A} \neq 0\};$$
$$SL_n(K) = \{\mathtt{A} \in M_n(K) \big| \det \mathtt{A} = 1\};$$
$$O_n(K) = \{\mathtt{A} \in M_n(K) \big| \mathtt{A}^T\mathtt{A} = \mathtt{E}\};$$
$$U_n(\mathbb{C}) = \{\mathtt{A} \in M_n(\mathbb{C}) \big| \mathtt{A}^{-1} = \overline{\mathtt{A}^T}\};$$
$$GA_n(\mathbb{C}) = \left\{ \begin{pmatrix} \mathtt{A} & b \\ 0 & 1 \end{pmatrix} \big| \det \mathtt{A} \neq 0,\ b \in K^n \right\};$$
$$Is_n(\mathbb{R}) = \left\{ \begin{pmatrix} \mathtt{A} & b \\ 0 & 1 \end{pmatrix} \big| \mathtt{A}^{-1} = \mathtt{A}^T,\ b \in \mathbb{R}^n \right\}.$$

▷ Упражнение — проверить соответствующие изоморфизмы.

1.2 Группы подстановок

ОПР 1.2.1 (Подстановки)**.**

- *Пусть* $X = \{1, 2, \ldots, n\}$, *все отображения* $\pi\colon X \to X$ *можно записать двумя строками:*

$$\pi = \begin{pmatrix} i_1 & i_2 & \ldots & i_n \\ j_1 & j_2 & \ldots & j_n \end{pmatrix},\ \textit{где } \pi(i_k) = j_k - \forall k.$$

Эта запись не однозначна, например:

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 2 \\ 3 & 2 & 1 \end{pmatrix} = \ldots.$$

- *Правило перемножения:*

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

то есть если переписать как $\pi_1 \cdot \pi_2 = \pi_3$, *то можно нарисовать:*

$$\begin{array}{ccccc} 1 & \xrightarrow{\pi_2} & 2 & \xrightarrow{\pi_1} & 1; \\ 2 & \xrightarrow{\pi_2} & 1 & \xrightarrow{\pi_1} & 3; \\ 3 & \xrightarrow{\pi_2} & 3 & \xrightarrow{\pi_1} & 2. \end{array}$$

— по правилам композиции отображений.

ОПР 1.2.2 (Множеств перемещаемых и неперемещаемых элементов)**.**
Обозначим для подстановки $\pi \in S_n$*:*

$$\begin{cases} F_\pi = \{i \in X \big| \pi(i) = i\}; \\ T_\pi = \{i \in X \big| \pi(i) \neq i\}. \end{cases}$$

— соответственно множества неподвижных *(или* неперемещаемых*)* и перемещаемых *элементов. Ясно, что:*

1. $F_\pi \cap T_\pi = \varnothing$;
2. $F_\pi \cup T_\pi = X$;
3. $\pi(F_\pi) = F_\pi$;

[5] Определение из теоремы первого семестра: $M_n(K)$ — множество всех квадратных матриц порядка n над полем K.

4. $\pi(T_\pi) = T_\pi$.

ОПР 1.2.3 (Независимых подстановок)**.**

Подстановки π *и* σ *называются* независимыми*, если они не имеют общих перемещаемых символов (элементов), т.е.* $T_\pi \cap T_\sigma = \varnothing$.

Лемма 1.2.4 (Перестановочность независимых подстановок)**.**

▷ Независимые подстановки перестановочны, т.е. если $T_\pi \cap T_\sigma = \varnothing \Rightarrow \pi\sigma = \sigma\pi$

▷ **Доказательство**.

∘ Используем равенство:

$$(\sigma\pi)(i) = \begin{cases} i, & \text{если } i \notin T_\pi \cup T_\sigma; \\ \pi(i), & \text{если } i \in T_\pi; \\ \sigma(i), & \text{если } i \in T_\sigma. \end{cases} \Rightarrow \sigma\pi = \pi\sigma.$$

□

ОПР 1.2.5 (Цикла)**.**

Подстановку σ *называют* циклом *длины* r*, если множество её перемещаемых символов* T_σ *можно занумеровать так, что* $T_\sigma = \{i_1, i_2, \ldots, i_r\}$*, где* $\sigma(i_1) = i_2,\ \sigma(i_2) = i_3,\ \ldots,\ \sigma(i_r) = i_1$*. Обозначается* $\sigma = (i_1, i_2, \ldots, i_r)$ *и всего имеем* r *различных записей для* σ*.*

Теорема 1.2.6 (О разложении на циклы)**.**

▷ Всякая подстановка разлагается в произведение попарно независимых циклов. Это разложение единственно с точностью до порядка цикла. Такое разложение называется *каноническим разложением.*

▷ **Доказательство**.

∘ Можно проверить индукцией по числу перемещаемых элементов: $\forall i_1 \in T_\pi\colon \exists r > 1\colon$

$$\begin{array}{ccccccccccc} i_1 & \xrightarrow{\pi} & i_2 & \xrightarrow{\pi} & i_3 & \xrightarrow{\pi} & \ldots & \xrightarrow{\pi} & i_r & \xrightarrow{\pi} & i_1 \\ & & \shortparallel & & \shortparallel & & \shortparallel & & \shortparallel & & \\ & & i_1 & & i_1, i_2 & & \ldots & & \ldots & & \end{array}$$

Пусть $\sigma_1 = (i_1, i_2, \ldots, i_r),\ \pi' = \sigma_1^{-1}\pi$, тогда $\pi'(i_k) = i_k - \forall k = 1, 2, \ldots, r$; т.е. π' имеет меньше перемещаемых элементов по сравнению с π. По предположению индукции $\pi = \sigma_1\pi' = \sigma_1(\sigma_2 \ldots \sigma_r)$ — попарно независимы.

□

ОПР 1.2.7 (Сопряженные подстановки)**.**

Подстановки π *и* π' *называются* сопряженными в S_n*, если* $\exists\sigma \,|\, \pi' = \sigma\pi\sigma^{-1}$.

Следствие 1.2.7.1 (Условие сопряженности)*.*

▷ Две подстановки сопряжены в $S_n \Leftrightarrow$ они *имеют одинаковое цикловое строение*, т.е. одинаковое количество независимых циклов каждой возможной длины.

▷ **Доказательство**.

($\Leftarrow$) Разложим π и π' на циклы:

$$\pi = (i_1 \ldots i_r)(j_1 \ldots j_s)(\ldots)\ldots; \tag{1}$$

$$\pi' = (i'_1 \ldots i'_r)(j'_1 \ldots j'_s)(\ldots)\ldots. \tag{2}$$

Пусть

$$\sigma = \begin{pmatrix} i_1 & i_2 & \ldots & i_r & j_1 & j_2 & \ldots & j_s & \ldots \\ i'_1 & i'_2 & \ldots & i'_r & j'_1 & j'_2 & \ldots & j'_s & \ldots \end{pmatrix}, \tag{3}$$

тогда σ — подстановка и кроме того $\pi' = \sigma\pi\sigma^{-1}$:

$$\begin{array}{ccc} i_1 & \xrightarrow{\pi} & i_2 \quad \ldots \\ \sigma^{-1}\uparrow & & \downarrow\sigma \\ i'_1 & \xrightarrow[\pi']{} & i'_2 \quad \ldots \end{array}.$$

(⇒) Пусть даны (1) и (3), тогда легко вывести, что $\sigma\pi\sigma^{-1} = \pi'$ из (2), т.е. π и π' имеют одинаковое цикловое строение.

□

Следствие 1.2.7.2. Классов попарно сопряженных подстановок имеется столько, сколько есть разбиений натурального числа n в сумму натуральных слагаемых по порядку убывания.

1.3 Разложение на транспозиции

ОПР 1.3.1 (Транспозиции)**.**

Транспозиция — *это цикл длины* 2, *обозначается* $\tau = (k,\, \ell)$.

ОПР 1.3.2 (Знака и чётности подстановки)**.**

Пусть π — *подстановка, тогда число* $\operatorname{sgn}\pi = \prod\limits_{i<j} \dfrac{\pi(j)-\pi(i)}{j-i}$ — *называется* знаком подстановки.

Если $\operatorname{sgn}\pi = 1$, *то подстановка называется* чётной, *ну, а в противном случае* — нечётной.

ОПР 1.3.3 (Декремента подстановки)**.**

Декремент подстановки π — *это разность между числом всех символов (элементов) на которые действует подстановка и числом независимых циклов, включая циклы длины 1.*

Пример 1.3.3.1 (Декремента)**.**

▷ Пусть $\pi = (1\,2\,3)(4\,5)(6)$, 6 символов, значит декремент, обозначим который за $d(\pi) = 6 - 3 = 3$.

Теорема 1.3.4 (О транспозициях)**.**

▷ Выполнено:

1. Всякая подстановка разлагается в произведение транспозиций, число которых равно декременту подстановки;
2. $\operatorname{sgn}(\sigma\pi) = \operatorname{sgn}\sigma \cdot \operatorname{sgn}\pi$;
3. Если $\pi = \tau_1\tau_2\ldots\tau_k$, где τ_i — транспозиции, то $\operatorname{sgn}\pi = (-1)^k$, в частности чётность подстановки совпадает с чётностью декремента.

▷ **Доказательство**.

1. Пусть $\pi = \sigma_1\sigma_2\ldots\sigma_s$, где σ_k — это цикл длины ℓ_k и циклы независимы; разложим циклы на произведение транспозиций по формуле: $(i_1 i_2\ldots i_{r-1} i_r) = (i_1 i_2)(i_2 i_3)\ldots(i_{r-1} i_r)$, тогда в разложении π будет транспозиций $\sum\limits_{i=1}^{s}(\ell_i - 1) = \left(\sum\limits_{i=1}^{s}\ell_i\right) - s$, короче говоря, утверждается, что это есть в точности $d(\pi)$[6] .
2. Рассмотрим $\operatorname{sgn}(\sigma\pi) = \prod\limits_{i<j}\dfrac{\sigma(\pi(j))-\sigma(\pi(i))}{j-i} = \prod\limits_{i<j}\dfrac{\sigma(\pi(j))-\sigma(\pi(i))}{\pi(j)-\pi(i)} \cdot \prod\limits_{i<j}\dfrac{\pi(j)-\pi(i)}{j-i} = \operatorname{sgn}\sigma\cdot\operatorname{sgn}\pi$, ну и всё, сразу получилось.
3. Так как $\pi = \tau_1\tau_2\ldots\tau_k$, то ввиду пункта 2.: $\operatorname{sgn}\pi = \operatorname{sgn}\tau_1 \cdot \operatorname{sgn}\tau_2 \cdot \ldots \cdot \operatorname{sgn}\tau_k$, поэтому достаточно доказать, что знак транспозиции равен (-1). Пусть $\tau = (k,\, \ell)$ — транспозиция, можем считать, что

$$\boxed{1 \leqslant k < \ell < n},$$

тогда

$$\operatorname{sgn}\tau = \prod_{i<j}\frac{\tau(j)-\tau(i)}{j-i} = \frac{\tau(\ell)-\tau(k)}{\ell-k} \cdot {}_{\text{(случай } j=k\text{)}}\prod_{i<k}\frac{\tau(k)-\tau(i)}{k-i}\cdot$$

$$\cdot{}_{\text{(случай } j=\ell\text{)}}\prod_{\substack{i<\ell\\ i\neq k}}\frac{\tau(\ell)-\tau(i)}{\ell-i} \cdot {}_{\text{(случай } i=k\text{)}}\prod_{\substack{k<j\\ j\neq\ell}}\frac{\tau(j)-\tau(k)}{j-k} \cdot {}_{\text{(случай } i=\ell\text{)}}\prod_{\ell<j}\frac{\tau(j)-\tau(\ell)}{j-\ell} =$$

$$= \frac{k-\ell}{\ell-k}\cdot\prod_{i<k}\frac{\ell-i}{k-i}\cdot\prod_{\substack{i<\ell\\ i\neq k}}\frac{k-i}{\ell-i}\cdot\prod_{\substack{k<j\\ j\neq\ell}}\frac{j-\ell}{j-k}\cdot\prod_{\ell<j}\frac{j-k}{j-\ell} = -1.$$

□

[6] Потому, что $\sum\limits_{i=1}^{s}\ell_i$ — это общее количество элементов, а s — количество циклов ⇒ их разность — определение декремента подстановки 1.3.3 — прим. ред.

1.4 Подгруппы

ОПР 1.4.1 (Напоминание определения группы)**.**
Пусть G — группа; A, $B \subset G$ — подмножества; тогда обозначим $AB = \{ab \,|\, a \in A,\, b \in B\}$; $A^{-1} = \{a^{-1} \,|\, a \in A\}$.

ОПР 1.4.2 (Подгруппы)**.**
Подмножество H группы G является её подгруппой[7] *(было в 1-ом семестре), если $e \in H$, $HH \subseteq H$, $H^{-1} \subseteq H$ (обозначается $H \preccurlyeq G$ — означает, что H — подгруппа).*

Пример 1.4.2.1 (Подгруппы)**.**

▷ Множество всех чётных подстановок из S_n образует подгруппу (которая обозначается A_n). Это сразу получается из теоремы о транспозициях 1.3.4 на стр. 9.

Теорема 1.4.3 (Свойства подгрупп)**.**

▷ Выполнено:

1. Пересечение семейства подгрупп — всегда подгруппа (в данной группе, конечно, а вот если объединить, то уже может и не быть);
2. Если H — подгруппа группы G, то множество aHa^{-1} — тоже подгруппа группы G (называется сопряжённой с H);
3. Если A — подмножество группы G и $A \neq \varnothing$, то множество $< A >= \{a_1^{\varepsilon_1} a_2^{\varepsilon_2} \dots a_n^{\varepsilon_n} \,|\, a_i \in A,\, \varepsilon_i = \pm 1,\, n \geqslant 1\}$ — образует наименьшую подгруппу группы G, содержащую A.

▷ **Доказательство**.

1. Ну просто: пусть $H_i \preccurlyeq G,\ i \in I$, то есть задано семейство подгрупп; а $H = \bigcap\limits_{i \in I} H_i$. Проверим, что H — подгруппа G: нужно проверить 3 свойства. Во-первых, заметим, что единица $e \in H_i - \forall i_{\text{(определение подгруппы)}} \Rightarrow$ $\Rightarrow e \in \bigcap\limits_{i \in I} H_i = H$; пусть $a,\, b \in H \Rightarrow a,\, b \in H_i - \forall i \Rightarrow ab,\, a^{-1} \in H_i - \forall i \ \Rightarrow ab,\, a^{-1} \in \bigcap\limits_{i \in I} H_i = H$.
2. $e = aea^{-1} \in aHa^{-1}$, значит единица там лежит. Если взять два элемента — axa^{-1} и aya^{-1} и перемножить, то получим: $axa^{-1} \cdot aya^{-1} = a(xy)a^{-1} \in aHa^{-1}$, если $x \in H$. Для обратного элемента: $(axa^{-1})^{-1} = ax^{-1}a^{-1} \in aHa^{-1}$, если $x,\, y \in H$.
3. Во-первых заметим, что множество $< A >$ — подгруппа группы G: опять нужно проверить 3 свойства. $e = aa^{-1} \in < A >$; если $a_1,\, a_2,\, \dots,\, a_n,\, b_1,\, \dots,\, b_m \in A_i,\ \varepsilon_i = \pm 1,\ \sigma_j = \pm 1$, то $a_1^{\varepsilon_1} \cdot a_2^{\varepsilon_2} \cdot \ldots \cdot a_n^{\varepsilon_n} \cdot b_1^{\sigma_1} \cdot \ldots \cdot$ $\cdot\, b_m^{\sigma_m} \in < A >$; кроме того давайте обратим: $(a_1^{\varepsilon_1} \cdot a_2^{\varepsilon_2} \cdot \ldots \cdot a_n^{\varepsilon_n})^{-1} = a_n^{-\varepsilon_n} \cdot \ldots \cdot a_2^{-\varepsilon_2} \cdot a_1^{-\varepsilon_1}$ и конечно лежит в $< A >$. Ясно, что $< A > \supseteq A$, с другой стороны, если $H \preccurlyeq G$ и $H \supset A$, то $H \supseteq < A >$.

□

ОПР 1.4.4 (Подгруппы, порождённой множеством)**.**
Подгруппа $< A >$ называется подгруппой группы G, порождённой множеством *A. Если $< A >= G$, то A — называется* множеством, порождающим группу G.

Пример 1.4.4.1 (Группы, порождённой множеством)**.**

▷ Утверждается, что группа S_n — порождается множеством своих транспозиций. Действительно, мы же доказали, что всякая подстановка является произведением транспозиций.

[7] А вот интересно в «А.Г. Курош „Курс высшей алгебры“ издание девятое, 1968 г.»:
Подмножество A группы G называется *подгруппой* этой группы, если оно само является группой относительно операции, определённой в группе G.
При проверке того, является ли подмножество A группы G подгруппой этой группы, достаточно проверить: 1) содержится ли в A произведению любых двух элементов из A; 2) содержит ли A вместе со всяким своим элементом и его обратный элемент. Действительно, из справедливости закона ассоциативности в группе G следует его справедливость для элементов из A, а принадлежность к A единицы группы G вытекает из 2) и 1) (как произведение элемента и его обратного — прим. ред.).

1.5 Разложение на смежные классы

ОПР 1.5.1 (Левого и правого смежного класса)**.**

Пусть H — подгруппа группы G, тогда множества $aH = \{ah \mid h \in H\}$ и $Ha = \{ha \mid h \in H\}$ — называются, соответственно, левым *и* правым смежными классами подгруппы H в группе G с представителем $a \in G$.

Теперь ещё одна простая, но важная теорема:

Теорема 1.5.2 (Свойства смежных классов)**.**

▷ Выполнено:

1. Левые (правые) смежные классы подгруппы разбивают группу (другими словами разные классы не пересекаются, объединение даёт группу);
2. Любые два смежных класса — равномощны;
3. Число левых классов подгруппы H совпадает с числом правых классов подгруппы H в группе G. Оно называется *индексом подгруппы* и обозначается $|G : H|$.

▷ **Доказательство**.

1. Введём на группе G отношение левой смежности относительно подгруппы H следующим способом: $a \sim b \Leftrightarrow a^{-1}b \in H$. Это — эквивалентность, надо проверить свойства:
   - ✓ $a \sim a$, так как $e = a^{-1}a \in H$;
   - ✓ Если $a \sim b \Rightarrow b \sim a$, так как $b^{-1}a = (a^{-1}b)^{-1} \in H$, а H — замкнута относительно обращения;
   - ✓ $a \sim b,\ b \sim c \Rightarrow a \sim c$, так как $a^{-1}c = (a^{-1}b)(b^{-1}c) \in H$.

   Давайте выясним, как выглядит класс эквивалентности с представителем $a \in G \mid a \sim x \Leftrightarrow a^{-1}x = h \in H \Leftrightarrow x = ah,\ h \in H$, т.е. это левый смежный класс подгруппы H представителем a. Следовательно так как классы эквивалентности разбивают множество, то можем утверждать, что левые смежные классы разбивают группу. Доказательство для правой смежной группы — аналогично: $a \sim b \Leftrightarrow ab^{-1} \in H$ (можете проверить сами или прочтите).
2. Соответствие $h \leftrightarrow ah$, где $h \in H$ — взаимнооднозначное, действительно: если предположить, что $ah_1 = ah_2$, то умножив на a^{-1}, получим $h_1 = h_2 \Rightarrow |H| = |aH|$. Аналогично и для другого класса: $|H| = |Ha|$.
3. Напишем: так как соответствие $x \leftrightarrow x^{-1}$ взаимнооднозначное, то соответствие $aH \leftrightarrow (aH)^{-1} = H^{-1}a^{-1} = Ha^{-1}$ (т.к. $H^{-1} \subseteq H$ по определению и $(y^{-1})^{-1} = y - \forall y \in H$, поэтому если потребовать включения, то $H^{-1} = H$). Значит это соответствие взаимнооднозначное, получаем, что число левых классов равно числу правых. Всё, теорема доказана.

□

Так, следствие сразу из неё:

Следствие 1.5.2.1 (Теорема Лагранжа).

▷ Пусть

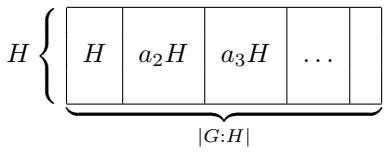
H — подгруппа конечной группы G.

▷ Тогда

Порядок группы[8] $|G| = |H| \cdot |G : H|$, в частности порядок подгруппы делит нацело порядок группы.

▷ **Доказательство**.

◦ Состоит в том, что вы смотрите на картинку.



□

[8]Не нашёл такого понятия в лекциях, на всякий случай уточнил в «А.Г. Курош „Курс высшей алгебры“ издание девятое, 1968 г.»: Если группа G состоит из конечного числа элементов, то она называется *конечной группой*, а число элементов в ней — *порядком* группы.

1.6 Порядок элемента, циклические группы

ОПР 1.6.1 (Порядка элемента)**.**

Порядком элемента группы называется число (символ):

$$\operatorname{ord} g = \begin{cases} n, & \text{если } g^n = e,\ g^r \neq e \text{ при } 0 < r < n; \\ \infty, & \text{если } g^n \neq e - \forall n. \end{cases}$$

Лемма 1.6.2 (Свойства порядка)**.**

▷ Пусть
$\operatorname{ord} g = n < \infty$.

▷ Тогда

1. $g^k = e \Leftrightarrow n|k$;
2. $g^k = g^\ell \Leftrightarrow k \equiv \ell (\mathrm{mod}^9\ n)$;
3. Порядок элемента $\operatorname{ord} g^k = \dfrac{n}{\text{НОД}(n,\ k)}$.

▷ **Доказательство**.

1. Пусть $k = nq + r,\ o \leqslant r < n$, тогда $g^k =_{\text{(по правилам произведения)}} (g^n)^q \cdot g^r = e \cdot g^r = g^r = e \Leftrightarrow r = 0 \Leftrightarrow n|k$.
2. Очевидно: $g^k = g^\ell \Leftrightarrow g^{k-\ell} = e \Leftrightarrow_{\text{(ввиду 1.)}} n|(k - \ell) \Leftrightarrow k \equiv \ell (\mathrm{mod}\ n)$.
3. Пусть $d = \text{НОД}(n,\ k)$, тогда $n = d \cdot n',\ k = d \cdot k',\ \text{НОД}(n',\ k') = 1$. Теперь возьмём g^k, возведём в степень ℓ: $(g^k)^\ell = e \Leftrightarrow_{\text{(ввиду 1.)}} n|(k\ell) \Leftrightarrow (d \cdot n')|(dk' \cdot \ell)$, ясно, что d можно убрать $\Leftrightarrow n'|(k'\ell)$, но n' и k' — взаимнопросты $\Leftrightarrow n'|\ell$. Из этого мы видем, что $\operatorname{ord}(g^k) = n' = \dfrac{n}{d} = \dfrac{n}{\text{НОД}(n,\ k)}$, вот и всё, это доказано.

□

ОПР 1.6.3 (Циклической подгруппы)**.**

Пусть G — группа, $g \in G$, тогда подгруппа $< g >$ (состоящая из степеней элемента g) называется циклической подгруппой[10]*, порождаемой элементом g. Но ещё можно сказать: если сама группа совпадает с множеством степеней одного и того же элемента, то группа G называется циклической ($G =< g >$).*

Теорема 1.6.4 (Изоморфность циклических групп одного порядка)**.**

▷ Всякая циклическая группа изоморфна[11] аддитивным группам колец $\mathbb{Z}$ или $\mathbb{Z}_n$[12].

▷ **Доказательство**.

◦ Очевидно: пусть $G =< g >$, если $g^k \neq e - \forall k \neq 0$, то соответствие $k \leftrightarrow g^k$ является изоморфизмом между нашей группой и $\mathbb{Z}$. Если $\operatorname{ord} g = n < \infty$, то соответствие $k \leftrightarrow g^k$, при $0 \leqslant k < n$ — является изоморфизмом между G и $\mathbb{Z}_n$ (ну это почти очевидно $1 \leftrightarrow e$, $2 \leftrightarrow g^2$, ...).

□

Следствие 1.6.5 (Теоремы Лагранжа).

[9] $a \equiv b (\mathrm{mod}\ n) \Leftrightarrow n|(a - b)$ — взято из первого семестра.

[10] Обозначим через $\{a\}$ подмножество группы G, составленное из всех степеней элемента a; в него входит и сам элемент a, являющийся своей первой степенью. ... Подгруппа $\{a\}$ называется *циклической подгруппой группы G, порождённой элементом a*. Как показывает равенство $a^m \cdot a^n = a^n \cdot a^m = a^{m+n}$, она всегда коммутативна, даже если сама группа G и некоммутативна.

... Группа G называется *циклической* группой, если она состоит из степеней одного из своих элементов a, т.е. совпадает с одной из своих циклических подгрупп $\{a\}$; элемент a называется в этом случае *образующим элементом* группы G. Всякая циклическая группа, очевидно, абелева. — А.Г. Курош „Курс высшей алгебры“ издание девятое, 1968 г.

[11] Приведу для интересующихся теорему из А.Г. Курош „Курс высшей алгебры“ издание девятое, 1968 г.: Все бесконечные циклические группы изоморфны между собой; изоморфны между собой также все конечные циклические группы данного порядка n.

За одно определение изоморфизма оттуда же: Группы G и G' называются *изоморфными*, если между ними можно установить такое взаимнооднозначное соответствие, при котором для любых элементов a и b из G и соответствующих им элементов a', b' из G' произведению ab соответствует произведение $a'b'$. ... можно показать, что при изоморфном соответствии между группами G и G' единице группы G соответствует единица группы G', и если элементу a из G соответствует элемент a' из G', то элементу a^{-1} соответствует элемент a'^{-1}.

[12] $\mathbb{Z}_n = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$, где $[a]_n = \{b \in \mathbb{Z} \mid b \equiv a (\mathrm{mod}\ n)\}$ — взято из первого семестра.

▷ Пусть

G — группа порядка $n < \infty$ (группа конечного порядка).

▷ Тогда

$\forall g \in G\colon g^n = e$.

▷ **Доказательство**.

∘ Пусть $H =< g > \preccurlyeq G$, тогда $|H| = \operatorname{ord} g = k$. По теореме Лагранжа 1.5.2.1 на стр. 11: $|G| = |H| \cdot |G : H| \Rightarrow$ $\Rightarrow k \big| n \Rightarrow n = k\ell, \ell \in \mathbb{N}$. Отсюда $g^n = g^{k\ell} = (g^k)^\ell = e^\ell = e$.

□

Следствие 1.6.6 (Цикличность группы простого порядка).

▷ Группа простого порядка является циклической, то есть если $|G| = p$— простое $\Rightarrow G =< g >$.

▷ **Доказательство**.

∘ Пусть $\exists g \in G$, $g \neq e$; $H =< g >$, тогда:

1. $|H| > 1$;
2. Из теоремы Лагранжа: $|H| \mid |G| = p \Rightarrow$ так как p — простое, то $|H| = p$.

$H \subseteq G \Rightarrow H = G$ таким образом $G =< g >$.

Более сложно, конечно, устроены группы составного порядка.

□

Следствие 1.6.7 (Малая теорема Ферма).

▷ Пусть

p — простое число, a — целое число и кроме того предположим, что a и p взаимопросты: $(a, p) = 1$.

▷ Тогда

Утверждается, что $a^{p-1} \equiv 1 (\mathrm{mod}\ p)$.

▷ **Доказательство**.

∘ Пусть $\mathbb{Z}_p$ — кольцо вычетов по модулю p, так как p — простое, то $\mathbb{Z}_p$ — поле; тогда $\mathbb{Z}_p^*$ — мультипликативная группа обратимых элементов из $\mathbb{Z}_p$, имеет порядок $p - 1$. Ясно, что класс $\tilde{a}$ элемента a отличен от нуля, $\tilde{a} \in \mathbb{Z}_p^*$, а по следствию 1.6.5 на стр. 12: $\tilde{a}^{p-1} = \tilde{1}$, другими словами $a^{p-1} \equiv 1 (\mathrm{mod}\ p)$.

□

Следствие 1.6.7.1 (Формула Эйлера).

▷ Пусть

a и n — целые числа, предположим $n > a$, $(a, n) = 1$.

▷ Тогда

$a^{\varphi(n)} \equiv 1 (\mathrm{mod}\ n)$, где $\varphi(n)$ = количество натуральных чисел, меньших n и взаимно простых с n. Функция $\varphi(n)$ называется *φ-функцией Эйлера* (у Эйлера есть и другие функции), смотрите определение 2.7.4.

▷ **Доказательство**.

∘ Пусть $\mathbb{Z}_n$ — кольцо вычетов по модулю n, тогда $|\mathbb{Z}_n^*| = \varphi(n)$ и утверждение следует из следствия 1.6.5 на стр. 12; действительно, уравнение $ax \equiv 1 (\mathrm{mod}\ n)$ — разрешимо $\Leftrightarrow n \big| (ax - 1) \Leftrightarrow ax - 1 = ny$ для $y \in \mathbb{Z} \Leftrightarrow$ $ax - ny = 1$, то есть когда это уравнение разрешимо в $\mathbb{Z}$, а мы такие уравнения рассматривали — линейное диофантово уравнение, тогда мы можем сказать, что НОД$(a,\ n) \big| 1$, а это означает, что a и n — взаимно простые (то есть такой x существует $\Leftrightarrow (a,\ n) = 1$, то есть количество обратных элементов x равно $\varphi(n)$).

□

1.7 Действие группы на множестве

ОПР 1.7.1 (Действия группы на множестве)**.**
Группа G действует на множестве X, *если задано отображение $G \times X \to X$, где паре (g, x) сопоставляется $gx \in X$ такое, что $\forall f, g \in G, \forall x \in X$:*

1. $(fg)x = f(gx)$;
2. $ex = x$.

Обозначения: $G : X$ — означает, что G действует на X.

Пример 1.7.1.1 (Действия группы на множестве)**.**

1. G — группа преобразований множества X;
2. Левое регулярное действие группы G на себе: здесь $X = G$, а $(g, x) \to g \cdot x$;
3. Правое регулярное действие G на себе: $X = G$, а $(g, x) \to x \cdot g^{-1}$. Давайте проверим, что аксиомы в этом случае выполняются: обозначим $(fg) \circ x = x \cdot (fg)^{-1} = x \cdot g^{-1}f^{-1} =_{\text{(можно понять)}} f \circ (x \cdot g^{-1}) = f \circ (g \circ x)$, так вот это тождество получилось, это аксиома 1, только операция заменена на кружочек.
4. Сопряженное действие G на себе: $X = G$, $(g, x) \to g \cdot x \cdot g^{-1}$; легко проверить все аксиомы.
5. Левое регулярное действие G на множестве X левых смежных классов подгруппы H группы G определим так: $X = G/H \Rightarrow (g, xH) \to g \cdot xH$, легко проверить.

ОПР 1.7.2 (Орбиты и стабилизатора элемента)**.**
Пусть группа G действует на множестве X, тогда:

- *множество* $\mathrm{Orb}(x) = \{gx \,|\, g \in G\}$ — *называется* G-орбитой элемента $x \in X$;
- *множество* $\mathrm{Stab}(x) = \{g \in G \,|\, gx = x\}$ — *называется* стабилизатором элемента $x \in X$.

Теорема 1.7.3 (О мощности орбиты)**.**

▷ Пусть
Группа G действует на множестве X.

▷ Тогда

1. G-орбиты разбивают множество X;
2. Стабилизаторы двух элементов одной орбиты сопряжены в G и имеют одинаковый порядок;
3. Мощность орбиты равна индексу стабилизатора точки орбиты: $|\mathrm{Orb}(x)| = |G : \mathrm{Stab}(x)|$.

▷ **Доказательство**.

1. Введём на X отношение $\sim$ по правилу: $x \sim y \Leftrightarrow \exists g \in G$: $gx = y$. Это отношение эквивалентности, проверим симметричность, рефлексивность и транзитивность:
   - ✓ $x \sim x$, т.к. $ex = x$;
   - ✓ $x \sim y \Rightarrow y \sim x$, т.к. если $gx = y$, то $x = g^{-1}y$;
   - ✓ $x \sim y$, $y \sim z \Rightarrow x \sim z$, т.к. если $gx = y$, $fy = z$, то $(fg)x = f(gx) = fy = z$.

   Надо проверить, что это классы эквивалентности, это — орбиты $\Rightarrow$ орбиты разбивают X.

   ◦ Отметим, что $\mathrm{Stab}(x)$— всегда подгруппа G. Далее, пусть $gx = y$ (то есть две точки лежат в одной орбите), обозначим $H = \mathrm{Stab}(x), K = \mathrm{Stab}(y)$ и проверим, что $gHg^{-1} \subseteq K$ (на самом деле тут будет равенство). Действительно: $(ghg^{-1})y = gh(g^{-1}y) = ghx = gx = y$. Теперь как доказать, что там не только включение, но и равенство: так как $x = g^{-1}y$, то аналогично $g^{-1}K(g^{-1})^{-1} \subseteq H$. Значит, $g^{-1}Kg \subseteq H \Rightarrow K \subseteq gHg^{-1} \Rightarrow K = gHg^{-1}$, значит стабилизаторы сопряжены и в частности $|K| = |H|$.

   ◦ Пусть $x \in X$ и g, $g' \in G$, тогда $gx = g'x$ (проблема в том, что запись не однозначна, gx может совпадать с $g'x$) $\Leftrightarrow x = g^{-1}g'x \Leftrightarrow g^{-1}g' \in \mathrm{Stab}(x) = H \Leftrightarrow g^{-1}g'H = H \Leftrightarrow gH = g'H$ (у нас было введено отношение левой подгруппы, разбивающей на смежные классы). Поэтому различных элементов вида gx для $g \in G$ столько, сколько различных классов вида gH для $g \in G$. Число классов мы называем индексом подгруппы, итак, $|\mathrm{Orb}(x)| = |G : H| = |G : \mathrm{Stab}(x)|$.

□

Следствие 1.7.3.1 (Связь порядка группы, орбиты и стабилизатора).

▷ Пусть

Конечная группа G действует на множестве X.

▷ Тогда

Утверждается, что $\forall x \in X\colon |G| = |\operatorname{Orb}(x)| \cdot |G|$, в частности $|\operatorname{Orb}(x)|$ делит $|\operatorname{Stab}(x)|$.

▷ **Доказательство**.

∘ Пусть $H = \operatorname{Stab}(x)$, тогда по теореме Лагранжа 1.5.2.1 на стр. 11: $|G| = |H| \cdot |G : H| = |\operatorname{Stab}(x)| \cdot |\operatorname{Orb}(x)|$ (из третьего пункта предыдущей теоремы).

□

Пример 1.7.3.2 (Вращения тетраэдра).

▷ Пусть

G — группа вращений правильного тетраэдра (значит такие ортогональные преобразования, которые совмещают тетраэдр сам с собой).

▷ Тогда

Утверждается, что $|G| =_{(x\,-\,\text{вершина})} |\operatorname{Orb}(x)| \cdot |\operatorname{Stab}(x)| = 4 \cdot 3 = 12$ (4 вершины всего, а 3 из них — те вращения, которые x оставляют на месте (т.к. центр всегда на месте)). Более того, $G \backsimeq A_4$ (изоморфна множеству подстановок четырёх её вершин).

▷ **Доказательство**.

∘ Действительно, G содержит:

✓ 1 единичный элемент (понятно, всё останется на месте);

✓ $4 \cdot 2 = 8$ тройных циклов (поворот на 120°, по 2 поворота в 4-х осях);

✓ 3 произведения двух независимых транспозиции (через середины противоположных рёбер проведём прямые и можно повернуть на угол π, таких имеется 3, так как всего рёбер 6, а с противоположными — 3 пары).

То есть $1 + 8 + 3 = 12 = |A_4| = \frac{4!}{2}$.

□

1.8 Теоремы Бернсайда и Пойа о перечислении орбит

ОПР 1.8.1 (Множества неподвижных точек).
Пусть $G : X$, X/G — множество всех G-орбит, нас интересует сколько их, мощность одной мы уже умеем считать. Обозначим: $\operatorname{Fix}(g) = \left\{x \in X \middle| gx = x\right\}$ — множество неподвижных точек *элемента $g \in G$.*

Теорема 1.8.2 (Бернсайда).

▷ Пусть

Конечная группа G действует на конечном множестве X.

▷ Тогда

Число G-орбит $|X/G| = \dfrac{1}{|G|} \cdot \sum\limits_{g \in G} |\operatorname{Fix}(g)|$.

▷ **Доказательство**.

∘ Пусть $X_1, X_2, \ldots, X_n = X$ — все G-орбиты из X и F — множество пар $\{(g,x)\big| gx = x,\ g \in G,\ x \in X\}$; тогда считаем:

$$|F| =_{\text{(считаем по первому элементу)}} \sum_{g\in G} |\operatorname{Fix}(g)| = \sum_{x\in X} |\operatorname{Stab}(x)| = \sum_{i=1}^{n}\left(\sum_{x\in X_i} |\operatorname{Stab}(x)|\right) =$$

$$=_{\text{(Следствие 1.7.3.1 на стр. 15)}} \sum_{i=1}^{n}\left(\sum_{x\in X_i} \frac{|G|}{|X_i|}\right) = \sum_{i=1}^{n} |X_i| \cdot \frac{|G|}{|X_i|} = n \cdot |G|.$$

Следовательно

$$|X/G| =_{(X_1,\ \ldots,\ X_n\ -\ \text{орбиты})} n = \frac{1}{|G|} \cdot \sum_{g\in G} |\operatorname{Fix}(g)|.$$

□

ОПР 1.8.3 (Циклового индекса)**.**

Пусть $G \preccurlyeq S_n$, обозначим через j_k количество независимых циклов длины k в разложении $g \in G$; последовательность $(j_1, j_2, \ldots, j_n)$ называется цикловым индексом *элемента $g \in G$.*

Многочлен $f_G(x_1, x_2, \ldots, x_n) = \dfrac{1}{|G|} \cdot \sum\limits_{g\in G} x_1^{j_1} \cdot x_2^{j_2} \cdot \ldots \cdot x_n^{j_n}$ — называется цикловым многочленом *подгруппы G.*

Пример 1.8.3.1 (Подсчёта циклового многочлена)**.**

▷ Пусть $G = S_3$, какой у нее цикловой многочлен?

g	(j_1, j_2, j_3)
$e = (1)(2)(3)$	(3, 0, 0)
(1, 2, 3)	(0, 0, 1)
(1, 3, 2)	(0, 0, 1)
(1, 2)(3)	(1, 1, 0)
(1, 3)(2)	(1, 1, 0)
(2, 3)(1)	(1, 1, 0)

,

тогда $f_{S_3}(x_1, x_2, x_3) = \frac{1}{6} \cdot (x_1^3 + 2 \cdot x_3 + 3 \cdot x_1 x_2)$.

ОПР 1.8.4 (Подобия относительно группы функций)**.**

Пусть группа G действует на множестве X, две функции $\alpha, \beta\colon X \to Y$ называются подобными *относительно группы G ($\alpha(x) \overset{G}{\sim} \beta(x)$), если $\exists g \in G\big|\, \beta(x) = (g \circ \alpha)(x) := \alpha(g^{-1}x) - \forall x \in X$.*

Теорема 1.8.5 (Пойа)**.**

▷ Пусть

$|X| = n$, $|Y| = r$, G действует на множестве X, то есть $G \preccurlyeq S_n$.

▷ Тогда

Число классов подобных функций относительно G равно $f_G(r, r, \ldots, r) = \frac{1}{|G|} \cdot \sum\limits_{g\in G} r^{j_1+j_2+\ldots+j_n}$.

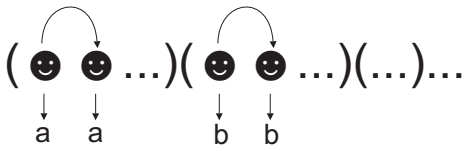
▷ **Доказательство**.

∘ Введём цикловой индекс группы $f_G(x_1, x_2, \ldots, x_n) = \frac{1}{|G|} \cdot \sum_{g\in G} x_1^{j_1} \cdot x_2^{j_2} \cdot \ldots \cdot x_n^{j_n}$, понятно, что для двух элементов с одинаковыми цикловыми индексами число x-ов „накопится“. Рассмотрим множество функций $F = \{f\big|\, f\colon X \to Y\}$, тогда G действует на F по правилу: $(g \circ f)(x) := f(g^{-1}(x))$ — так определяется, то есть аргумент сдвигаем действием подстановки, а потом функцией — это действие на множестве функций.

∘ По сути дела класс подобия — это G-орбита, утверждается, что число классов подобных функций равно $f_G(r, r, \ldots, r) = \frac{1}{|G|} \cdot \sum_{g\in G} r^{j_1+j_2+\ldots+j_n}$, где $(j_1, j_2, \ldots, j_n)$ — цикловой индекс g. Получается это применением формулы Бернсайда, вот и всё:

$$|G/X| = \frac{1}{|G|} \cdot \sum_{g\in G} |\operatorname{Fix} g|,$$

возьмём функцию f, пусть она неподвижна, тогда это означает, что действия не происходит, но $g = (\ldots)(\ldots)(\ldots)\ldots$ — циклы, а g^{-1} — тоже, только циклы надо перевернуть, это означает:



Видно, что на каждом элементе цикла функция принимает одно и то же значение, то есть на каждый цикл возможно по r значений функции f, а так как $\sum_i j_i$ — количество всех циклов, то $|\operatorname{Fix} g| = r^{j_1} \cdot r^{j_2} \cdot \ldots \cdot r^{j_n}$.

□

Пример 1.8.5.1 (Подсчёта количества подобных функций)**.**

▷ Подсчитаем число раскрасок граней тетраэдра в 3 цвета, различных при любых поворотах. Граней — четыре, цветов — три. Раскраска — функция из множества граней в множество цветов. Группа вращений тетраэдра действует на множестве граней, а потому и на множестве функций-раскрасок:

Тип элемента $g \in G$	Количество	$\lvert\operatorname{Fix}(g)\rvert$
$(1)(2)(3)(4)$	1	3^4
$(1,\,2,\,3)(4)$	8	3^2
$(1,\,2)(3,\,4)$	3	3^2

Получается число существенно различных раскрасок — $\frac{1}{12} \cdot (3^4 + 8 \cdot 3^2 + 3 \cdot 3^2) = 15$.

1.9 Гомоморфизмы, нормальные подгруппы и фактор группы

ОПР 1.9.1 (Гомоморфизма)**.**
Отображение $\varphi\colon G \to G'$ двух групп называется гомоморфизмом*, если $\varphi(ab) = \varphi(a) \cdot \varphi(b) - \forall a,\, b \in G$.*[13]

Пример 1.9.1.1 (Гомоморфизма)**.**

▷ Пусть $G = S_n$, $G' = \{\pm 1\}$, тогда $\varphi\colon \pi \to \operatorname{sgn}\pi$ — гомоморфизм;

▷ Пусть $G = M_n(K)$, $G' = K \setminus \{0\}$, тогда $\varphi\colon \mathtt{A} \to \det \mathtt{A}$ — гомоморфизм.

ОПР 1.9.2 (Образа и ядра гомоморфизма)**.**
Множества $\operatorname{Im}\varphi = \{\varphi(a) \big| \, a \in G\}$ *и* $\ker\varphi = \{a \in G \big| \, \varphi(a) = e'\}$ *— называются соответственно* образом *и* ядром *гомоморфизма $\varphi\colon G \to G'$.*

ПРЕДЛ 1.9.3 (Ядро и образ — подгруппы)**.**

▷ $\operatorname{Im}\varphi$ и $\ker\varphi$ — подгруппы группы G.

▷ **Доказательство**.

- Проверим для образа:
  - ✓ Пусть e — единица группы G, а e' — группы G'; тогда $\varphi(e) = \varphi(e) \cdot \varphi(e)$, но уравнение $x = x \cdot x$ имеет в группе G' единственное решение $x = e'$. Следовательно $\varphi(e) = e' \in \operatorname{Im}\varphi$, осталось проверить замкнутость относительно обращения и умножения.
  - ✓ Если $\varphi(a) \in \operatorname{Im}\varphi$, то можно писать: $e' = \varphi(e) = \varphi(aa^{-1}) = \varphi(a) \cdot \varphi(a^{-1})$, то есть $[\varphi(a)]^{-1} = \varphi(a^{-1}) \in \operatorname{Im}\varphi$.
  - ✓ Далее $\varphi(a) \cdot \varphi(b) = \varphi(ab) \in \operatorname{Im}\varphi$

  $\Rightarrow \operatorname{Im}\varphi$ — подгруппа группы G'.
- Проверим для ядра:
  - ✓ Пусть a и $b \in \ker\varphi$, тогда $\varphi(ab) = \varphi(a) \cdot \varphi(b) = e' \cdot e' = e'$. Это доказывает, что $ab \in \ker\varphi$.
  - ✓ Проверим обратимость: $\varphi(a^{-1}) = [\varphi(a)]^{-1} = (e')^{-1} = e' \Rightarrow a^{-1} \in \ker\varphi$.
  - ✓ Так как $\varphi(e) \to e'$, то $e \in \ker\varphi$.

[13] Или как красиво в «А.Г. Курош „Курс высшей алгебры“ издание девятое, 1968 г.»: Отображение φ группы G на группу G', ставящее в соответствие всякому элементу a из G однозначно определённый элемент $a' = a\varphi$ из G', называется *гомоморфным отображением* G на G' (или просто *гомоморфизмом*), если всякий элемент a' из G' служит при этом отображении образом некоторого элемента a из G, $a' = a\varphi$, и если для любых элементов a и b группы G $(ab)\varphi = a\varphi \cdot b\varphi$. Далее там сделано замечание, что до изоморфизма не хватает только взаимной однозначности.

Следует $\ker\varphi$ — подгруппа группы G.

□

Замечание 1.9.3.1 (Свойство ядра).

▷ Заметим, что $\ker\varphi$ обладает дополнительным свойством: если $x \in \ker\varphi$, то $gxg^{-1} \in \ker\varphi - \forall g \in G$. Действительно: $\varphi(gxg^{-1}) = \varphi(g) \cdot \underbrace{\varphi(x)}_{=e'} \cdot \varphi(g)^{-1} = e'$.

Лемма 1.9.4 (Нормальная подгруппа)**.**

▷ Для подгруппы N группы G следующие утверждения равносильны:

1. $\forall x \in N$, $\forall g \in G$: $gxg^{-1} \in N$;
2. $\forall g \in G$: $gNg^{-1} \subseteq N$;
3. $\forall g \in G$: $gNg^{-1} = N$;
4. $\forall g \in G$: $gN = Ng$.

Такая подгруппа называется *нормальной подгруппой*.

▷ **Доказательство**.

1) $\Rightarrow$ 2) $gxg^{-1} = \{gxg^{-1} \big| x \in N\} \subseteq N$;
2) $\Rightarrow$ 3) Имеем: $gNg^{-1} \subseteq N$, $g \leftrightarrow g^{-1} \Rightarrow g^{-1}N(g^{-1})^{-1} \subseteq N \Rightarrow g^{-1}Ng \subseteq N \Rightarrow N \subseteq gNg^{-1}$;
3) $\Rightarrow$ 4) Умножим на g и получим;
4) $\Rightarrow$ 1) Так как $gN = Ng$, то $\forall x \in N$: $\exists y \in N \big| gx = yg \Rightarrow gxg^{-1} = y \in N$.

□

Теорема 1.9.5 (Фактор группа)**.**

▷ Пусть

Пусть N — нормальная подгруппа группы G (обозначается $N \triangleright G$).

▷ Тогда

1. Множество G/N всех левых смежных классов подгруппы N в группе G образует группу относительно умножения классов: $aN \cdot bN = (ab) \cdot N$. Эта группа называется *фактор группой* группы G по нормальной подгруппе N.
2. Отображение φ: $G \to G/N$ по правилу φ: $a \to aN$ — является гомоморфизмом группы с ядром N и образом G/N.

▷ **Доказательство**.

1. Множество G/N — замкнуто относительно умножения классов, действительно: $(aN)\cdot(bN) =_{\text{(ассоциативность)}} a(Nb)N =_{\text{(предыдущая лемма)}} a(bN)N =_{(N^2 = N)} (ab)N$.

   Очевидна ассоциативность умножения, единицей G/N будет $eN = N$. Обратный класс: $(aN)^{-1} = a^{-1}N$.
2. Гомоморфизм: φ: $a \to aN$, φ: $b \to bN \Rightarrow \varphi$: $ab \to abN = aN \cdot bN$. $\operatorname{Im}\varphi = \{aN \big| a \in G\} = G/N$. Ядро $\ker\varphi = \{a \in G \big| aN = eN\} = \{a \in G \big| e^{-1}a \in N\} = N$.

□

ОПР 1.9.6 (Простой группы)**.**
Группа называется простой*, если она имеет ровно две нормальные подгруппы: единичную и саму себя:* $\{e\} \triangleright G$, $G \triangleright G$. *Если* $\exists N \triangleright G$: $\{e\} < N < G$, *то* G *в некотором роде состоит из двух меньших групп.*

Теорема 1.9.7 (Ключевая теорема о гомоморфизме)**.**

▷ Пусть

φ: $G \to G'$ — гомоморфизм групп.

▷ Тогда

$G/\ker\varphi \backsimeq \operatorname{Im}\varphi$ (изоморфна) — ключевая теорема о гомоморфизме.

▷ **Доказательство**.

∘ Зададим соответствие между G/N, где $N = \ker\varphi$ и $\operatorname{Im}\varphi$ по правилу: $aN \overset{\tilde{\varphi}}{\longleftrightarrow} \varphi(a)$, это соответствие взаимнооднозначное: $aN = bN \Leftrightarrow a^{-1}b \in N = \ker\varphi \Leftrightarrow \varphi(a^{-1}b) = e' \Leftrightarrow (\varphi(a))^{-1}\cdot\varphi(b) = e' \Leftrightarrow \varphi(a) = \varphi(b)$. Если существует, то это соответствие — изоморфизм групп: $\tilde{\varphi}(aN\cdot bN) = \tilde{\varphi}(abN) = \varphi(ab) = \varphi(a)\cdot\varphi(b) = \tilde{\varphi}(aN)\cdot\tilde{\varphi}(bN)$.

□

1.10 Прямое произведение и прямая сумма

ОПР 1.10.1 (Прямого произведения и суммы)**.**

Пусть A и B — мультипликативные группы, тогда множество $A\times B = \{(a,\,b)\big|\, a\in A,\, b\in B\}$ образует группу относительно следующей операции умножения: $(a,\,b)\cdot(a',\,b') = (aa',\,bb')$. Эта группа называется прямым произведением *A и B и обозначается: $A\times B$.*

Аналогично определяется $G_1\times G_2\times\ldots\times G_n$ и $\overbrace{G\times G\times\ldots\times G}^{n} = G^n$ — декартова степень.
Если операция записывается аддитивно, то обозначим $A\oplus B$ (вместо $\times$), $G_1\oplus G_2\oplus\ldots\oplus G_n$ и G^n.

Теорема 1.10.2 (Критерий расщепления группы на две)**.**

▷ Пусть

$A,\, B\rhd G,\; AB = G,\; A\cap B = \{e\}$.

▷ Тогда

$G\simeq A\times B$.

▷ **Доказательство**.

∘ По условию — $\forall a\in A,\, b\in B,\, g\in G$: $g = ab$. Установим соответствие $g\leftrightarrow(a,\,b)$, это соответствие взаимнооднозначное: если $g = a'b',\; a'\in A,\; b'\in B$, то $ab = a'b',\; (a')^{-1}a = b'b^{-1}\in A\cap B = \{e\}\Rightarrow$ $\Rightarrow (a')^{-1}a = e;\; (b')b^{-1} = e\Rightarrow a = a'$ и $b = b'$ (таким образом однозначность расщепления доказана).

∘ Изоморфность: покажем теперь, что $ab = ba$, при $a\in A,\; b\in B$. Рассмотрим так называемый „*коммутатор*“: $aba^{-1}b^{-1}\colon \underbrace{a}_{A}\underbrace{b\cdot a^{-1}b^{-1}}_{A}\subseteq A\cap B = \{e\}\Rightarrow ab\cdot a^{-1}b^{-1} = e\Rightarrow ab = ba$. Поэтому если $g = ab,\; g' = a'b'$, где $a,\, a'\in A;\; b,\, b'\in B$, то $gg' = aba'b' =_{(\text{свойство})} aa'\cdot bb'$. Таким образом если $g\leftrightarrow(a,\,b),\; g'\leftrightarrow(a',\,b')\Rightarrow$ $\Rightarrow gg'\leftrightarrow(aa',\,bb')$.

□

Пример 1.10.2.1 (Расщепления)**.**

▷ Пусть p и q — взаимнопростые натуральные числа, тогда $\mathbb{Z}_{pq}$ — циклическая группа порядка k, $\mathbb{Z}_{pq}\simeq\mathbb{Z}_p\times\mathbb{Z}_q$.

▷ **Доказательство**.

∘ Действительно: пусть $\mathbb{Z}_{pq} =< g >,\; \operatorname{ord} g = pq;\; A =< g^q >,\; B =< g^p >$. Ясно, что A и $B\rhd G = \mathbb{Z}_{pq}$ (в абелевой группе любая подгруппа нормальная, там сопряжение исчезает). $|A| = p,\; |B| = q\Rightarrow A\cap B\preccurlyeq A,\; A\cap B\preccurlyeq B\Rightarrow {}_{(\text{теорема Лагранжа})}|A\cap B| = 1,\; A\cap B = \{e\}$.
Осталось доказать, что произведение подгруппы — вся группа: $AB = G$. По свойствам взаимнопростых чисел, диафантово уравнение $px + qy = k$ — разрешимо $\forall k\in$
Z. Тогда $g^k = g^{px+qy} = (g^p)^x\cdot(g^q)^y\in B\cdot A = AB$ (китайская теорема о достатках).

□

Пример 1.10.2.2 (Прямого произведения, Тор)**.**

▷ $S^1\times S^1$ — равномерная сфера или окружность, равная $\{(a,\,b)\big|\, a,\, b\in S\} = \{z\in\mathbb{C}\big|\,|z| = 1\}$.

1.11 Приведение целочисленной матрицы к канонической элементарными преобразованиями

ОПР 1.11.1 (Элементарные преобразования строк)**.**

Пусть $\mathtt{A}$ *— целочисленная матрица с* n *столбцами (про строки ничего не говорится, их может быть бесконечное количество, они не на что не влияют), существуют преобразования строк (столбцов)* $\mathtt{A}$*, называемые* элементарными*:*

1. *Прибавление к одной строке (столбцу) другой строки (столбца), умноженного на* $\lambda \in \mathbb{Z}$*;*
2. *Перестановка строк (столбцов);*
3. *Умножения строки (столбца) на обратимый скаляр из* $\mathbb{Z}$*, то есть на* ± 1*.*

Теорема 1.11.2 (Приведение к каноническому виду)**.**

▷ Всякую целочисленную матрицу с n столбцами элементарными преобразованиями 1. — 3. можно привести к каноническому виду:

$$\mathtt{D} = \begin{pmatrix} d_1 & 0 & \dots & 0 & 0 \\ 0 & d_2 & \ddots & \vdots & \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \dots & 0 & d_m & \\ & & & & \\ 0 & & \dots & & 0 \end{pmatrix}, \; d_i | d_{i+1} - \forall i, \; m \geqslant 0.$$

Числа d_1, d_2, …, d_m — называются *инвариантным множеством матрицы*, они определяются по исходной матрице однозначно.

▷ **Доказательство**.

∘ Исследуем случаи по $a = \min\{|a_{ij}| \,\|\, |a_{ij}| \neq 0\}$ для линейных уравнений $a = (a_{ij})$, $1 \leqslant j \leqslant n$, $i = 1, 2, \dots, n$.

Случай 1. $\mathtt{A} = 0$, тогда доказывать нечего.

Случай 2. $\mathtt{A} \neq 0$ и существует элемент $a = a_{ij} \neq 0$, делящий нацело остальные элементы матрицы. Элементарным преобразованием 2. добьёмся, чтобы элемент a стоял на месте (1, 1), а элементарным преобразованием 1. приведём матрицу $\mathtt{A}$ к виду:

a	0	…	0
0			
$\vdots$		$\mathtt{A}'$	
0			

.

$\mathtt{A}'$ имеет меньшее количество столбцов, дальше можно сказать, что срабатывает индукция.

Случай 3. Нет такого элемента, который бы делил нацело, тогда пусть $a = a_{ij}$ — элемент наименьший по модулю и не нулевой, но a не делит какой-то элемент матрицы нацело. Тогда если $a \nmid b$, то

1. $b = a \cdot \lambda + r$, тогда $0 < r < a$, $\lambda \in \mathbb{Z}$; тогда преобразованием 1. можно получить матрицу с элементом r на месте b. Далее срабатывает индукция;
2. В итоге $\mathtt{A}$ приводится элементарными преобразованиями к диагональному виду $\mathtt{D}$.

Единственность $\mathtt{D}$ следует из сохранения чисел $D_k = $ НОД({миноры порядка k из $\mathtt{A}$}), $k < \operatorname{rk}\mathtt{A}$; при элементарных преобразованиях. Почему сохраняется? Что происходит с минорами $\mathtt{A}$ при элементарных преобразованиях:
К одной строке добавляем другую, умноженную на число, нарисуем образно:

предположим, что к i-ой строке добавили j-ую, умноженную на λ. Предположим, что они не проходили через этот минор, тогда он не меняется; если i-ая строка не походит, а j-ая проходит, он не изменяется; если он находится вне, тоже не изменяется; если i в нём, а j-ая строке нет, то тогда к строке минора добавляется внешняя строка, тогда он изменяется, но минор — это детерминант строк, а он полилинейный, то есть получится сумма детерминантов для i-ой и j-ой, умноженной на λ строк, то есть первое слагаемое — „старый“ минор, а второй — образованный какими-то строками, то есть какой-то минор из совокупности миноров порядка k, то есть либо миноры порядка k не изменятся, либо к некоторым прибавятся другие, умноженные на числа, но ведь НОД-то не изменится.
Есть ещё другие элементарные преобразований, например перестановка строк: максимум, что изменится — знак и так далее.
Видим, что $D_1 = d_1,\ D_2 = d_1d_2,\ D_3 = d_1d_2d_3,\ \ldots,\ D_n = d_1d_2d_3\ldots d_n$ и $D_i = 0$, при $i > n$. Видим, что $d_1 = D_1,\ d_2 = D_2/D_1,\ d_3 = D_3/D_2,\ \ldots,\ d_n = D_n/D_{n-1}$ и всё.

□

1.12 Свободные и конечно порождённые абелевы группы

ОПР 1.12.1 (Свободной группы)**.**
Абелева группа F называется свободной группой *с базисом $x_1, x_2, \ldots, x_n$, если всякий элемент из F имеет единственное представление вида $F = k_1 \cdot x_1 + k_2 \cdot x_2 + \ldots + k_n \cdot x_n$, где $k_i \in \mathbb{Z}$.*

Пример 1.12.1.1 (Свободной группы)**.**

▷ Пусть $F = \mathbb{Z}^n$, тогда

$$\begin{cases} x_1 = (1, 0, 0, \ldots, 0), \\ x_2 = (0, 1, 0, \ldots, 0), \\ \vdots \\ x_n = (0, 0, \ldots, 0, 1). \end{cases},$$

то есть строка единичной матрицы, отсюда $f(k_1, k_2, \ldots, k_n) = k_1 \cdot x_1 + k_2 \cdot x_2 + \ldots + k_n \cdot x_n$ — эта запись однозначна. Таким образом свободные абелевы группы существуют $\forall n$; число n называется, кстати, *рангом* группы.

УПР 1.12.1.2 (Изоморфность $\mathbb{Z}^n$)**.**

▷ Если F — свободная абелева группа, то $F \simeq \mathbb{Z}^n$.

Значение свободной абелевой группы определяет следующая теорема:

Теорема 1.12.2 (Изоморфность n-порождённой абелевой группы)**.**

▷ Всякая n-порождённая абелева группа G является (или изоморфна) подходящей фактор-группе F/N свободной абелевой группы ранга n.

▷ **Доказательство**.

∘ Пусть $G =< g_1, g_2, \ldots, g_n >$ и пусть F — свободная абелева группа с базисом $x_1, x_2, \ldots, x_n$, тогда отображение вида $\varphi\colon F \to G$ по правилу $\varphi\colon k_1 \cdot x_1 + k_2 \cdot x_2 + \ldots + k_n \cdot x_n \to k_1 \cdot g_1 + k_2 \cdot g_2 + \ldots + k_n \cdot g_n$, где $k_i \in \mathbb{Z}$, тогда это отображение является гомоморфизмом: возьмём два элемента

$$\varphi\left(\sum_i k_i \cdot x_i + \sum_j \ell_j \cdot x_j\right) = \varphi\left(\sum_j (k_i + \ell_i) \cdot x_i\right) =_{\text{(правило сложения в абелевых группах)}} \sum_i (k_i + \ell_i) \cdot g_i =$$

$$= \sum_i (k_i \cdot g_i) + \sum_j (\ell_j \cdot g_j) = \varphi\left(\sum_i k_i \cdot x_i\right) + \varphi\left(\sum_j \ell_j \cdot x_j\right).$$

Так как $\operatorname{Im}\varphi \ni g_1, g_2, \ldots, g_n$ (очевидно), то $\operatorname{Im}\varphi = G$ (из условия) и по теореме о гомоморфизмах получаем: $G = \operatorname{Im}\varphi \simeq F/\ker\varphi = F/N$, где $N = \ker\varphi$.

□

Замечание 1.12.2.1 (Все n-порождённые абелевы группы).

▷ Перечисляя подгруппы $N \preccurlyeq F$ свободной группы F, получим все n-порождённые абелевы группы.

Базис выбран не однозначно и нас интересует переход между ними.

ОПР 1.12.3 (Элементарные преобразования)**.**

Пусть $a_1, a_2, \ldots, a_s$ — система элементов свободной (это даже не важно) абелевой группы F, её элементарными преобразованиями назовём следующие:

1. *Прибавление к одному элементу системы другой, умноженный на целое число, в символах это выглядит так:*

$$\begin{cases} a_r \to a'_r = a_r + \lambda \cdot a_s, & s \neq r, \\ a_k \to a'_k = a_k, & k \neq r. \end{cases};$$

2. *Перестановка элементов системы;*
3. *Умножение некоторых элементов системы на (-1) (обратный элемент кольца $\mathbb{Z}$).*

УТВ 1.12.4 (Базис переходит в базис)**.**

▷ Всякие элементарные преобразования обратимы, базис абелевой группы элементарными преобразованиями переходит в базис (последнее важно).

▷ **Доказательство**.

1. Пусть
$$\begin{cases} x'_r = x_r + \lambda \cdot x_s, & r \neq s, \\ x'_k = x_k, & k \neq r. \end{cases},$$
причём $x_1, x_2, \ldots, x_n$ — базис и тогда $x'_1, x'_2, \ldots, x'_n$ — тоже базис. А что такое базис? Проверим, что можно однозначно записать: беру
$$\sum_i k_i \cdot x_i =_{\text{(естественно)}} k_r \cdot x_r + k_s \cdot x_s + \sum_{i \neq s,r} k_i \cdot x_i =_{\text{(нужно записать так)}}$$
$$= k_r \cdot (x_r + \lambda \cdot x_s) - k_r \cdot \lambda \cdot x_s + k_s \cdot x_s + \sum_{i \neq s,r} k_i \cdot x_i = k_r \cdot x'_r + (k_s - \lambda \cdot k_r) \cdot x'_s + \sum_{i \neq s,r} k_i \cdot x_i;$$
если $\sum_i \ell_i \cdot x'_i = 0$, то что мы получаем? То можем переписать образ без x'_i:
$$\ell_r \cdot x_r + (\ell_s + \lambda \cdot \ell_r) \cdot x_s + \sum_{i \neq s,r} \ell_i \cdot x_i = 0$$
(фактически я заменил $x'_r \to x_r + \lambda \cdot x_s$), отсюда $\ell_r = 0$, $\ell_s + \lambda \cdot \ell_r = 0$ и ещё напишем: $\ell_i = 0$, $i \neq r$, s; тогда все $\ell_i = 0$, короче говоря, запись $\sum_i \ell_i \cdot x'_i$ — однозначна.
2. Аналогично проверяется (даже проще) утверждение для 2. и 3. Так, я оставлю вам упражнение.

□

УПР 1.12.4.1 (Переходы между базисами)**.**

▷ Пусть $x_1, x_2, \ldots, x_n$ — базис свободной абелевой группы F, дальше пусть $x'_1, x'_2, \ldots, x'_n$ — некоторый набор n элементов из F. Пусть $x'_i = \sum\limits_{j=1}^{n} C_{ij} \cdot x_j$ (через базис, вообще говоря, любой элемент выражается), $\mathtt{C}$ — матрица целочисленная порядка $(n \times n)$ такая, что $\mathtt{C} = (C_{ij}) \in M_n(\mathbb{Z})$; тогда $x'_1, x'_2, \ldots, x'_n$ — базис $F \Leftrightarrow \det \mathtt{C} = \pm 1 \Leftrightarrow \mathtt{C}$ имеет целочисленную обратную матрицу. В случаях элементарных преобразований:

$$1.: \begin{pmatrix} 1 & 0 & \ldots & 0 \\ \vdots & \ddots & \ldots & 0 \\ \vdots & x & \ddots & \vdots \\ 0 & \ldots & 0 & 1 \end{pmatrix} = T_{rs}(x)$$

— трансвекция (x на месте (r, s)),

$$2.: \left(\delta_{i\pi(i)}\right), \delta_{ij} = \begin{cases} 1, & i = j, \\ 0, & i \neq j. \end{cases};$$

π подстановка,

$$3.: \begin{pmatrix} \pm 1 & 0 & \dots & 0 \\ 0 & \ddots & \vdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & \pm 1 \end{pmatrix}.$$

Осознали переходы между базисами.

Теорема 1.12.5 (Базис подгруппы свободной абелевой группы)**.**

▷ Пусть

N — подгруппа свободной абелевой группы F с фиксированным базисом $x_1, x_2, \dots, x_n$.

▷ Тогда

N — свободная, ранга $\leqslant n$ и, самое главное, N и F имеют некоторые согласованные базисы такого типа:

$$F\colon y_1, y_2, \dots, y_n;\ N\colon d_1 \cdot y_1, d_2 \cdot y_2, \dots, d_m \cdot y_m,$$

где $d_i \in \mathbb{N},\ d_i \mid d_{i+1}$.

▷ Замечание

Зачем нужна теорема? Дело в том, что мы тогда легко опишем фактор группу F/N.

▷ **Доказательство**.

◦ Пусть N — порождённая элементами $a_1, a_2, a_3, \dots$ (вообще говоря, может бесконечным количеством, но в нашей абелевой группе не больше счётного количества); $a_i = \sum_j a_{ij} \cdot x_j$, $a_{ij} \in \mathbb{Z}$; сопоставим паре систем $(x_1, x_2, \dots, x_n)$ и $(a_1, a_2, \dots, a_n)$ матрицу

$$\mathtt{A} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix},$$

элементарным преобразованиям системы $a_1, a_2, \dots, a_n$ соответствуют элементарные преобразования строк $\mathtt{A}$ (почти очевидно и ясно). Далее элементарным преобразованием системы $(x_1, x_2, \dots, x_n)$ соответствуют элементарные преобразования столбцов $\mathtt{A}$ (этот момент более тонкий, но его разобрали в примере, помните?). В общем-то можно и наоборот — от столбцов к $a_1, a_2, \dots, a_n$ и от строк к $(x_1, x_2, \dots, x_n)$.

◦ По теореме о целочисленных преобразованиях целочисленной матрицы 1.11.2 на стр. 20, можно $\mathtt{A}$ привести к каноническому диагональному виду $\mathtt{D} = \operatorname{Diag}(d_1, \dots, d_m, 0, \dots)$, $d_i \mid d_{i+1}$, $m = \operatorname{rk}\mathtt{A}$, $d_i \in \mathbb{N}$. Это означает, что существует базис $y_1, y_2, \dots, y_n$ для F такой, что $b_1 = d_1 \cdot y_1$, $b_2 = d_2 \cdot y_2, \dots, b_m = d_m \cdot y_m$ — системы порождённые для N, тогда $b_1, b_2, \dots, b_m$ — базис N:

$$\sum_{i=1}^{m} k_i \cdot b_i = 0 \Leftrightarrow \sum_{i=1}^{m} (k_i \cdot d_i) \cdot y_i = 0 \Leftrightarrow C_i \cdot y_i = 0 - \forall i \Leftrightarrow k_i = 0 - \forall i,$$

всё. Таком образом $b_1, b_2, \dots, b_m$ — требуемый базис.

□

Хорошо, давайте разберёмся с фактор-группами:

Лемма 1.12.6 (Изоморфность прямых сумм фактор групп)**.**

▷ Пусть

$G_1, G_2, \dots, G_n$ — некоторые группы, $N_i \lhd G_i - \forall i$.

▷ Тогда

$$(G_1 \oplus G_2 \oplus \dots \oplus G_n)/(N_1 \oplus N_2 \oplus \dots \oplus N_n) \simeq (G_1/N_1) \oplus (G_2/N_2) \oplus \dots \oplus (G_n/N_n).$$

▷ **Доказательство**.

∘ Пусть $\varphi_i\colon G_i \to G_i/N_i$ — гомоморфизм факторизации, фактически $\varphi_i(x) = x + N_i$, то есть элементу сопоставляется тот класс, где он содержится; тогда $\varphi\colon (g_1, g_2, \ldots, g_n) \to (\varphi_1(g_1), \varphi_2(g_2), \ldots, \varphi_n(g_n))$ — гомоморфизм (сумма в сумму переводится и всё); $\operatorname{Im}\varphi = \bigoplus_i G_i/N_i$ и $\ker\varphi = \bigoplus_i N_i$. По теореме о гомоморфизмах 1.9.7 на стр. 18: $\bigoplus_i G_i/N_i = \operatorname{Im}\varphi \simeq \bigoplus_i G_i/\ker\varphi = \bigoplus_i G_i/\bigoplus_i N_i$, вот мы и получили, что надо.

□

Теорема 1.12.7 (Разложение в прямую сумму конечной порождённой абелевой группы)**.**

▷ Всякая конечная абелева группа разлагается в прямую сумму конечных или бесконечных циклов: $G \simeq \mathbb{Z}_{d_1} \oplus \mathbb{Z}_{d_2} \oplus \ldots \oplus \mathbb{Z}_{d_m} \oplus \underbrace{\mathbb{Z} \oplus \mathbb{Z} \oplus \ldots \oplus \mathbb{Z}}_{n-m}$ — так устроена.

▷ **Доказательство**.

∘ Пусть G — n-порождённая группа, по теореме 1.12.2 на стр. 21 мы можем утверждать, что $G \simeq F/N$, где F — свободная абелева группа, тогда по теореме 1.12.5 на стр. 23 исходный базис F можно перестроить, то есть F и N имеют согласованные базисы(то, что там рисовал раньше): $F\colon y_1, y_2, \ldots, y_m, y_{m+1}, \ldots, y_n$; $N\colon d_1 \cdot y_1, d_2 \cdot y_2, \ldots, d_m \cdot y_m$, причём $d_i \in \mathbb{N}$, $d_i \mid d_{i+1}$; тогда

$$G \simeq F/N \simeq_{(\text{ свободная абелева группа } \mathbb{Z}^n = \mathbb{Z}\oplus\mathbb{Z}\oplus\ldots\oplus\mathbb{Z}\text{, вот я это и записал })}$$
$$\simeq (< y_1 > \oplus < y_2 > \oplus \ldots \oplus < y_n >)/(< d_1 \cdot y_1 > \oplus < d_2 \cdot y_2 > \oplus \ldots \oplus < d_m \cdot y_m >) \simeq$$
$$\simeq_{(\text{лемма})} < y_1 >/< d_1 \cdot y_1 > \oplus < y_2 >/< d_2 \cdot y_2 > \oplus \ldots \oplus < y_m >/< d_m \cdot y_m > \oplus < y_{m+1} > \oplus \ldots \oplus < y_n > \simeq$$
$$\simeq \mathbb{Z}_{d_1} \oplus \mathbb{Z}_{d_2} \oplus \ldots \oplus \mathbb{Z}_{d_m} \oplus \mathbb{Z} \oplus \ldots \oplus \mathbb{Z}.$$

□

Займёмся вопросами единственности, нас интересует на сколько однозначно разложение.

Следствие 1.12.7.1 (Разложение в сумму конечно-порождённой абелевой группы).

▷ Всякая конечно-порождённая абелева группа является прямой сумой бесконечных циклических групп или примарных циклических (матрица в степени p — простое число).

▷ **Доказательство**.

∘ Пусть $d = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_s^{k_s}$, p_i — различные простые числа, $k_i \in \mathbb{N}$; тогда $\mathbb{Z}_d \simeq \mathbb{Z}_{p_1^{k_1}} \oplus \mathbb{Z}_{p_2^{k_2}} \oplus \ldots \oplus \mathbb{Z}_{p_s^{k_s}}$, так как $p_1^{k_1}, p_2^{k_2}, \ldots, p_s^{k_s}$ — попарно взаимно простые (утверждение 1.10.2.1 на стр. 19: если $(p, q) = 1$, то $\mathbb{Z}_{pq} \simeq Z_p \oplus \mathbb{Z}_q$).

□

ОПР 1.12.8 (Периодической, примарной и p-кратной части группы)**.**
Для абелевой группы G обозначим $T(G) = \{g \in G \mid \operatorname{ord} g < \infty\}$, дальше:

$$T_p(G) = \{g \in G \mid \operatorname{ord} g = p^k,\ p - \textit{простое},\ k \in \mathbb{N}\}$$

и $pG = \{pg \mid g \in G\}$.

Можно подчеркнуть: здесь p — простое число, тогда $T(G)$, $T_p(G)$ и pG — подгруппы: это легко, если $ng = 0$ (порядка n), $mh = 0$ (элемент порядка h), тогда $nm \cdot (g \pm h) = 0$; если $p^k \cdot g = 0$ и $p^\ell \cdot h = 0 \Rightarrow p^{k+\ell} \cdot (g \pm h) = 0; \operatorname{ord}(g \pm h) \mid p^{k+\ell} \Rightarrow \operatorname{ord}(g \pm h) = p^m; pg \pm ph = p \cdot (g \pm h)$.

Эти подгруппы называются соответственно периодической частью *группы G*, *p*-примарной частью *и p*-кратной частью *группы G.*

ОПР 1.12.9 (Изоморфизм частей)**.**

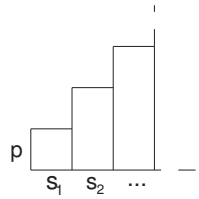
Так как при изоморфизме сохраняется порядок элемента, а так же свойство быть кратным, то изоморфизм $G \simeq G'$ влечёт изоморфизм $T(G) \simeq T(G')$, $T_p(G) \simeq T_p(G')$ и $pG \simeq pG'$ (конечно очевидно, конечные переходят в конечные и тому подобное). Всякая абелева группа G имеет вид: $G \simeq \left(\bigoplus_{p\text{ - простое}} T_p(G)\right) \oplus \mathbb{Z}_r$ (мы это где-то доказали). Если $G \simeq G'$, то $T_p(G) = T_p(G')$ и, кроме того, $\mathbb{Z}_r = G/T(G) \simeq G/T(G') = \mathbb{Z}_s \Leftrightarrow r = s$ (упражнение).

Теорема 1.12.10 (Разложение абелевой группы в прямую сумму)**.**

▷ Всякая абелева группа разлагается в прямую сумму примарно-циклических и бесконечно-циклических, и количество соответствующих слагаемых не зависит от способа разложения.

▷ **Доказательство**.

∘ Достаточно провести для p групп: пусть $G = \overbrace{\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \ldots \oplus \mathbb{Z}_p}^{s_1} \oplus \overbrace{\mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^2} \oplus \ldots \oplus \mathbb{Z}_{p^2}}^{s_2} \oplus \ldots$; надо доказать, что числа s_1, s_2, … не зависят от способа разложения. Для этого на самом деле нарисуем:



Рассмотрим отображение $\varphi\colon x \to px$, имеем: $|G| = p^{s_1} \cdot (p^2)^{s_2} \cdot \ldots = p^{s_1+2s_2+\cdots}$, дальше я возьму $|pG| = p^{s_2} \cdot (p^2)^{s_3} \cdot \ldots = p^{s_2+2s_3+\cdots}$, этот процесс можно продолжить: $\log_p |G| = s_1 + 2s_2 + \ldots$; $\log_p |pG| = s_2 + 2s_3 + \ldots$. Что мы имеем: очень похожая ситуация как в Жордановой форме, отсюда s_1, s_2, … — однозначно определены по порядку группы.

□

Глава 2

Основы теории чисел

ОПР 2.1 (Последовательности Фибоначчи)**.**
Пусть (F_n) — последовательность Фибоначчи, *то есть* $F_0 = 0,\ F_1 = 1,\ \ldots,\ F_{n+1} = F_n + F_{n-1}$; *выпишем первые:* 0, 1, 1, 2, 3, 5, 8, ... *Будем использовать идею:* $F_{n+1} = F_n + F_{n-1}$ — *целая часть плюс остаток.*

Лемма 2.2 (Нижняя оценка последовательности Фибоначи)**.**

▷ Число $F_{5+n} > 10 \cdot F_n$, при $n \geqslant 2$.

▷ **Доказательство**.

- Индукцией по n:
  - ✓ Мы имеем при $n = 2$: $F_7 = 13 > 10 \cdot 1 = 10 \cdot F_2$ — верно.
  - ✓ Далее $n - 1 \mapsto n$:

$$F_{5+n} = F_{n+4} + F_{n+3} = 2 \cdot F_{n+3} + F_{n+2} = 3 \cdot F_{n+2} + 2 \cdot F_{n+1} = 5 \cdot F_{n+1} + 3 \cdot F_n = \\ = 8 \cdot F_n + 5 \cdot F_{n-1} > 8 \cdot F_n + 4 \cdot F_{n-1} \geqslant 8 \cdot F_n + 2 \cdot F_n = 10 \cdot F_n,$$

так как $F_n = F_{n-1} + F_{n-2} \leqslant 2 \cdot F_{n-1}$.

□

Лемма 2.3 (Нижняя оценка чисел Фибоначи)**.**

▷ Число $F_{n+5\cdot\ell} > 10^\ell \cdot F_n,\ n \geqslant 2$.

▷ **Доказательство**.

- Индукцией по ℓ:
  - ✓ $\ell = 1$ — лемма 2.2.
  - ✓ $\ell - 1 \mapsto \ell$:

$$F_{n+5\cdot\ell} = F_{5+n+5\cdot(\ell-1)} >_{\text{(лемма 2.2)}} 10 \cdot F_{n+5\cdot(\ell-1)} > \\ >_{\text{(индукционное предположение)}} 10 \cdot 10^{\ell-1} \cdot F_n = 10^\ell \cdot F_n.$$

□

Теорема 2.4 (Ламе)**.**

▷ Пусть
a и b — натуральные числа, считаем $a > b$ и ℓ = число десятичных знаков в десятичном представлении числа b.

▷ Тогда
Число деления в алгоритме Евклида для вычисления НОД$(a,\ b)$ не больше, чем $5 \cdot \ell$.

▷ Замечание

Фактически: $10^{\ell-1} < b < 10^{\ell} \Rightarrow \lg \ell < \ell < \lg \ell + 1 \Rightarrow$ качественно — оценка шагов логарифмическая.

▷ **Доказательство**.

- Из алгоритма Евклида имеем:
$$\begin{cases} a & = b \cdot q_1 + r_2; \\ b & = r_2 \cdot q_2 + r_3; \\ r_2 & = r_3 \cdot q_3 + r_4; \\ \vdots & \\ r_{n-2} & = r_{n-1} \cdot q_{n-1} + r_n; \\ r_{n-1} & = r_n \cdot q_n. \end{cases}$$ — n шагов. У нас последовательность чисел такова, что $\begin{cases} 0 < r_2 < b; \\ 0 < r_3 < r_2; \\ \vdots \\ 0 < r_n < r_{n-1}. \end{cases}$,
но $r_n \neq 0$ и r_n, r_{n-1} — целые $\Rightarrow 1 = F_2 \leqslant r_n$, $2 = F_3 \leqslant r_{n-1}$, …, где F_i — i-ое число Фибоначчи.
- Далее распишем:
$$r_{n-2} = r_{n-1} \cdot q_{n-1} + r_n \geqslant r_{n-1} + r_n \geqslant F_3 + F_2 = F_4,$$
$$r_{n-3} = r_{n-2} \cdot q_{n-2} + r_{n-1} \geqslant r_{n-2} + r_{n-1} \geqslant F_4 + F_3 = F_5,$$
$$\dots$$
продолжая, получим: $b = r_1 \geqslant F_{(n-2)-1+4} = F_{n+1}$.
- Предположим $n > 5 \cdot \ell$, тогда $n \geqslant 5 \cdot \ell + 1 \Rightarrow (n+1) \geqslant 5 \cdot \ell + 2$, заменяем индексы: $b \geqslant F_{n+1} \geqslant F_{5 \cdot \ell + 2} >_{\text{(Лемма)}} 10^{\ell} \cdot$ $\cdot F_2 = 10^{\ell}$. (то есть b больше своей длины). Это противоречит предположению о числе b, следует $n \leqslant 5 \cdot \ell$.

□

Замечание 2.4.1 (Особенность оценки).

▷ Эта оценка достигается на последовательности Фибоначчи при некотором ℓ.

2.5 Непрерывные дроби и их свойства

ОПР 2.5.1 (Конечной непрерывной дроби)**.**

Из алгоритма Евклида:

$$\begin{cases} a & = b \cdot q_1 + r_2; \\ b & = r_2 \cdot q_2 + r_3; \\ r_2 & = r_3 \cdot q_3 + r_4; \\ \vdots & \\ r_{n-2} & = r_{n-1} \cdot q_{n-1} + r_n; \\ r_{n-1} & = r_n \cdot q_n. \end{cases}$$

получаем:

$$\frac{a}{b} = q_1 + \frac{r_2}{b} = q_1 + \frac{1}{b/r_2} = q_1 + \frac{1}{q_2 + \dfrac{1}{r_2/r_3}} = q_1 + \frac{1}{q_2 + \dfrac{1}{q_3 + \dfrac{1}{r_3/r_4}}} = \dots = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ddots \cfrac{}{q_{n-1} + \cfrac{1}{q_n}}}}}.$$

Это выражение называется конечной непрерывной дробью *(иногда говорят* цепной дробью*). Отметим, что в этом представлении для* $\frac{a}{b}$ *имеем* $q_n > 1$ *и все* $q_i \geqslant 1$.

Обозначения:

$$[q_1, q_2, \dots, q_k] = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ddots \cfrac{}{q_{k-1} + \cfrac{1}{q_k}}}}},$$

это выражение называется k-ой подходящей дробью, *для кротости обозначим* δ_k. *Из определения видно:*

- $[q_1,\, q_2,\, \ldots,\, q_k] = q_1 + \dfrac{1}{[q_2,\, q_3,\, \ldots,\, q_k]}$;
- $[q_1,\, \ldots,\, q_{k-1},\, q_k] = \left[q_1,\, q_2,\, \ldots,\, q_{k-1} + \dfrac{1}{q_k}\right]$.

Теорема 2.5.2 (Соответствия)**.**

▷ Пусть

$q_1,\, q_2,\, \ldots,\, q_n,\, \ldots$ — произвольная последовательность непрерывных чисел и $[q_1,\, q_2,\, \ldots,\, q_n] = \dfrac{P_n}{Q_n}$, при $n \geqslant 1$.

▷ Тогда

$\begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} q_2 & 1 \\ 1 & 0 \end{pmatrix} \cdot \ldots \cdot \begin{pmatrix} q_n & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} P_n & P_{n-1} \\ Q_n & Q_{n-1} \end{pmatrix}$; верно и обратное утверждение, то есть из матричного равенства следует равенство для подходящей дроби.

▷ **Доказательство**.

- Используем индукцию, естественно:
  - ✓ По определению положим $P_0 = 1,\ Q_0 = 0$, тогда при $n = 1$ — верно.
  - ✓ Используем индукционных переход $n - 1 \mapsto n$: предположим, что $[q_2,\, q_3,\, \ldots,\, q_n] = \dfrac{X_{n-1}}{Y_{n-1}}$. Предположение индукции гласит: $\begin{pmatrix} q_2 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} q_3 & 1 \\ 1 & 0 \end{pmatrix} \cdot \ldots \cdot \begin{pmatrix} q_n & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} X_{n-1} & X_{n-2} \\ Y_{n-1} & Y_{n-2} \end{pmatrix}$; тогда

$$\begin{pmatrix} P_n & P_{n-1} \\ Q_n & Q_{n-1} \end{pmatrix} = \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} X_{n-1} & X_{n-2} \\ Y_{n-1} & Y_{n-2} \end{pmatrix} = \begin{pmatrix} q_1 \cdot X_{n-1} + Y_{n-1} & q_1 \cdot X_{n-2} + Y_{n-2} \\ X_{n-1} & X_{n-2} \end{pmatrix} \Rightarrow$$

$$\Rightarrow \frac{P_n}{Q_n} = \frac{q_1 \cdot X_{n-1} + Y_{n-1}}{X_{n-1}} = q_1 + \frac{Y_{n-1}}{X_{n-1}} = q_1 + \frac{1}{[q_2,\, q_3,\, \ldots,\, q_n]} = [q_1,\, q_2,\, \ldots,\, q_n].$$

□

Следствие 2.5.2.1 (Дополнительные равенства).

▷ Выполняется:

1. $P_n \cdot Q_{n-1} - Q_n \cdot P_{n-1} = (-1)^n$;
2. Числа P_n и Q_n взаимопросты, при $n \geqslant 1$;
3. $\dfrac{P_n}{Q_n} - \dfrac{P_{n-1}}{Q_{n-1}} = \dfrac{(-1)^k}{Q_n \cdot Q_{n-1}}$;
4. $\dfrac{P_n}{Q_n} = q_1 + \sum\limits_{k=2}^{n} \dfrac{(-1)^n}{Q_k \cdot Q_{k-1}}$;
5. $P_n = q_n \cdot P_{n-1} + P_{n-2},\ Q_n = q_n \cdot Q_{n-1} + Q_{n-2}$, для $n \geqslant 2$;
6. $Q_n \geqslant 2^{\frac{n-2}{2}}$, $n \geqslant 2$.

▷ **Доказательство**.

1. Надо взять детерминант от матричного равенства.
2. Из первого пункта видно: если это не так, то есть делитель единицы.
3. Из первого пункта.
4. $\dfrac{P_n}{Q_n} = \dfrac{P_1}{Q_1} + \left(\dfrac{P_2}{Q_2} - \dfrac{P_1}{Q_1}\right) + \left(\dfrac{P_3}{Q_3} - \dfrac{P_2}{Q_2}\right) + \ldots + \left(\dfrac{P_n}{Q_n} - \dfrac{P_{n-1}}{Q_{n-1}}\right)$ и по предыдущему пункту.
5. Используя матричное равенство: $\begin{pmatrix} P_{n-1} & P_{n-2} \\ Q_{n-1} & Q_{n-2} \end{pmatrix} \cdot \begin{pmatrix} q_n & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} P_n & P_{n-1} \\ Q_n & Q_{n-1} \end{pmatrix}$.
6. По индукции опять:
   - ✓ $n = 1$: $Q_2 =_{\text{(пункт 5.)}} q_2 \geqslant 1 = 2^{\frac{2-2}{2}}$.
   - ✓ Индукционный переход $n - 1 \mapsto n$: $Q_n =_{\text{(пункт 5.)}} q_n \cdot Q_{n-1} + Q_{n-2} \geqslant Q_{n-1} + Q_{n-2} \geqslant 2 \cdot Q_{n-2} \geqslant$ $\geqslant_{\text{(индукционное предположение)}} 2 \cdot 2^{\frac{n-2-2}{2}} = 2^{\frac{n-2}{2}}$.

□

2.6 Приближение иррациональных чисел подходящими дробями

ОПР 2.6.1 (Подходящей дроби к иррациональному числу)**.**

Пусть $\alpha \in \mathbb{R},\ \alpha \geqslant 0$; *обозначим* $\lfloor\alpha\rfloor$ *— целая часть* α*, то есть ближайшее слева целое число, а за* $\{\alpha\}$ *— дробную часть* α*, тогда* $\lfloor\alpha\rfloor \leqslant \alpha < \lfloor\alpha\rfloor + 1$ *и* $\alpha = \lfloor\alpha\rfloor + \{\alpha\}$. $\lfloor\alpha\rfloor \in \mathbb{Z}$ *и* $0 \leqslant \{\alpha\} < 1$*, предположим, что* α *— иррациональное, тогда* $\alpha = \lfloor\alpha\rfloor + \{\alpha\} = \lfloor\alpha\rfloor + \dfrac{1}{1/\{\alpha\}}$; *тогда* $\dfrac{1}{\{\alpha\}} > 1$ *и иррациональное.*

Обозначим $q_1 = \lfloor\alpha\rfloor,\ \alpha_1 = \{\alpha\} \Rightarrow \alpha = q_1 + \alpha_1$. *Выберем* $\dfrac{1}{\alpha_1} = q_2 + \alpha_2,\ q_2 = \left\lfloor\dfrac{1}{\alpha_1}\right\rfloor,\ \alpha_2 = \left\{\dfrac{1}{\alpha}\right\}$, *тогда* $\alpha = q_1 + \dfrac{1}{q_2 + \alpha_2}$. *Далее* $q_3 = \left\lfloor\dfrac{1}{\alpha_2}\right\rfloor,\ \alpha_3 = \left\{\dfrac{1}{\alpha_2}\right\}$, $\ldots$; *тогда*

$$\alpha = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ddots}}}.$$

Последовательность дробей $\delta_k = [q_1,\, q_2,\, \ldots,\, q_k]$ *называется* k-ой подходящей дробью к иррациональному числу α.

Имеет место следующее равенство: $\alpha = [q_1,\, q_2,\, \ldots,\, q_n + \alpha_n] - \forall n \geqslant 1$. *Определим теперь бесконечно подходящую дробь* $[q_1,\, q_2,\, \ldots,\, q_n,\, \ldots]$ *как предел* $\lim\limits_{n\to\infty} \dfrac{P_n}{Q_n} = q_1 + \sum\limits_{k=2}^{\infty} \dfrac{(-1)^k}{Q_k \cdot Q_{k-1}}$. *Этот предел существует, почему? как сумма знакопеременного ряда с убывающими, стремящимися к нулю элементами.*

Лемма 2.6.2 (Границы α)**.**

▷ Для всякого n либо $\delta_{n-1} < \alpha < \delta_n$, либо $\delta_n < \alpha < \delta_{n-1}$.

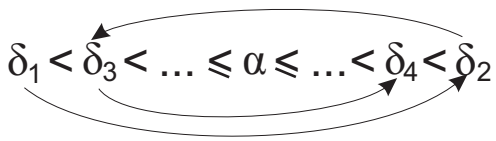
▷ **Доказательство**.

∘ Рассмотрим функцию $f(x) = [q_1,\, q_2,\, \ldots,\, q_{n-1},\, x]$, тогда $f(q_n) = \dfrac{P_n}{Q_n} = \delta_n,\ f(q_n + \alpha_n) = \alpha,\ f\left(q_n + \dfrac{1}{q_{n+1}}\right) = \dfrac{P_{n+1}}{Q_{n+1}} = \delta_{n+1}$.

∘ Следовательно $f(x) = \dfrac{x \cdot P_{n-1} + P_{n-2}}{x \cdot Q_{n-1} + Q_{n-2}}$, более того

$$f'(x) = \frac{P_{n-1} \cdot (x \cdot Q_{n-1} + Q_{n-2}) - Q_{n-1} \cdot (x \cdot P_{n-1} - P_{n-2})}{(x \cdot Q_{n-1} + Q_{n-2})^2}.$$

Функция дифференцируема и производная положительна или отрицательна, функция строго монотонна. На самом деле это — гипербола, $q_n < \underbrace{q_n + \alpha_n}_{=\alpha} < q_n + \dfrac{1}{q_{n+1}} \Rightarrow f(q_n) \gtrless f(\alpha) \gtrless f\left(q_n + \dfrac{1}{q_{n+1}}\right) \Rightarrow \delta_n \gtrless \alpha \gtrless \delta_{n+1}$. На самом деле это:



□

Теорема 2.6.3 (Единственность представления иррациональных чисел)**.**

▷ Любые иррациональные числа имеют единственное представление в виде подходящей дроби.

▷ **Доказательство**.

∘ Пусть $\alpha = [q_1, q_2, \ldots]$ — бесконечная непрерывная дробь, равная $[q'_1,\ q'_2, \ldots]$; предположим, что $q_1 = q'_1, \ldots, q_{k-1} = q'_{k-1}, q_k \neq q'_k$; пусть функция $f(x) = [q_1, q_2, \ldots, q_{k-1}, x]$, тогда мы знаем, что $f(q_k) = \frac{P_k}{Q_k}$; $f(q_k + \alpha_k) = \alpha$; $f\left(q_k + \frac{1}{q_{k+1}}\right) = \frac{P_{k+1}}{Q_{k+1}}$. Аналогично $f(q'_k + \alpha'_k) = \alpha$, но f — строго монотонная функция, следовательно $q_k + \alpha_k = q'_k + \alpha'_k$, мы знаем, что $0 < \alpha_k,\ \alpha'_k < 1$, а $q_k,\ q'_k \in \mathbb{Z}$; отсюда заключаем, что $q_k = q'_k$.

□

УПР 2.6.4 (Представление рациональных чисел)**.**

▷ Доказать, что рациональные числа имеют единственное представление в виде конечной десятичной дроби $[q_1, q_2, \ldots, q_n]$, но $q_n > 1$ (если бы имели в конце $2 = 1 + \frac{1}{1}$, $3 = 2 + \frac{1}{1}$ и последний $\neq 1$; $\frac{1}{2} = \frac{1}{1+1/1}$, при $n > 1$).

Теорема 2.6.5 (Приближение дробей)**.**

▷ $|\alpha - \delta_{k-1}| > |\alpha - \delta_k|$, то есть всякая последующая дробь точнее приближает, чем предыдущая.

▷ **Доказательство**.

∘

□

ОПР 2.6.6 (Наилучшего приближения)**.**

Число a/b, где $a \in \mathbb{Z}$, $b \in \mathbb{N}$ — называется наилучшим приближением *к числу α, если $\forall x,\ y \in \mathbb{Z},\ y > 0$: если x/y — лучше приближается: $|\alpha - x/y| < |\alpha - a/b|$, то $y > b$.*

Теорема 2.6.7 (Наилучшее приближение для вещественного числа)**.**

▷ Подходящая дробь $\delta_k = P_k/Q_k$ является наилучшим приближением для соответствующего вещественного числа α.

▷ **Доказательство**.

∘ Случай 1:
n — четное, тогда $\frac{P_{n-1}}{Q_{n-1}} < \alpha < \frac{P_n}{Q_n}$; пусть $x \in \mathbb{Z}$, $y \in \mathbb{N}$ и $\left|\alpha - \frac{x}{y}\right| < \left|\alpha - \frac{P_n}{Q_n}\right|$, тогда

$$\left|\frac{x}{y} - \frac{P_{n-1}}{Q_{n-1}}\right| < \left|\frac{P_n}{Q_n} - \frac{P_{n-1}}{Q_{n-1}}\right| =_{\text{(Следствие 2.5.2.1 на стр. 28)}} \frac{1}{Q_n \cdot Q_{n-1}},$$

но

$$\left|\frac{x}{y} - \frac{P_{n-1}}{Q_{n-1}}\right| = \frac{m}{y \cdot Q_{n-1}} \geqslant_{\text{(т.к. } m \in \mathbb{N})} \frac{1}{y \cdot Q_{n-1}}.$$

Значит, $\frac{1}{y \cdot Q_{n-1}} < \frac{1}{Q_n \cdot Q_{n-1}}$, т.е. $y > Q_n$, а это и есть свойство наилучшего приближения.

∘ Случай 2:
n — нечетное, тогда $\frac{P_n}{Q_n} < \alpha < \frac{P_{n-1}}{Q_{n-1}}$, а далее рассуждение аналогичные случаю 1.

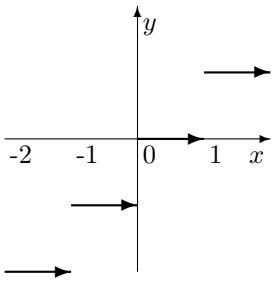
□

2.7 Арифметические функции

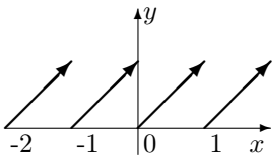
2.7.1 Целая и дробная части числа

ОПР 2.7.1.1 (Целой и дробной частей числа)**.**
Целая часть: $\lfloor x \rfloor \in \mathbb{Z},\ \lfloor x \rfloor \leqslant x \leqslant \lfloor x \rfloor + 1;\ x = \lfloor x \rfloor + \alpha;\ 0 \leqslant \alpha < 1,\ \{x\} = \alpha$ — дробная часть.

Целая часть числа



Дробная часть числа



Теорема 2.7.1.2 (Свойства целой части числа)**.**

1. $\lfloor x + m \rfloor = \lfloor x \rfloor + m - \forall m \in \mathbb{Z}$;
2. $\lfloor x/n \rfloor = \left\lfloor \frac{\lfloor x \rfloor}{n} \right\rfloor - \forall n \in \mathbb{N}$;
3. $\lfloor x \rfloor + \lfloor y \rfloor \leqslant \lfloor x + y \rfloor \leqslant \lfloor x \rfloor + \lfloor y \rfloor + 1$.

▷ **Доказательство**.

1. $x = \lfloor x \rfloor + \alpha$, где $0 \leqslant \alpha < 1$, $\lfloor x \rfloor \in \mathbb{Z} \Rightarrow x + m = \lfloor x \rfloor + \alpha + m$;
2. $x = \lfloor x \rfloor + \alpha$, $0 \leqslant \alpha < 1$; представим $\lfloor x \rfloor = nq + r$, где $0 \leqslant r < n$; $r,\ q \in \mathbb{Z}$, тогда разделили с остатком на n: $\frac{\lfloor x \rfloor}{n} = q + \frac{r}{n} \Rightarrow \left\lfloor \frac{\lfloor x \rfloor}{n} \right\rfloor = q$. Теперь рассмотрим $x = nq + r + \alpha \Rightarrow \frac{x}{n} = q + \frac{r}{n} + \frac{\alpha}{n} = q + \frac{r+\alpha}{n}$, но $0 \leqslant \alpha < 1 \Rightarrow$ так как $r \in \mathbb{Z}$: $0 \leqslant r + \alpha < n \Rightarrow \left\lfloor \frac{x}{n} \right\rfloor = q = \left\lfloor \frac{\lfloor x \rfloor}{n} \right\rfloor$.
3. Упражнение.

□

ОПР 2.7.1.3 (Кратности числа)**.**
Пусть p — простое число, n — натуральное число, тогда существует число $k \geqslant 0$ такое, что $p^k \mid n$, $p^{k+1} \nmid n$. Обозначим $k = k_p(n)$ — кратность числа p *в* n.

Следствие 2.7.1.4 (Формула для кратности факториала).

▷ $k_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \ldots$

▷ **Доказательство**.

○ Индукцией по n (начало очевидно, сразу индукционный переход): в числе $n! = 1 \cdot 2 \cdot \ldots \cdot n$ делятся на p сомножители p, $2p$, …, $n_1 p$, где $n_1 p < n$, а n_1 — максимальное, $n_1 = \left\lfloor \frac{n}{p} \right\rfloor$. Тогда: $k_p(n!) = k_p(p \cdot 2p \cdot \ldots \cdot n_1 p) = n_1 + k_p(n_1!) =_{\text{(индукция)}} \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n_1}{p} \right\rfloor + \ldots = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{\lfloor n/p \rfloor}{p} \right\rfloor + \ldots =_{\text{(Теорема 2.7.1.2)}} \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \ldots$

□

Пример 2.7.1.5 (На кратность)**.**

▷ Найдём количество нулей в десятичном разложении числа 100!. Это минимум из чисел $k_2(100!)$ и $k_5(100!)$ (так как каждая цифра 2 вместе с цифрой 5 дают нам в произведении нуль — прим. ред.)

$$k_2(100!) = \left\lfloor \frac{100}{2} \right\rfloor + \left\lfloor \frac{100}{4} \right\rfloor + \left\lfloor \frac{100}{8} \right\rfloor + \left\lfloor \frac{100}{16} \right\rfloor + \left\lfloor \frac{100}{32} \right\rfloor + \left\lfloor \frac{100}{64} \right\rfloor = 50 + 25 + 12 + 6 + 3 + 1 = 97;$$

$$k_5(100!) = \left\lfloor \frac{100}{5} \right\rfloor + \left\lfloor \frac{100}{25} \right\rfloor + \left\lfloor \frac{100}{125} \right\rfloor = 20 + 4 = 24.$$

Следовательно, нулей — 24.

2.7.2 Число делителей и сумма делителей

ОПР 2.7.2.1 (Числа и суммы делителей)**.**

Число натуральных делителей натурального числа n обозначается $\tau(n) = \sum\limits_{d|n} 1$. *Сумма натуральных делителей натурального числа n обозначается* $\sigma(n) = \sum\limits_{d|n} d$.

ОПР 2.7.2.2 (Мультипликативной функции)**.**

Арифметическая функция $f\colon \mathbb{N} \to \mathbb{C}$ *называется* мультипликативной, *если* $f(m \cdot n) = f(m) \cdot f(n)$ *для любых взаимнопростых чисел* m, n.

Пример 2.7.2.3 (Мультипликативных функций)**.**

▷ $i(n) = 1 \text{—} \forall n$;

▷ $e(n) = n \text{—} \forall n$.

Теорема 2.7.2.4 (О мультипликативных функциях)**.**

▷ Пусть

f— мультипликативная функция.

▷ Тогда

Функция $g(n) = \sum\limits_{d|n} f(d)$ — так же является мультипликативной.

▷ **Доказательство**.

◦ Пусть m, $n \in \mathbb{N}$ и они взаимнопростые, тогда

$$g(m \cdot n) = \sum_{d|mn} f(d) = \sum_{d_1|m,\ d_2|n} f(d_1 \cdot d_2) = \sum_{d_1|m,\ d_2|n} f(d_1) \cdot f(d_2) = \left(\sum_{d_1|m} f(d_1)\right) \cdot \left(\sum_{d_2|n} f(d_2)\right) = g(m) \cdot g(n).$$

□

Следствие 2.7.2.5 (Мультипликативность функций числа и суммы делителей).

▷ Функции $\tau(n)$, $\sigma(n)$ — мультипликативны.

▷ **Доказательство**.

◦ $\tau(n) = \sum\limits_{d|n} 1 = \sum\limits_{d|n} i(d)$; $\sigma(n) = \sum\limits_{d|n} d = \sum\limits_{d|n} e(d)$.

□

Следствие 2.7.2.6 (Выражения для функций числа и суммы делителей).

▷ Пусть

$n = \prod\limits_{i=1}^{s} p_i^{k_i}$, p_i — различные простые числа, $k \in \mathbb{N}$.

▷ Тогда

◦ $\tau(n) = \prod\limits_{i=1}^{s} (k_i + 1)$;

◦ $\sigma(n) = \prod\limits_{i=1}^{s} \frac{p_i^{k_i+1}-1}{p_i-1}$.

▷ **Доказательство**.

◦ Ввиду мультипликативности получаем: $\tau(n) = \prod\limits_{i=1}^{s} \tau(p_i^{k_i})$, осталось найти $\tau(p^k)$, p— простое, но ясно, что p^k имеет следующие натуральные делители: $\underbrace{1, p, p^2, \ldots, p^k}_{k+1}$, значит, $\tau(p^k) = k + 1$.

◦ Аналогично: $\sigma(n) = \prod\limits_{i=1}^{s} \sigma(p_i^{k_i})$, найдём $\sigma(p^k) = 1 + p + p^2 + \ldots + p^k = \frac{p^{k+1}-1}{p-1}$.

□

2.7.3 Функция Мебиуса

ОПР 2.7.3.1 (Функции Мебиуса)**.**

Функция

$$\mu(n) = \begin{cases} 1, & n = 1; \\ 0, & \exists p — \textit{простое}\colon p^2 \mid n; \\ (-1)^s, & n = p_1 \cdot p_2 \cdot \ldots \cdot p_s,\ p_i — \textit{различные простые}. \end{cases}$$

называется функцией Мебиуса.

Теорема 2.7.3.2 (О функции Мебиуса)**.**

1. Функция Мебиуса — мультипликативная;
2. $\delta(n) := \sum\limits_{d|n} \mu(d) = \begin{cases} 1, & n = 1, \\ 0, & n > 1. \end{cases}$
3. Имеет место формула обращения Мебиуса:

$$g(n) := \sum_{d|n} f(d) \Leftrightarrow f(n) = \sum_{d|n} \mu(d) \cdot g\left(\frac{n}{d}\right) = \sum_{d|n} \mu\left(\frac{n}{d}\right) \cdot g(d).$$

▷ **Доказательство**.

1. Рассмотрим:
   а). При $m = 1$ или $n = 1$: $\mu(n \cdot m) = \mu(n) \cdot \mu(m)$.
   б). Пусть $m,\ n > 1$, $(m,\ n) = 1$, тогда:
   - ✓ Если $\exists p > 1 \big| p^2 \big| m$ или $p^2 \big| n$, то $p^2 \big| m \cdot n \Rightarrow \mu(m \cdot n) = 0 = \mu(n) \cdot \mu(m)$.
   - ✓ Если $m = p_1 \cdot p_2 \cdot \ldots \cdot p_s,\ n = q_1 \cdot q_2 \cdot \ldots \cdot q_r$, где $p_1,\ p_2,\ \ldots,\ p_s$ и $q_1,\ q_2,\ \ldots,\ q_r$ — различные простые числа, то $m \cdot n = p_1 \cdot p_2 \cdot \ldots \cdot p_s \cdot q_1 \cdot q_2 \cdot \ldots \cdot q_r \Rightarrow \mu(m \cdot n) = (-1)^{s+t} = (-1)^s \cdot (-1)^t = \mu(m) \cdot \mu(n)$.
2. $\delta(1) = \sum_{d|1} \mu(d) = \mu(1) = 1$. Так как μ — мультипликативна, то и δ — мультипликативная функция (мы доказали теорему 2.7.2.4 на стр. 32), поэтому для $n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots p_s^{k_s}$, где $p_1,\ p_2,\ \ldots,\ p_s$ — различные простые числа, имеем:
$$\delta(n) = \prod_{i=1}^{s} \delta(p_i^{k_i}),$$
найдем
$$\delta(p^k) = \sum_{d|p^k} \mu(d) = \mu(1) + \mu(p) + \mu(p^2) + \ldots + \mu(p^k) = 1 + (-1) + 0 + \ldots + 0 = 0 - \forall k > 0,$$
следовательно $\delta(n) = 0$, если $n > 1$.
3. ($\Rightarrow$) Имеем:
$$\sum_{d|n} \mu\left(\frac{n}{d}\right) \cdot g(d) =_{\text{(понятно)}} \sum_{d|n} \mu(d) \cdot g\left(\frac{n}{d}\right) =_{\text{(условие)}} \sum_{d|n} \left[\mu(d) \cdot \left(\sum_{c|(n/d)} f(c)\right)\right] = \sum_{c|n} \left[\sum_{d|(n/c)} \mu(d) \cdot f(c)\right] =$$
$$= \sum_{c|n} \left[f(c) \cdot \left(\sum_{d|(n/c)} \mu(d)\right)\right] =_{\text{(пункт 2.)}} \sum_{c|n} \left(f(c) \cdot \delta\left(\frac{n}{c}\right)\right) = f(n).$$

($\Leftarrow$)
$$\sum_{d|n} f(d) = \sum_{d|n} f\left(\frac{n}{d}\right) =_{\text{(условие)}} \sum_{d|n} \left[\sum_{c|(n/d)} \mu\left(\frac{n}{c \cdot d}\right) \cdot g(c)\right] = \sum_{c|n} \left[\sum_{d|(n/c)} \mu\left(\frac{n}{c \cdot d}\right) \cdot g(c)\right] =$$
$$= \sum_{c|n} \left[g(c) \cdot \left(\sum_{d|(n/c)} \mu\left(\frac{n}{c \cdot d}\right)\right)\right] =_{\text{(Пункт 2.)}} \sum_{c|n} g(c) \cdot \delta\left(\frac{n}{c}\right) = g(n).$$

□

ОПР 2.7.4 (Функции Эйлера)**.**

$\varphi(n)$ — количество натуральных чисел не превосходящих n и взаимно простых с n, называется φ-функцией Эйлера*:* $\varphi(n) = \{m \in \mathbb{N} \,|\, m \leqslant n,\ (n,\ m) = 1\}$.

Теорема 2.7.5 (Свойства функции Эйлера)**.**

1. $\sum\limits_{d|n} \varphi(d) = n$ — *формула Гаусса*;
2. φ — мультипликативная функция (т.е. $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$);
3. $\varphi\left(\prod\limits_{i=1}^{s} p_i^{k_i}\right) = \prod\limits_{i=1}^{s}\left(p_i^{k_i} - p_i^{k_i-1}\right) = \left(\prod\limits_{i=1}^{s} p_i^{k_i}\right) \cdot \left(\prod\limits_{i=1}^{s} 1 - \frac{1}{p_i}\right)$.

▷ **Доказательство**.

1. Пусть $A = \{1,\ 2,\ \ldots,\ n\}$, d делит n и $A_d = \{x \in A \,|\, \text{НОД}(x,\ n) = d\} = \{x = d \cdot k \,|\, k \in A,\ k \nmid m,\ k < \frac{n}{d}\}$ тогда $A = \bigcup_{d|n} A_d$ и $A_{d_1} \cap A_{d_2} = \varnothing$, если $d_1 \neq d_2$ (то есть это разбиение A); тогда

$$n = \|A\| = \sum_{d|n} \|A_d\| = \sum_{d|n} \varphi\left(\frac{n}{d}\right),$$

где $(x, n) = d \Leftrightarrow \left(\frac{x}{d}, \frac{n}{d}\right) = 1$, $1 \leqslant \frac{x}{d} \leqslant \frac{n}{d}$; отсюда $\sum\limits_{d|n} \varphi\left(\frac{n}{d}\right) = \sum_{d|n} \varphi(d) = n$.

2. Имеем: $\sum\limits_{d|n} \varphi(d) = n = e(n)$, тогда по формуле обращения Мёбиуса мы можем утверждать, что

$$\varphi(n) = \sum_{d|n} \mu(d) \cdot e\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \cdot \frac{n}{d};$$

но если m и n — взаимнопростые, то

$$\varphi(m \cdot n) = \sum_{d|m\cdot n} \left(\mu(d) \cdot \frac{m \cdot n}{d}\right) = \sum_{\substack{d_1|m \\ d_2|n}} \mu(d_1 \cdot d_2) \cdot \frac{m}{d_1} \cdot \frac{n}{d_2} =_{((d_1,\, d_2) = 1)} \sum_{\substack{d_1|m \\ d_2|n}} \mu(d_1) \cdot \mu(d_2) \cdot \frac{m}{d_1} \cdot \frac{n}{d_2} =$$

$$= \sum_{d_1|m} \left(\mu(d_1) \cdot \frac{m}{d_1}\right) \cdot \sum_{d_2|n} \left(\mu(d_2) \cdot \frac{n}{d_2}\right) = \varphi(m) \cdot \varphi(n).$$

3. Если $n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_s^{k_s}$, где $p_1, p_2, \ldots, p_s$ — различные простые числа, то ввиду пункта 2: $\varphi(n) = \prod_{i=1}^{s} \varphi(p_i^{k_i})$, осталось посчитать, чему равна $\varphi(p_i^{k_i})$: если p — простое, то не взаимопросты с p^k следующие числа от 1 до p^k: $p,\ 2 \cdot p,\ \ldots,\ p^{k-1} \cdot p$ и их p^{k-1} штук, значит $\varphi(p^k) = p^k - p^{k-1} = p^k \cdot (1 - \frac{1}{p})$.

□

Теорема 2.7.6 (Теорема Дирихле)**.**

▷ Вероятность, с которой 2 произвольно взятых числа a и b — взаимопросты равна $\frac{6}{\pi^2} \approx 0,6$.

▷ **Доказательство**.

◦ Доказательство будет эвристическое (т.е. неполное, так как слишком сложное): предположим, что эта вероятность равна p, $0 \leqslant p \leqslant 1$, пусть $d \in \mathbb{N}$ и $A_d = \{(x,\ y) \in \mathbb{N}^2 \,|\, \text{НОД}(x,\ y) = d\}$, тогда $\mathbb{N}^2 = \bigcup_{d\geqslant 1} A_d$ — это разбиение; так как $\text{НОД}(x,\ y) = d \Leftrightarrow \text{НОД}(\frac{x}{d},\ \frac{y}{d}) = 1$, то вероятность попадания в A_d равна $\frac{p}{d^2}$ (числа стали в d раз более редкие), отсюда $1 = \sum\limits_{d=1}^{\infty} \frac{p}{d^2} \Rightarrow p = \frac{1}{\sum\limits_{d=1}^{\infty} \frac{1}{d^2}} = \frac{1}{\pi^2/6} = \frac{6}{\pi^2}$.

□

2.8 Структура кольца вычетов.

ОПР 2.8.1 (Прямой суммы).
Пусть $R_1, R_2, \ldots, R_s$ *— кольца, тогда их* прямой суммой *называется кольцо:*

$$R_1 \oplus R_2 \oplus \ldots \oplus R_s = \{(r_1, r_2, \ldots, r_s) \big| r_i \in R_i\}$$

с операциями сложения и умножения покомпонентно: $(r_1, r_2, \ldots, r_s) + (r'_1, r'_2, \ldots, r'_s) = (r_1 + r'_1, r_2 + r'_2, \ldots, r_s + r'_s)$, $(r_1, r_2, \ldots, r_s) \cdot (r'_1, r'_2, \ldots, r'_s) = (r_1 \cdot r'_1, r_2 \cdot r'_2, \ldots, r_s \cdot r'_s)$.
Очевидно, что кольцо с нулем $(0, 0, \ldots, 0)$ *и единицей* $(1, 1, \ldots, 1)$, *если* $1 \in R_i - \forall i$.

Теорема 2.8.2 (Китайская теорема о достатках).

▷ Пусть
$m \in \mathbb{N}$ и $m = m_1 \cdot m_2 \cdot \ldots \cdot m_s$, где НОД$(m_i,\ m_j) = 1$, если $i \neq j$.

▷ Тогда
Утверждается: $\mathbb{Z}_m \simeq \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \ldots \oplus \mathbb{Z}_{m_s}$.

▷ **Доказательство**.

◦ Установим изоморфизм φ по правилу: если я беру $x(\mathrm{mod}\, m)$, так вот ему нужно сопоставить

$$(x(\mathrm{mod}\, m_1),\ x(\mathrm{mod}\, m_2),\ \ldots,\ x(\mathrm{mod}\, m_s)):$$

Взаимнооднозначность:

$$x \equiv x'(\mathrm{mod}\, m_i) - \forall i \Leftrightarrow m_i | (x - x') - \forall i \Leftrightarrow_{\text{(числа взаимопросты)}} \prod_{i=1}^{s} m_i = m | (x - x') \Leftrightarrow$$
$$\Leftrightarrow_{(m_i \text{ — попарно взаимопросты})} x \equiv x'(\mathrm{mod}\, m).$$

Сравним количество элементов: $\|\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \ldots \oplus \mathbb{Z}_{m_s}\| = \prod_{i=1}^{s} m_i = m = \|\mathbb{Z}_m\| \Rightarrow \varphi$ — взаимнооднозначное отображение $\mathbb{Z}_n$ на $\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \ldots \oplus \mathbb{Z}_{m_s}$.
Изоморфность: следует из свойств: $x + y(\mathrm{mod}\, m) = x(\mathrm{mod}\, m) + y(\mathrm{mod}\, m)$, $x \cdot y(\mathrm{mod}\, m) = x(\mathrm{mod}\, m) \cdot y(\mathrm{mod}\, m)$.

□

Замечание 2.8.2.1 (Поиск x).

▷ Покажем прямо как найти $x \big|\ x(\mathrm{mod}\, m_i) = r_i$, где $r_1, r_2, \ldots, r_s$ — заранее заданный набор целых чисел:

◦ Нас интересует $x \big|\ x \equiv r_i(\mathrm{mod}\, m_i)$, $i = 1, 2, \ldots, s$, решаем: пусть $m = m_1 \cdot m_2 \cdot \ldots \cdot m_s$, $n_i = \frac{m}{m_i}$, тогда (n_i, m_i) — взаимопросты, значит существуют u_i и v_i — целые такие, что (★) $m_i \cdot u_i + n_i \cdot v_i = 1$.

◦ Положим $x_0 = \sum_{i=1}^{s} r_i \cdot n_i \cdot v_i$, тогда $x_0 \equiv r_i(\mathrm{mod}\, m_i) - \forall i$, так как $n_i \cdot v_i \equiv 1(\mathrm{mod}\, m_i)$ — из (★) , а $n_j \equiv 0(\mathrm{mod}\, m_i)$, $j \neq i$; тогда $r_j \cdot n_j \cdot v_j \equiv 0(\mathrm{mod}\, m_i)$, $x_0 \equiv r_i(\mathrm{mod}\, m_i)$. Если x — еще одно решение этой системы сравнений, то $x \equiv r_i(\mathrm{mod}\, m_i) - \forall i \Rightarrow x - x_0 \equiv 0(\mathrm{mod}\, m_i) - \forall i$, другими словами $m_i | (x - x_0) - \forall i \Rightarrow$ так как m_i взаимопросты, $m | (x - x_0) \Rightarrow x - x_0 = m \cdot t \Rightarrow x = x_0 + m \cdot t$.

Следствие 2.8.2.1 (Другое разложение).

▷ Если $m = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_s^{k_s}$, p_i — различные простые, то $\mathbb{Z}_m \simeq \mathbb{Z}_{p_1^{k_1}} \oplus \mathbb{Z}_{p_2^{k_2}} \oplus \ldots \oplus \mathbb{Z}_{p_s^{k_s}}$ — прямая сумма колец.

▷ **Доказательство**.

◦ Лектору доказывать нечего, а нам — некогда.

□

Пример 2.8.2.2 (Как эта простенькая теоремка используется).

▷ Как представить в 32-разрядной двоичной арифметике числа большие $\sim 10^{40}$? Имеем: НОД$(2^k-1,\ 2^\ell-1) = 2^{\text{НОД}(k,\ \ell)}-1$, действительно:

- Пусть $d = \text{НОД}(k,\ \ell)$, так как $d|k$ и $d|\ell$, то $(2^d-1)|(2^k-1)$ и $(2^\ell-1)$ (так как $a^m-1 = (a-1)\cdot(a^{m-1}+\ldots+a+1)$; если $k = d\cdot q$, то $2^k-1 = (2^d)^q-1 = (2^d-1)\cdot((2^d)^{q-1}+(2^d)^{q-2}+\ldots+2^d+1)$).
- Но почему этот делитель наибольший? Пусть $n|(2^k-1)$ и $n|(2^\ell-1)$, надо доказать, что он делит 2^d-1: $2^k \equiv 1(\mathrm{mod}\, n)$, $2^\ell \equiv 1(\mathrm{mod}\, n)$, но существуют $u,\ v \in \mathbb{Z} \mid d = k\cdot u+\ell\cdot v$, тогда $2^d = 2^{k\cdot u+\ell\cdot v} = (2^k)^u\cdot\cdot(2^\ell)^v \equiv 1(\mathrm{mod}\, n) \Rightarrow n|(2^d-1)$.
- Получили необходимое, отсюда следует, что так как 32, 31, 29, 27, 25 — попарно взаимопросты, то взаимопросты числа $2^{32}-1$, $2^{31}-1$, $2^{29}-1$, $2^{27}-1$, $2^{25}-1$, следовательно $\mathbb{Z}_{(2^{32}-1)\cdot\ldots\cdot(2^{25}-1)} \simeq \mathbb{Z}_{2^{32}-1}\oplus\ldots\oplus Z_{2^{25}-1}$, причем они представимы в бинарной 32-разрядной арифметике. Но $(2^{32}-1)\cdot\ldots\cdot(2^{25}-1) = 2^{32+\ldots+25}-\ldots+\ldots = 2^{144}-\ldots+\ldots \geqslant 2^{144}-2^{143} = 2^{143} \sim 10^{43}$.

2.9 Структура мультипликативной группы кольца вычетов

2.9.1 Обозначение

▷ Если R — ассоциативное кольцо с единицей, то обозначим R^* — группу всех обратимых элементов из R.

Теорема 2.9.2 (Разложение R^*)**.**

▷ Если $m = m_1\cdot m_2\cdot\ldots\cdot m_s$, где m_i — попарно взаимнопростые натуральные числа, то $\mathbb{Z}_m^* \simeq \mathbb{Z}_{m_1}^*\times\mathbb{Z}_{m_2}^*\times\ldots\times\mathbb{Z}_{m_s}^*$.

▷ **Доказательство**.

- Если $R \simeq R_1\oplus R_2\oplus\ldots\oplus R_s$, то понятно $R^* = R_1^*\times R_2^*\times\ldots\times R_s^*$ (из определения 1.10.1 на стр. 19).

□

Следствие 2.9.2.1 (Для разложения на простые множетели).

▷ Если $m = p_1^{k_1}\cdot p_2^{k_2}\cdot\ldots\cdot p_s^{k_s}$, то $\mathbb{Z}_m^* = \mathbb{Z}_{p_1^{k_1}}^*\times\mathbb{Z}_{p_2^{k_2}}^*\times\ldots\times\mathbb{Z}_{p_s^{k_s}}^*$ (из следствия 2.8.2.1 на стр. 35).

Теорема 2.9.3 (Подгруппа K^* — циклическая группа)**.**

▷ Пусть K — поле, $G \preccurlyeq K^*$, $|G| < \infty$, тогда G — циклическая группа.

▷ **Доказательство**.

- Наша группа G — абелева и ещё конечная, а конечная абелева группа изоморфна прямому произведению циклических примарных групп; предположим, что в этом разложении есть множители порядка q^k и q^ℓ, где q — простое, $1 \leqslant \ell \leqslant k$; тогда уравнение $x^{q^k} = 1$ имеет в группе G решения, число которых $\geqslant q^k\cdot q^\ell > q^k$. Но в поле многочлен $x^n = 1$ имеет не более чем n корней — противоречие, показывает, что не может быть в примарных множителях двух с одним и тем же $q \Rightarrow$ в различных группах G участвуют примарные циклические множители по разным простым q, тогда G — циклическая группа.
- Если $\text{НОД}(p,\ q) = 1 \Rightarrow \mathbb{Z}_p\times\mathbb{Z}_q \simeq \mathbb{Z}_{pq}$ (было такое 1.10.2.1 на стр. 19).

□

Теорема 2.9.4 (Группа простого числа)**.**

▷ Если p — простое число, то мультипликативная группа кольца вычетов $\mathbb{Z}_p^*$ — циклическая группа.

▷ **Доказательство**.

- Используя конечность $\mathbb{Z}_p^*$ и то, что $\mathbb{Z}_p$ — поле, оно следует из 2.9.3.

□

Замечание 2.9.4.1 (Циклические группы).

▷ Можно показать, что мультипликативные группы по примарному модулю: $\mathbb{Z}^*_{p^k}$ — циклические, при $p \geqslant 3$ — простом и $k \in \mathbb{N}$ — любом (сложные вычисления, я их приводить не буду).

▷ Группы $\mathbb{Z}_2, \mathbb{Z}_4$ — являются циклическими, а дальше уже нет, но $\mathbb{Z}^*_{2^k} \simeq \mathbb{Z}_2 \times \mathbb{Z}_{2^{k-2}}$, при $k \geqslant 3$.

ОПР 2.9.5 (Дискретного логарифма)**.**

Если $G =< g >$ — конечная циклическая группа с порождающим элементом g, то $\forall x \in G\colon \exists! k(x) \big| x = g^{k(x)}$, считаем $0 \leqslant k(x) < \operatorname{ord}(g)$ — порядок элемента $< \infty$. Тогда число $k(x)$ называется дискретным логарифмом (индексом) *числа x по основанию g и обозначается $\operatorname{Log}_g x = \operatorname{ind}_g(x)$.*

Отображение $x \mapsto \operatorname{Log}_g(x)$ умножение элементов переводит в сложение по модулю $\operatorname{ord} g$, это хорошо! Отображение $x \mapsto g^k = x$ — легко вычислимо, обратное отображение плохо вычислимо (это применяется в криптографии).

2.10 Некоторые нелинейные диофантовые уравнения

2.10.1 Кольцо целых Гауссовых чисел

ОПР 2.10.1.1 (Нормы)**.**

Пусть R — целостное кольцо, то есть R — ассоциативное, коммутативное кольцо с единицей и без делителей нуля; отображение $N\colon R \setminus \{0\} \to \mathbb{Z}_+$ называется нормой*, если*

1. *$N(a \cdot b) \geqslant N(a)$ и равенство достигается, когда $b \in R^*$, то есть b — обратный в R;*
2. *$\forall a \in R\colon \forall b \in R \setminus \{0\}\colon \exists q, r \in R \big| a = b \cdot q + r$, при этом $r = 0$ или $N(r) < N(b)$.*

ОПР 2.10.1.2 (Евклидового кольца)**.**

Кольцо R, снабженное нормой N, называется евклидовым кольцом *(в том смысле, что можно использовать алгоритм Евклида).*

Пример 2.10.1.3 (Норм)**.**

▷ $R = \mathbb{Z}$ — ассоциативное, коммутативное кольцо с единицей, тогда $N(x) = |x|$;

▷ $R = K[x]$, где K — поле, тогда $N(f(x)) := \text{ст.} f(x)$.

Теорема 2.10.1.4 (Подмножество комплексных чисел)**.**

▷ Пусть

$\Gamma := \{a + b \cdot i \big| a, b \in \mathbb{Z}\} \subset \mathbb{C}$.

▷ Тогда

Γ — евклидово кольцо относительно нормы $N(a + b \cdot i) = a^2 + b^2$, ещё можно записать так: $N(\alpha) = \alpha \cdot \bar{\alpha} = |\alpha|^2$.

▷ **Доказательство**.

- Γ — ассоциативное, коммутативное кольцо с единицей и без делителей нуля, замкнуто относительно сложения и умножения комплексных чисел (все свойства, легко проверить, выполняются).
- Норма — отображение, проверим свойства нормы:
  - ✓ $N(\alpha \cdot \beta) = |\alpha \cdot \beta|^2 = |\alpha|^2 \cdot |\beta|^2 = N(\alpha) \cdot N(\beta)$, более того ясно, что $\geqslant N(\alpha)$, при $\beta \neq 0$. Равенство будет $\Leftrightarrow N(\beta) = 1 \Leftrightarrow_{(\beta = c + d \cdot i)} c^2 + d^2 = 1$; $c, d \in \mathbb{Z}$, тогда пара $(c, d) = [(\pm 1, 0)$ или $(0, \pm 1)$, то есть другими словами $c + d \cdot i = 1, -1, i, -i$; в частности $\Leftrightarrow c + d \cdot i \in \Gamma^*$, почему? Элементы $\pm 1, \pm i$ — обратимы в кольце Γ:
    а). Ясно $\pm 1, \pm i \in \Gamma^*$;
    б). Предположим $c + d \cdot i \in \Gamma^*$, тогда существует обратный элемент $(a, b) \big| (a + b \cdot i) \cdot (c + d \cdot i) = 1$, где $a, b, c, d \in \mathbb{Z}$, тогда $1 = N(1) = N(\alpha \cdot \beta) = \underbrace{N(\alpha)}_{\in \mathbb{Z}_+} \cdot \underbrace{N(\beta)}_{\in \mathbb{Z}_+} \Rightarrow N(\alpha) = N(\beta) = 1$.
  - ✓ Проверим второе свойство нормы: пусть $\alpha, \beta \in \Gamma$, $\beta \neq 0$, тогда существует число $\frac{\alpha}{\beta} \in \mathbb{C}$. Существует $q \in \Gamma$ — ближайшая точка такая, что $\left|\frac{\alpha}{\beta} - q\right| \leqslant \frac{1}{\sqrt{2}}$. Обозначим $r = \alpha - \beta \cdot q$, тогда $N(r) = |\alpha - \beta \cdot q|^2 = |\beta|^2 \cdot \left|\frac{\alpha}{\beta} - q\right|^2 \leqslant \frac{1}{2} \cdot |\beta|^2 < |\beta|^2 = N(\beta)$.

□

Следствие 2.10.1.5 (Свойства подмножества комплексных чисел).

▷ В кольце Г справедливы все свойства евклидового кольца, то есть существует алгоритм Евклида для нахождения НОД, разрешимы линейные диофантовые уравнения, разложение на неразложимые множители единственно.

2.10.2 Теорема и уравнение Эйлера

ОПР 2.10.2.1 (Уравнения Эйлера).
$x^2 + y^2 = n$; $x, y \in \mathbb{Z}$, $n \in \mathbb{N}$ *когда такое уравнение разрешимо в целых числах?*

Теорема 2.10.2.2 (Эйлера).

▷ Уравнение $x^2+y^2 = n$, $n \in N$ разрешимо в кольце $\mathbb{Z} \Leftrightarrow$ простые делители n вида $(4\cdot k+3)$ входят в каноническое разложение n с четными показателями.

▷ Пример

$x^2 + y^2 = 6 = 2 \cdot 3$, но $3 = 4 \cdot 0 + 3$ — показатель нечётный $\Rightarrow$ уравнение неразрешимо, то есть на окружности радиусом $\sqrt{6}$ нет точек с целыми координатами.

▷ **Доказательство**.

- Рассмотрим для $n = p$ — простое:
  - ✓ Если $p = 2$, то $x^2 + y^2 = 2 \Rightarrow x = \pm 1$, $y = \pm 1 \Rightarrow$ разрешимо.
  - ✓ Если $p \geqslant 3$, то:

    ($\Rightarrow$) $p = 4k+1$ (так как если взять $4k+3$, то степень будет нечётной и условие теоремы не выполнится): пусть $x, y \in \mathbb{Z} \,\big|\, x^2 + y^2 = p$, можно считать, что $0 < x$, $y < \sqrt{p}$, тогда $x^2 \equiv -y^2 (\mathrm{mod}\, p)$, $y \not\equiv 0 (\mathrm{mod}\, p)$ и ещё нам известно, что $\mathbb{Z}_p$ — поле; $\exists z \,\big|\, y \cdot z \equiv 1 (\mathrm{mod}\, p)$, тогда $(x \cdot z)^2 \equiv -1 (\mathrm{mod}\, p)$, отметим, что $-1 \not\equiv 1 (\mathrm{mod}\, p)$ $(p \geqslant 3)$, порядок $\mathrm{ord}\,(x \cdot z) = 4$. Но порядок элемента делит порядок группы (теорема), то есть другими словами $4 \mid |\mathbb{Z}_p^*| = p - 1$, $p - 1 = 4k \Rightarrow p = 4k + 1$.

    ($\Leftarrow$) Пусть $p = 4k + 1$ — простое число, покажем, что уравнение $x^2 + y^2 = p$ разрешимо в $\mathbb{Z}$. Так как $4 \mid |\mathbb{Z}_p^*|$, так как $|\mathbb{Z}_p^*| = p - 1$ и $\mathbb{Z}_p^*$ — циклическая группа (Следствие 1.6.6 на стр. 13), то есть $\mathbb{Z}_p^* =< g >$, $\mathrm{ord}\, g = p - 1 = 4 \cdot k$, рассмотрим $(g^{2\cdot k})^2 = g^{4\cdot k} = 1$, с другой стороны $g^{2\cdot k} \neq 1 \Rightarrow$ $\Rightarrow g^{2\cdot k} = -1$. Таким образом $\exists c \in \mathbb{Z} \,\big|\, c^2 \equiv -1 (\mathrm{mod}\, p)$, другими словами $p \mid (c^2 + 1) = (c + i) \cdot (c - i)$. Если p и $(c - i)$ — взаимнопросты, то p и $(c + i)$ также будут взаимнопросты, так как отображение $a + b \cdot i \mapsto a - b \cdot i$ — автоморфизм Г, теперь по свойствам евклидовых колец p и $(c - i) \cdot (c + i)$ — взаимнопросты, но $p \mid (c - i) \cdot (c + i) = c^2 + 1$ — невозможно, следовательно $d = \text{НОД}(p,\ c - i) \notin \Gamma^*$. Имеем: $p = d \cdot d'$; $d, d' \in \Gamma$; $d' \notin \Gamma^*$, отсюда $p^2 = N(p) = N(d \cdot d') = N(d) \cdot N(d') = (x^2 + y^2) \cdot$ $\cdot (u^2+v^2)$, $x^2+y^2 = N(d) > 1$, так как d необратимый элемент $(\notin \Gamma^*)$; аналогично $u^2+v^2 = N(d') > 1$, так как $d' \notin \Gamma^*$. Следовательно, ввиду единственности разложения на простые множители целых чисел: $p = x^2 + y^2 = u^2 + v^2 \Rightarrow$ уравнение разрешимо в целых числах.
- Рассмотрим для n — составного:

  ($\Rightarrow$) Пусть $x^2 + y^2 = n$; $x, y \in \mathbb{Z}$, $d = \text{НОД}(x,\ y)$, тогда очевидно $d^2 \mid n \Rightarrow \left(\frac{x}{d}\right)^2 + \left(\frac{y}{d}\right)^2 = \frac{n}{d^2} = m$, можем считать, что $x_0 = \frac{x}{d}$, $y_0 = \frac{y}{d}$ — взаимнопростые $\Rightarrow$ либо $x_0^2 + y_0^2 = m$, либо $\text{НОД}(x,\ y) = 1$ — упрощаем. Если $p \mid m$, то $x^2 \equiv -y^2 (\mathrm{mod}\, p)$; $x, y \in \mathbb{Z}$; если $p \mid y$, то $p \mid x$ и они не взаимнопросты, что противоречит взаимной простоте x и y, следовательно $p \nmid y \Rightarrow \exists z \in \mathbb{Z} \,\big|\, z^2 \equiv -1 (\mathrm{mod}\, p)$, тогда (мы доказали) $p = 4\cdot k+1$.

  ($\Leftarrow$) Уравнение $x^2 + y^2 = p$ разрешимо в $\mathbb{Z}$ при $p = 4 \cdot k + 1$, уравнение $x^2 + y^2 = q^2$ разрешимо в $\mathbb{Z}$, при $q = 4 \cdot k + 3$; осталось заметить, что если

$$\begin{cases} a^2 + b^2 = m, \\ c^2 + d^2 = n. \end{cases} \Rightarrow (ac - bd)^2 + (ad + bc)^2 = mn = N\Big((a + b \cdot i) \cdot (c + d \cdot i)\Big).$$

□

2.11 Уравнение Пелля

ОПР 2.11.1 (Уравнения)**.**
Это уравнение, имеющие вид $x^2 - D \cdot y^2 = 1$.

Теорема 2.11.2 (Условие бесконечного числа решений)**.**

▷ Пусть

D — натуральное число, большее 1 и свободное от квадратов (означает, что если $p|D \Rightarrow p^2 \nmid D$).

▷ Тогда

Уравнение Пелля $x^2 - D \cdot y^2 = 1$ — имеет бесконечно много целочисленных решений, причём всякое решение имеет вид $(\pm x_k, \pm y_k)$, где $x_k + y_k \cdot \sqrt{D} = (a + b \cdot \sqrt{D})^k,\ k \in \mathbb{Z},\ a, b \in \mathbb{N}$. Пара (a, b) — тоже образует решение, так называемое *фундаментальное*.

▷ Замечание

Заметим, что это уравнение всегда имеет тривиальное решение $x = 1$, $y = 0$.

▷ **Доказательство**.

∘ Структура группы на множестве решений: пусть K — поле чисел $\{a + b \cdot \sqrt{D} \mid a, b \in \mathbb{Z}\}$ (рассматриваем такие комбинации, так как уравнение разлагается на $(x + y \cdot \sqrt{D}) \cdot (x - y \cdot \sqrt{D}) = 1$); тогда $K \subset \mathbb{R}$ — очевидно; K — замкнуто относительно сложения, умножения, вычитания и обращения не нулевых элементов, а представление в форме $a + b \cdot \sqrt{D}$; $a, b \in \mathbb{Z}$ — единственное.

✓ Если их сложить или вычесть, ясно, что будет число того же вида, так же и умножение, вот разделить уже сложнее; $a + b \cdot \sqrt{D} = 0 \Leftrightarrow a = b = 0$, (очевидно, при условии $a, b \in \mathbb{Z}$), отсюда вытекает единственность. $(a + b \cdot \sqrt{D}) \cdot (x + y \cdot \sqrt{D}) = (ax + by \cdot D) + (ay + bx) \cdot \sqrt{D} =_{\text{(предполагаем)}} 1 \Leftrightarrow$

$$\Leftrightarrow \begin{cases} ax + by \cdot D = 1, \\ bx + ay = 0. \end{cases} \quad \Leftrightarrow_{\text{(через формулы Крамера)}} \begin{cases} x = \frac{a}{a^2 - D \cdot b^2}, \\ y = \frac{-b}{a^2 - D \cdot b^2}. \end{cases},$$

отметим, что $a^2 - D \cdot b^2 \neq 0$, иначе $\sqrt{D}$ — рационально; поэтому есть обратное число. Следовательно мы можем утверждать, что K — поле; так как лежит в $\mathbb{R}$ и выполнены коммутативность, ассоциативность и т.д.

✓ K — является векторным пространством размерности k над $\mathbb{Q}$ с базисом $1, \sqrt{D}$. Если $x = a + b \cdot \sqrt{D} \in K$, то сопоставим α — оператор умножения на α, то есть $A\colon x \to \alpha \cdot x,\ x \in K$; вычислим его базис: его матрица $\mathtt{A}$ в базисе $\vec{e}_1 = 1$, $\vec{e}_2 = \sqrt{D}$ имеет вид:

$$\begin{cases} \mathtt{A} \cdot 1 = a + b \cdot \sqrt{D}, \\ \mathtt{A} \cdot \sqrt{D} = b \cdot D + a \cdot \sqrt{D}. \end{cases} \Rightarrow \mathtt{A_e} = \begin{pmatrix} a & b \cdot D \\ b & a \end{pmatrix}$$

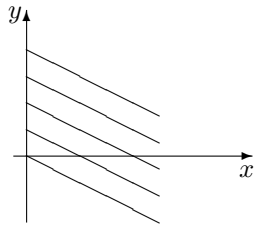
✓ В соответствии получим число

$$a + b \cdot \sqrt{D} \leftrightarrow \begin{pmatrix} a & b \cdot D \\ b & a \end{pmatrix}$$

— является изоморфизмом между полем K и алгеброй матриц указанного вида (другими словами, если взять операторы $\mathtt{A}(\alpha)$ и $\mathtt{A}(\beta)$, то $(\mathtt{A}(\alpha) + \mathtt{A}(\beta))\colon x \to (\alpha + \beta) \cdot x = \alpha \cdot x + \beta \cdot x = \mathtt{A}(\alpha) \cdot x + \mathtt{A}(\beta) \cdot x$ — сумма матриц; $\mathtt{A}(\alpha) \cdot \mathtt{A}(\beta) \cdot x = \alpha \cdot (\beta \cdot x) = (\alpha \cdot \beta) \cdot x = \mathtt{A}(\alpha \cdot \beta)$, а взаимноднозначность сразу очевидна).

✓ Сопоставим матрице $\mathtt{A}(\alpha)$ её определитель: $\det \mathtt{A}(\alpha) = a^2 - D \cdot b^2$ и назовём его нормой числа α, обозначим $N(\alpha)$, тогда важное свойство: норма мультипликативна, т.е. $N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta)$, ещё если $a, b \in \mathbb{Z}$, то $N(\alpha) \in \mathbb{Z}$. Множество целочисленных решений (a, b) уравнения Пелля $x^2 - D \cdot y^2 = 1$ — отвечают множеству матриц указанного вида $\begin{pmatrix} a & D \cdot b \\ b & a \end{pmatrix}$ с определителем равным 1. Множество таких матриц — замкнуто относительно умножения и обращения в группе (следует и мультипликативность нормы: если определитель равен 1, то и произведение 1; для обратного — если определитель равен 1, то все остальные — целочисленные), следовательно множество чисел вида $a + b \cdot \sqrt{D}$ таких, что $a^2 - D \cdot b^2 = 1$ и $a, b \in \mathbb{Z}$ — обратимая тоже группа относительно умножения чисел.

◦ Предположим существование нетривиального решения (т.е. $\neq \pm 1$) уравнения Пелля, докажем, что эта группа имеет вид $\mathbb{Z}_2 \times \mathbb{Z}$, здесь $\mathbb{Z}_2 = \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$ — в матрицах, а в числах $\mathbb{Z}_2 = \{\pm 1\}$, то есть отвечает за изменение знака. Найдём порождающий элемент для бесконечной циклической группы $\mathbb{Z}$ (напомню: это гипербола $y = \sqrt{D} \cdot x$ и $x^2 - D \cdot y^2 = 1$, фактически хотим на ней найти целочисленное решение). Выберем среди всех нетривиальных решений с положительной абсциссой такое решение $(a,\, b)$, что число $\alpha = a + b \cdot \sqrt{D}$, считаем $a,\, b \in \mathbb{N}$, что число является наименьшим среди всех решений (чисел такого вида).



Решения в углу, там конечное число точек $a + \sqrt{D} \cdot b$, понятно найдётся наименьшее.

Пусть число $(x,\, y) \in \mathbb{N}^2$ — снова решение и $\beta = x + y \cdot \sqrt{D}$, тогда $\beta \geqslant \alpha$ (так как это снова нетривиальное решение), если $\beta = \alpha$, то так как представление чисел однозначно, $x = a$, $y = b$; если $\beta > \alpha$, то существует натуральное $k \Big|\ \alpha^k \leqslant \beta < \alpha^{k+1}$, умножим на α^{-k}, тогда $1 \leqslant \alpha^{-k} \cdot \beta < \alpha$, важно то, что число $\alpha^{-k} \cdot \beta$ тоже соответствует решению уравнения Пелля, но оно $< \alpha$ — противоречие выбору α, если его координаты являются натуральными числами, следовательно $\alpha^{-k} \cdot \beta = 1 \Rightarrow \beta = \alpha^k$, а это означает, что $x + y \cdot \sqrt{D} = (a + b \cdot \sqrt{D})^k$ — так как указано в теореме; другими словами мы показали, что эта группа — циклическая.

◦ Поймём, что у β коэффициент натуральный, на самом деле они могут быть и другими: вторая координата может быть меньше 0, но тогда если взять матрицу $\begin{pmatrix} a & D \cdot b \\ b & a \end{pmatrix}$ и обратить, это $\begin{pmatrix} a & -b \cdot D \\ -b & a \end{pmatrix}$, то число попадает ниже оси x-ов на гиперболе, это отвечает числу $\frac{1}{\alpha} < 1$, поэтому...

✓ Меняем минимизацию: требуем только, чтобы $a > 0$, так как у нас конечное число простых решений на рисунке до $(0,\, 0)$, иначе x уже будет отрицательным. Тогда получается противоречие и числа оказываются вида $(\pm 1) \cdot < \alpha >$, то есть $\{\pm \alpha^k \big|\ k \in \mathbb{Z}\}$.

◦ Докажем, что есть нетривиальное решение уравнения Пелля, используя подходящие дроби. Пусть $\frac{P_k}{Q_k}$ — k-ая подходящая дробь к иррациональному числу $\sqrt{D}$, по свойствам наилучшего приближения:

$$\left| \frac{P_k}{Q_k} - \sqrt{D} \right| < \frac{1}{Q_k^2}$$

(более сильная оценка приводилась), следовательно существует бесконечно много несократимых дробей $\frac{x}{y} \Big|\ \left| \frac{x}{y} - \sqrt{D} \right| < \frac{1}{y^2}$, можем считать $x,\, y > 0$, таким образом $\left| x - y \cdot \sqrt{D} \right| < \frac{1}{y}$. Оценим:

$$\left| x + y \cdot \sqrt{D} \right| = \left| x - y \cdot \sqrt{D} + 2y \cdot \sqrt{D} \right| \leqslant \left| x - y \cdot \sqrt{D} \right| + 2y \cdot \sqrt{D} < \frac{1}{y} + 2y \cdot \sqrt{D},$$

теперь делаем оценку:

$$\left| x^2 - D \cdot y^2 \right| = \left| (x - D \cdot y) \cdot (x + D \cdot y) \right| < \frac{1}{y} \cdot \left(\frac{1}{y} + 2y \cdot \sqrt{D} \right) = \frac{1}{y^2} + 2 \cdot \sqrt{D} \leqslant_{(\text{но } y \in \mathbb{N})} 1 + 2 \cdot \sqrt{D}.$$

Поэтому существует бесконечно много несократимых дробей $\frac{x}{y} \Big|\ x^2 - D \cdot y^2 = m$, где $m \in \mathbb{N}$, так как если $x,\, y \in \mathbb{Z}$, то это число будет целое; вообще говоря, результат может быть разным в $\mathbb{Z}$ числом, но они зажаты, следовательно на одной из гипербол их лежит бесконечно много, причём x координаты — различны. Следовательно будем рассматривать пары $(x,\, y)$ по модулю m, тогда найдётся бесконечно много пар $(x,\, y) \Big|\ x,\, y \in \mathbb{N}$, НОД$(x,\ y) = 1$ и $x \mod m = k$, $y \mod m = \ell - \forall x,\, y$, то есть найдётся такой класс.

✓ Пусть $(x_1,\, y_1)$ и $(x_2,\, y_2)$ — такие пары, пусть $\alpha = x_1 + y_1 \cdot \sqrt{D}$, $\beta = x_2 - y_2 \cdot \sqrt{D}$, тогда $\alpha \cdot \beta = (x_1 x_2 - D \cdot y_1 y_2) + (x_2 y_1 - x_1 y_2) \cdot \sqrt{D}$; рассмотрим его координаты:

$$x_1 x_2 - D \cdot y_1 y_2 \equiv_{(\text{ так как } x_2 \equiv x_1 (\mathrm{mod}\, m),\ y_2 \equiv y_1 (\mathrm{mod}\, m)\ )} x_1^2 - D \cdot y_1^2 = m,$$

значит $x_1 x_2 - D \cdot y_1 y_2$ делится на m. Рассмотрим $(x_2 y_1 - x_1 y_2) \equiv x_1 y_1 - x_1 y_1 \equiv 0 (\mathrm{mod}\, m)$, следовательно $\alpha \cdot \beta = m \cdot (a + b \cdot \sqrt{D})$, $a,\, b \in \mathbb{Z}$; возьмём $N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta) = (x_1^2 - D \cdot y_1^2) \cdot (x_2^2 - D \cdot y_2^2) = m^2 =_{(\text{с другой стороны})} N(m) \cdot N(a + b \cdot \sqrt{D}) = m^2 \cdot N(a + b \cdot \sqrt{D})$, $N(a + b \cdot \sqrt{D}) = 1 \Rightarrow a^2 - b^2 \cdot D = 1$.

✓ Мы получили решение, но вдруг оно тривиальное? Покажем, что $b \neq 0$: от противного, если $b = 0$, то норма равна $a^2 \Rightarrow a = \pm 1 \Rightarrow \alpha \cdot \beta = \pm m$; умножим его на $\bar{\beta}$: $\alpha\beta \cdot \bar{\beta} = \pm m \cdot \bar{\beta}$, $\bar{\beta} = x_2 + \sqrt{D} \cdot y_2 \Rightarrow \alpha \cdot$ $\cdot\, m = \pm m \cdot \bar{\beta} \Rightarrow \alpha = \pm\bar{\beta} \Rightarrow x_1 + \sqrt{D} \cdot y_1 = \pm x_2 \pm \sqrt{D} \cdot y_2 \Rightarrow x_1 = \pm x_2$, но мы брали x — натуральным $\Rightarrow x_1 = x_2$ — противоречит выбору множества решений с разными x координатами $\Rightarrow b \neq 0$ и решение не тривиально.

□

Замечание 2.11.2.1 (Как искать).

▷ Лежандр показал, что фундаментальное решение (a, b) получается как $a = P_s$, $b = Q_s$, где P_s/Q_s — первая подходящая дробь к числу $\sqrt{D}$ с условием $P_s^2 - D \cdot Q_s^2 = 1$. На самом деле он доказал больше оценок.

Это применяется для взлома криптографии хорошо.

2.12 Конечные поля и многочлены

2.12.1 Гомоморфизмы колец, идеалы и фактор кольца

ОПР 2.12.1.1 (Гомоморфизма колец)**.**

Пусть R и R' — кольца, отображение $\varphi\colon R \to R'$ — называется гомоморфизмом колец*, если*

1. $\varphi(x + y) = \varphi(x) + \varphi(y)$;
2. $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y) - \forall x,\, y \in R$.

Тогда $\varphi(0) = \varphi(0 + 0) = \varphi(0) + \varphi(0) \Rightarrow \varphi(0) = 0$; $0 = \varphi(0) = \varphi(x + (-x)) = \varphi(x) + \varphi(-x) \Rightarrow \varphi(-x) = -\varphi(x)$.

Множества $\operatorname{Im}\varphi = \{\varphi(x) \mid x \in R\}$ *и* $\ker\varphi = \{x \in R \mid \varphi(x) = 0\}$ *называются соответственно образом и ядром гомоморфизма φ. Легко проверить, что* $\operatorname{Im}\varphi$ *— подкольцо, то есть оно замкнуто относительно операций сложения, умножения и взятия противоположного элемента: со сложением и разностью очевидно:* $-\varphi(x) = \varphi(-x) \in \operatorname{Im}\varphi$; $\varphi(x) + \varphi(y) = \varphi(x + y) \in \operatorname{Im}\varphi$; $\varphi(x) \cdot \varphi(y) = \varphi(x \cdot y) \in \operatorname{Im}\varphi$.

ОПР 2.12.1.2 (Идеала)**.**

Подмножество I кольца R называется идеалом R*, если выполнено:*

1. *Если* $x,\, y \in I \Rightarrow x - y \in I$;
2. *Если* $x \in I$, $a \in R \Rightarrow ax$ *и* $xa \in I$;
3. $0 \in I$.

Обозначим за $I \lhd R$ *— идеал.*

УПР 2.12.1.3 (Идеал — подкольцо)**.**

▷ Проверить, что идеал I — подкольцо.

Пример 2.12.1.4 (Идеалов)**.**

▷ $\ker\varphi \lhd R$;

▷ $< m >= \{m \cdot k \mid k \in \mathbb{Z}\} \lhd \mathbb{Z}$ (действительно: если два числа кратны, то и их сумма кратна и так далее);

▷ $< P(x) >:= \{p(x) \cdot h(x) \mid h(x) \in K(x)\} \lhd K(x)$, если K — поле (если два многочлена кратны p, то и их произведение кратно p);

▷ $< p_1,\, p_2,\, \ldots,\, p_s >= \{p_1h_1 + p_2h_2 + \ldots + p_sh_s \mid h_i \in R\} \lhd R$ (разность тоже комбинация $h_1,\, h_2,\, \ldots,\, h_s$), если R — коммутативное кольцо.

Теорема 2.12.1.5 (Отношение эквивалентности)**.**

▷ Пусть

I — идеал кольца R.

▷ Тогда

Отношение сравнимости по модулю I: $a \equiv b(\mathrm{mod}\, I) \Leftrightarrow a - b \in I$ — является отношением эквивалентности на кольце R и даже конгруэнцией R (то есть отношение эквивалентности согласно с алгебраическими операциями). Фактор-множество $R/I := R/\equiv (\mathrm{mod}\, I)$ — является кольцом относительно индуцированных операций. Если R — ассоциативное, коммутативное и с единицей, то и R/I такое же. Если отображение $\varphi\colon a \to [a] := \{x \in R \mid x \equiv a(\mathrm{mod}\, I)\}$ — является гомоморфизмом из R в R/I, причём $\ker\varphi = I$. Если $\varphi\colon R \to R'$ — произвольный гомоморфизм, то $R/\ker\varphi \simeq \mathrm{Im}\,\varphi$.

▷ **Доказательство**.

- $\equiv (\mathrm{mod}\, I)$ — эквивалентность:

  Рефлексивность: $a \equiv a(\mathrm{mod}\, I) \Leftrightarrow a - a = 0 \in I \Rightarrow$ сравнимы;

  Симметричность: $a \equiv b(\mathrm{mod}\, I) \Rightarrow b \equiv a(\mathrm{mod}\, I)\colon a - b \in I \Rightarrow b - a = -(a-b) \in I$;

  Транзитивность: $a \equiv b,\ b \equiv c \Rightarrow a \equiv c(\mathrm{mod}\, I);\ a,\ b \in I,\ b - c \in I \Rightarrow a - c = (a-b) + (b-c) \in I$.
- $\equiv (\mathrm{mod}\, I)\colon$ конгруэнция

$$\begin{cases} a \equiv a'(\mathrm{mod}\, I), \\ b \equiv b'(\mathrm{mod}\, I). \end{cases} \Rightarrow \begin{cases} a + b \equiv a' + b'(\mathrm{mod}\, I), \\ ab \equiv a'b'(\mathrm{mod}\, I). \end{cases}, \text{ так как}$$

$$\begin{cases} a - a' \in I, \\ b - b' \in I. \end{cases} \Rightarrow \begin{cases} (a+b) - (a'+b') = (a-a') + (b-b') \in I, \\ ab - a'b' = ab - a'b + a'b - a'b' = (a-a')\cdot b + (b-b')\cdot a' \in I. \end{cases}$$

- Класс эквивалентности $[a] = \{x \in R \mid x - a \in I\} = \{x \in R \mid x - a = c \in I\} = \{a + c \mid c \in I\} := a + I$ — сдвиг идеала.
- Проверка аксиомы кольца для R/I: C_1 — ассоциативность сложения, C_2 — коммутативность сложения, C_4 — дистрибутивность, Y_1 — ассоциативность умножения, Y_2 — коммутативность умножения — имеют характер тождеств и потому верны в R/I; C_3 — существование нуля: $0 = [0] = 0 + I = I$, действительно: $(a+I) + (0+I) = a + I$; C_4 — противоположный элемент: противоположный к элементу $a+I$ — это $(-a)+I$; Y_3 — существование единицы: если 1 — единица кольца R, то класс $1 + I$ и будет единицей для R/I.
- Гомоморфизм φ и его ядро: $\varphi\colon a \to [a] = a + I$ понятно, это гомоморфизм, так как $\varphi(a+b) = (a+b) + I = (a+I) + (b+I) = \varphi(a) + \varphi(b)$, проверять нечего: $\varphi(a \cdot b) = ab + I = (a+I)\cdot(b+I) = \varphi(a)\cdot\varphi(b)$.

  Проверим ядро: $\varphi(a) = a + I = 0 + I \Rightarrow a - 0 = a \in I$, другими словами $\ker\varphi = I$.
- Произвольный гомоморфизм: пусть $\varphi\colon R \to R'$ — произвольный гомоморфизм, для краткости обозначим $I = \ker\varphi$, установим соответствие между R/I и $\mathrm{Im}\,\varphi$ по правилу: $a + I \to \varphi(a)$ — взаимнооднозначно. Это соответствие взаимнооднозначно, так как $a + I = b + I \Leftrightarrow a - b \in I = \ker\varphi \Leftrightarrow \varphi(a-b) = 0 \Leftrightarrow \varphi(a) = \varphi(b) \Rightarrow$ классы совпадают, когда их образы совпадают $\Rightarrow$ взаимнооднозначно.

  Оно сохраняет свойства операций, то есть сумма переходит в сумму, умножение в умножение: $(a+I) + (b+I) \leftrightarrow \varphi(a) + \varphi(b)$ — вот и всё; $(a+I)\cdot(b+I) \leftrightarrow \varphi(a)\cdot\varphi(b)$.

□

Пример 2.12.1.6 (Что можно получить, используя эту конструкцию)**.**

▷ Пусть $R = \mathbb{R}[x]$, $R' = \mathbb{C}$, $\varphi\colon f(x) \to f(i)$ — гомоморфизм из $\mathbb{R}[x]$ в $\mathbb{C}$. Найдём $\mathrm{Im}\,\varphi =_{\text{(утверждается)}} \mathbb{C}\colon a + bx \xrightarrow{\varphi} a + bi \Rightarrow$ образ совпадает со всем полем; найдём $\ker\varphi = \{f(x) \mid f(i) = 0\}$, по теореме Безу: $(x - i) \mid f(x)$, тогда $(x + i) \mid f(x)$ (так как если какое-то комплексное число будет решением, то и сопряжённое тоже, а f — имеет вещественный коэффициент).

По свойствам взаимнопростых многочленов: $x^2+1 = (x-i)\cdot(x+i)$ делит $f(x)$, другими словами идеал $< x^2+1 >= \{(x^2+1)\cdot h(x) \mid h(x) \in \mathbb{R}[x]\} \supset \ker\varphi$. Обратное включение — очевидно, следовательно $\ker\varphi =< x^2+1 >$.

Заключение: по теореме оказалось, что $\mathbb{C} = \mathrm{Im}\,\varphi \simeq R/\ker\varphi = \mathbb{R}[x]/ < x^2+1 >$, возникает вопрос: а нельзя ли так составить другие поля?

Теорема 2.12.1.7 (О существовании корня (Кронекера))**.**

▷ Пусть

K — произвольное поле, $p(x)$ — многочлен, причём $p(x)$ — неразложим в $K[x]$ на многочлены меньших степеней.

▷ Тогда

Существует поле L такое, что:

а). $L \supset K$ как подполе;

б). $L \ni \alpha \big| p(\alpha) = 0$ — корень;

в). L — наименьший среди своих подполей со свойствами а) и б).

Свойствами а), б) и в) поле L определяется однозначно с точностью до изоморфизма.

▷ **Доказательство**.

∘ Единственность L: пусть $\varphi\colon K[x] \to L$ по правилу $\varphi\colon f(x) \to f(\alpha)$, тогда φ — гомоморфизм (очевидно); найдём его ядро и образ:

✓ $\ker\varphi = \{f(x) \in K[x] \big| f(\alpha) = 0\}$, то есть $(x-\alpha) \mid f(x)$, с другой стороны $(x-\alpha) \mid p(x)$, так как α — корень p, значит $(x-\alpha) \mid d(x) = \text{НОД}(f(x),\ p(x)) \in K[x]$; по алгоритму Евклида получаем, что $d(x) \mid p(x)$ и ст. $d(x) \geqslant 1$. Ввиду неразложимости $p(x) = \Sigma \cdot d(x)$, где $\Sigma \in K$, $\Sigma \neq 0$ (так как если он раскладывается, то один из множителей — обратный элемент кольца).
С другой стороны $f(x) = d(x) \cdot h(x) = \Sigma^{-1} \cdot p(x) \cdot h(x)$, $p(x) \mid f(x)$, мы видим, что $f(x) \in\!< p(x) >$, другими словами $\ker\varphi \subseteq\!< p(x) >$. Обратное включение — опять очевидно: если мы возьмём многочлен $\Sigma^{-1} \cdot p(x) \cdot h(x)$, то $p(\alpha) = 0$. Следовательно $\ker\varphi =\!< p(x) >$.

✓ Исследуем образ: из теоремы 2.12.1.5 $\operatorname{Im}\varphi \simeq K[x]/\ker\varphi = K[x]/\!< p(x) >$, утверждается, что это поле: $K[x]/\!< p(x) >$. $K[x]$ — ассоциативное, коммутативное кольцо с единицей $\Rightarrow$ фактор кольцо такое же (по теореме). Осталось проверить последнюю аксиому Y_4 — обратимость элемента: если $f +\!< p(x) >\neq 0 +\!< p(x) >$, то существует обратный: имеем, что $f \notin\!< p >$ — не кратен, разность $(f-0)$ не входит в $< p(x) >$, другими словами f и p — взаимнопросты (ввиду неразложимости $p(x)$). Поэтому существуют u и $v \in K[x]$ такие, что $fu + pv = 1$ — разрешение линейного диафантового уравнения в кольце многочленов, тогда утверждается, что если $I =\!< p(x) >$, то $(f+I)\cdot(u+I) = fu+I = (1-pu)+I = 1+I$ (так как разность представителей сокращается в многочлены делящиеся на p: $fu = 1 (\operatorname{mod} I)$); другими словами $(f+I)^{-1} = u+I$.
Таким образом $K[x]/I$ — поле, а с другой стороны $\simeq \operatorname{Im}\varphi$ — поле, $\operatorname{Im}\varphi \subseteq L$, заметим, что $\operatorname{Im}\varphi \supseteq K$, α, так как $\varphi\colon f(x) \to f(\alpha) \Rightarrow c + 0\cdot x + 0\cdot x^2 \to c + \ldots \in K \Rightarrow K$ там лежит; с другой стороны: $x \xrightarrow{\varphi} \alpha \Rightarrow$ $\Rightarrow$ α лежит. Таким образом это подполе, содержащее K и α, а по свойству φ: $\operatorname{Im}\varphi = L$; в итоге $L \simeq K[x]/\!< p(x) >$, это и говорит, что оно единственно с точностью до изоморфизма.

∘ Существование: возьмём в качестве $L := K[x]/\!< p(x) >$, уже доказали, что L — поле, осталось проверить, что оно удовлетворяет свойствам а), б) и в): $K \hookrightarrow L$ — вложено; $c \in K$, сопоставим $c \leftrightarrow c + I$, где $I =\!< p(x) >$; $c + I = c' + I \Leftrightarrow c - c' \in I \Leftrightarrow p(x) \mid (c - c')$, где $p(x)$ — неразложимый многочлен степени $\geqslant 1$:

а). $(c - c')$ степени $0 \Leftrightarrow c - c' = 0 \Leftrightarrow c = c' \Rightarrow$ взаимнооднозначное. Ввиду свойств фактор кольца: множество $K' = \{c \in L \big| c \in K\}$ — образует подполе в поле L, изоморфное полю K (по правилам сложения, умножение видно, что в точности соответствует). Но мы не разлагаем изоморфные поля, поэтому считаем, что изоморфное поле K там лежит.

б). Пусть $p(x) = C_0 + C_1 x + \ldots + C_n x^n$, $C_i \in K$, положим $\alpha = x + I$, тогда проверим, что $p(\alpha) = (C_0 + I) + (C_1 + I)\cdot(x + I) + \ldots + (C_n + I)\cdot(x + I)^n = p(x) + I = 0 + I = 0$.

в). Если $f(x) \in K[x]$, то $f = ph + r$, где ст. $r <$ ст. p, тогда наш смежный класс $f + I = (ph + r) + I = r + I$, $r(\alpha) = a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}$, где a_i — коэффициенты, $r(x)$ как раз показывает, что если $L' \subseteq L$ — подполе, кроме того $L' \supset K$, α, то $L' \supset a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}$; $a_i \in K$, то есть $L' = L$.

□

Следствие 2.12.1.8 (Размерность поля из теоремы).

▷ Пусть L — из теоремы является векторным пространством над K с базисом 1, α, α^2, …, α^{n-1}, где $n =$ ст. $p(x)$, в частности мы видим: $\dim_K L = n$; если K — конечное поле порядка q, то $|L| = q^n$.

▷ **Доказательство**.

∘ Если $a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} = b_0 + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1}$, где $a_i, b_i \in K$, то $\sum_{i=1}^{n-1}(a_i - b_i)\cdot\alpha^i = 0$, это означает, что если $f(x) = \sum_{i=1}^{n-1}(a_i - b_i)\cdot x^i$, то мы получаем, что $f(\alpha) = 0$, а ст. $f <$ ст. $p(x)$; ввиду неразложимости: $p(x) \mid f(x)$, то есть $f(x) \equiv 0$ (так как степень меньшая) $\Rightarrow a_i - b_i = 0 - \forall i \Rightarrow$ представление однозначно.

□

Пример 2.12.1.9.

▷ Пусть $K = \mathbb{Z}_2 = \{0, 1\} = x^2 + x + 1$, тогда $p(x)$ — неразложим в $K[x]$ (если раскладывается, то на один многочлен степени 1 и имеет корень): $p[0] = 1 \neq 0$; $p[1] = 1 \neq 0 \Rightarrow p(x)$ — не имеет корней в поле $K = \{0, 1\}$. Тогда $\mathbb{Z}_2[x]/ < x^2 + x + 1 >$ по теореме — поле порядка $2^2 = 4$. Посмотрим таблицу сложения и умножения поля $L = K[x]/ < p(x) >$, $\alpha := x + < p(x) > \Rightarrow \alpha^2 + \alpha + 1 = 0$:

$+$	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

$\cdot$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

$(x + I) \cdot (x + I) = x^2 + I$, а $x^2 = (x^2 + x + 1) + (x + 1)$ — делится с остатком $(x + 1) \Rightarrow x^2 + I = (x + 1) + I$. $< \alpha >= \{\alpha, \alpha^2, \alpha^3, \ldots\} = \{\alpha, \alpha + 1, 1\}$ — цикл группы порядка 3.

2.12.2 Поле разложения

Теорема 2.12.2.1 (Поле разложения многочлена)**.**

▷ Пусть

K — поле, $f(x)$ — многочлен степени $\geqslant 1$.

▷ Тогда

Существует единственное, с точностью до изоморфизма, поле F такое, что:

а). $F \supset K$ как подполе;

б). $F \supset$ все корни многочлена $f(x)$;

в). F — минимально (наименьшее среди своих подполей).

Поле F называется *полем разложения многочлена* $f(x)$ на линейные множители.

▷ **Доказательство**.

∘ Единственность: пусть $p(x) \mid f(x)$ в $K[x]$ и $p(x)$ — неразложим (такой обязательно есть), по теореме Кронекера 2.12.1.7: $\exists \alpha \in F \big| p(\alpha) = 0$, $\exists!$ поле L такое, что:

а). $L \supset K$,

б). $L \ni \alpha \big| p(\alpha) = 0$,

в). L — минимально.

Более того, $F \supset L \supset K$, тогда F будет полем разложения для многочлена $f(x)/(x - \alpha)$ над L. Индукция по $n =$ ст. f показывает, что F — единственно (взяли f какой-то, его неразложимый делитель — корень в F, тогда делим, таким образом L — единственна, а дальше по степени и однозначности строится F). Шаг индукции: $n = 1$ — всегда: $F = K$ — верно; а дальше — что было перед.

∘ Существование F: пусть $p(x) \mid f(x)$ в $K[x]$, $p(x)$ — неразложимый и по теореме Кронекера строится поле L такое, что

а). $L \supset K$,

б). $L \ni \alpha \big| p(\alpha) = 0$,

в). L — минимальный.

Многочлен $f(x)/(x-\alpha)$ разложим на неразложимые множители в $L[x]$; если они имеют степень 1, то $L = F$; если нет, то снова присоединяем поле неразложимого многочлена, делящего частное $f(x)/(x - \alpha)$ и так далее (фактически та же индукция). И оно самое малое, конечно.

□

2.12.3 Порядок, единственность, существование конечных полей

Теорема 2.12.3.1 (Порядок конечного поля)**.**

▷ Всякое конечное поле имеет порядок p^n, при подходящем простом p и натуральном n; с другой стороны: $\forall$ простого p и натурального n — поле порядка p^n существует и только одно с точностью до изоморфизма.

▷ **Доказательство**.

∘ Порядок: пусть F — конечное поле, тогда $F \supset 0,\ 1;\ 1 \neq 0$ — аксиома; рассмотрим отображение $\varphi\colon \mathbb{Z} \to F$ такое, что

$$\varphi(n) = \begin{cases} \overbrace{1+1+\ldots+1}^{n} \in F, & n > 0; \\ 0, & n = 0; \\ -\overbrace{1-1-\ldots-1}^{n}, & n < 0. \end{cases},$$

тогда легко проверить, что φ — гомоморфизм колец: $\varphi(n+m) = \varphi(n)+\varphi(m)$, $\varphi(m\cdot n) = \varphi(m)\cdot\varphi(n) - \forall m,\ n \in \mathbb{Z}$ — непосредственно и определяется к свойствам поля. Ясно, что $\operatorname{Im}\varphi \subseteq F$ — конечен: $|\operatorname{Im}\varphi| < \infty \Rightarrow$ $\Rightarrow \ker\varphi \neq 0$. Если p — наименьшее натуральное, $p \in \ker\varphi$ и $p = k \cdot \ell$ — составное, где $1 < k,\ \ell < p$, то $0 = \varphi(p) = \overbrace{\varphi(k)}^{\neq 0} \cdot \overbrace{\varphi(\ell)}^{\neq 0}$ (так как p — наименьшее) $\Rightarrow$ в поле есть делитель 0, но поле не содержит $\Rightarrow$ число p — не составное. Поэтому легко проверить, что $\ker\varphi =< p >= \{p \cdot k \mid k \in \mathbb{Z}\}$.

Если $\varphi(n) = 0$ и $n = ph + r$, $0 \leqslant r < p$, то $0 = \varphi(n) = \varphi(p)\cdot\varphi(h) + \varphi(r) = \varphi(r)$, так как $\varphi(p) = 0 \Rightarrow$ нашлось меньшее число, но p — наименьшее натуральное $\Rightarrow r = 0$ и тогда $p \mid n$, в итоге $\operatorname{Im}\varphi \simeq \mathbb{Z}/\ker\varphi = \mathbb{Z}/ < p > \subseteq$ $\subseteq \mathbb{Z}_p$ — поле вычетов. Обозначим через $K = \operatorname{Im}\varphi$, тогда K — подполе поля F и порядок: $|K| = p$, где p — простое (наименьшее подполе, содержит f, порождено 0 и 1). Так как $K \preccurlyeq F$, можно рассмотреть как векторное пространство над K. Ввиду конечности F, оно имеет конечный базис $e_1,\ e_2,\ \ldots,\ e_n$ над полем K, то есть $F = \{\alpha_1 \cdot e_1 + \alpha_2 \cdot e_2 + \ldots + \alpha_n \cdot e_n \mid \alpha_i \in K\}$ — запись единственна. Поэтому

$$|F| = \overbrace{p \cdot p \cdot \ldots \cdot p}^{n} = p^k$$

(рассмотреть возможно по α).

∘ Единственность: пусть p — произвольное простое число, n — натуральное и F — поле порядка p^n, тогда $F^* = (F \setminus \{0\};\ \cdot)$ — конечная мультипликативная подгруппа мультипликативной группы поля порядка $p^n - 1$ (один элемент выкинут). По теореме Лагранжа: если $\alpha \in F^*$, то $\alpha^{p^n-1} = 1$, умножая на α: $\alpha^{p^n} = \alpha$ (выполнено и для 0) — для всех α и F. Таким образом F — поле, разложимого над $\mathbb{Z}_p$ многочлена $x^{p^n} - x$ (любой элемент поля F — корень этого уравнения, но число корней этого многочлена $\leqslant p^n \Rightarrow$ это поле разложимо над $\mathbb{Z}_p$). Но поле разложимого многочлена определяется однозначно с точностью до изоморфизма.

∘ Существование: пусть F — поле разложимого многочлена $x^{p^n} - x$ над полем $\mathbb{Z}_p$, рассмотрим множество $L = \{\alpha \in F \mid \alpha^{p^n} = \alpha\} \subseteq F$ (то есть множеств корней этого многочлена). Утверждается, что L — поле, то есть если $\alpha^{p^n} = \alpha$ и $\beta^{p^n} = \beta \neq 0$, то

$$\begin{cases} (\alpha \pm \beta)^{p^n} = \alpha \pm \beta, \\ (\alpha \cdot \beta)^{p^n} = \alpha \cdot \beta, \\ \left(\frac{\alpha}{\beta}\right)^{p^n} = \frac{\alpha}{\beta}. \end{cases}$$

— замкнуто относительно сложения, умножения и деления корней. Заметим, что в поле характеристики p: $(\alpha+\beta)^p = \sum_{k=0}^{p} \binom{p}{k} \cdot \alpha^{p-k} \cdot (-\beta)^k$, но $\binom{p}{k} = \frac{p\cdot(p-1)\cdot\ldots\cdot(p-k+1)}{1\cdot 2\cdot\ldots\cdot k}$ и $p \mid \binom{p}{k}$, если $0 < k < p$; но $\binom{p}{k}$ — натуральное число, сумма единиц, но так как кратно $p \Rightarrow \binom{p}{n} = 0$ в $F \Rightarrow (\alpha\pm\beta)^p = \alpha^p \pm \beta^p$, так как средние коэффициенты все 0, а крайние вот эти. Возводим и дальше в степень $\Rightarrow (\alpha\pm\beta)^{p^n} = \alpha^{p^n} \pm \beta^{p^n} =_{\text{(по условию)}}$ $\alpha \pm \beta$. Второе соотношение — очевидно и для частного тоже очевидно. Но так как L содержится в поле F, а F — поле разложимого многочлена $x^{p^n} - x$, то есть F — минимально, то $F = L$.

Надо найти порядок, надо понять, сколько корней многочлена: $|F|$ = число корней многочлена $x^{p^n} - x$, докажем, что имеет все корни разные: его производная имеет вид $p^n \cdot x^{p^n-1} - 1 = -1$, поэтому производная и многочлен — взаимопросты (производная равна константе), тогда мы знаем, что кратных корней нет, таким образом число корней равно степени многочлена $= p^n$, следовательно мы установили, что $|F| = p^n$, вот и всё.

□

Замечание 2.12.3.1.1 (Присоединение корня).

▷ Обычно F строим присоединяя к $\mathbb{Z}_p$ один корень неразложимого многочлена над $\mathbb{Z}_p$ степени n. Если один корень присоединить из теоремы Кронекера, будет p^n. А так как все поля одинакового порядка изоморфны, то всё.

Замечание 2.12.3.1.2 (Обозначения).

▷ Поле порядка p^n, где p — простое, обычно обозначают $\mathbb{F}_{p^n}$ или $GF(p^n)$ (поле Галуа).

2.12.4 Число неразложимых многочленов степени n над $\mathbb{Z}_p$

Теорема 2.12.4.1 (Число нормальных неразложимых многочленов)**.**

▷ Число нормальных (со старшим коэффициентом 1) неразложимых многочленов степени n над полем $\mathbb{Z}_p$ равно

$$\frac{1}{n}\cdot\sum_{d|n}\mu\left(\frac{n}{d}\right)\cdot p^d,$$

где μ — функция Мёбиуса.

▷ **Доказательство**.

∘ Пусть P_d — произведение всех нормальных неразложимых над $\mathbb{Z}_p$ многочленов степени d. Утверждается, что $x^{p^n}-x=\prod_{d|n}P_d(x)$, это следует из описания подполей в поле F порядка p^n (вообще-то сейчас мы это не поймём, немножко забежал вперёд, но я после объясню). Отсюда получаем (★) $p^n=\sum_{d|n}d\cdot N_d$, где (используем, что все корни разные кратности 1) $d\cdot N_d=$ ст. P_d, а N_d — число неразложимых нормальных многочленов степени d над $\mathbb{Z}_p$. Применяя к (★) формулу обращения Мёбиуса для функции: пусть $f(d)=d\cdot N_d$ — функция натурального аргумента, тогда получим: $n\cdot N_n=\sum_{d|n}\mu\left(\frac{n}{d}\right)\cdot p^d$ (потому, что мы обращали функцию) и $N_n=\frac{1}{n}\cdot\sum_{d|n}\mu\left(\frac{n}{d}\right)\cdot p^d$.

□

Следствие 2.12.4.2 (Неравенство числа нулю).

▷ $N_n>1-\forall n>1$, действительно, если $N_n=0$, то можно умножить на знаменатель n: $p^n\pm p^{n_1}\pm\ldots\pm p^{n_s}=0$, $n>n_1>n_2>\ldots>n_s>0$, $n_i\mid n$; значения функция Мёбиуса: 1, 0, −1. Разделим на p^{n_s}, получим $p^{k_0}\pm p^{k_1}\pm\ldots\pm 1=0$, $k_0>k_1>\ldots>k_{s-1}>0$, все числа делятся на p, а 1 — нет, что невозможно. Поэтому равенство нулю невозможно, противоречие показывает, что $N_n\geqslant 1$ (для $n=1$ — тривиально).

2.12.5 Подполя конечных полей

Теорема 2.12.5.1 (Подполе поля порядка p^n)**.**

▷ Поле порядка p^n, где p — простое, а n — натуральное, содержит подполе порядка $p^d\Leftrightarrow d\mid n$.

▷ **Доказательство**.

(⇒) Пусть $|F|=p^n$, $L\preccurlyeq F$ и $|L|=p^d$, тогда мы можем утверждать, что $L^*\preccurlyeq F^*$, по теореме Лагранжа: $|L^*|\mid|F^*|$, другими словами $(p^d-1)\mid(p^n-1)$ (нуль выбросили, исчез один элемент). Пусть $n=dh+r$, $0\leqslant\leqslant r<d$, тогда

$$(p^n-1)/(p^d-1)=\frac{(p^d)^h\cdot p^r-p^r+p^r-1}{p^d-1}=p^r\cdot\frac{(p^d)^h-1}{p^d-1}+\frac{p^r-1}{p^d-1}$$

(где $\frac{\alpha^k-1}{\alpha-1}$ — целое, так как это геометрическая прогрессия) $\Rightarrow\frac{p^r-1}{p^d-1}$ — целое, но $p^r-1<p^d-1\Rightarrow p^r-1=0\Leftrightarrow d\mid n$.

(⇐) Пусть $n=dh$, $h\in\mathbb{N}$, пусть L — поле разложения многочлена $x^{p^d}-x$, $|L|=p^d$, докажем, что всякое поле порядка p^n содержит поле порядка p^d, то есть если $\alpha\in L\Rightarrow\alpha^{p^d}=\alpha$, но тогда

$$\alpha^{p^n}=\alpha^{p^{dh}}=\alpha\underbrace{^{p^d\cdot p^d\cdot\ldots\cdot p^d}}_{h}=\left(\left(\ldots\left(\alpha^{p^d}\right)^{p^d}\ldots\right)^{p^d}\right)^{p^d}=\alpha.$$

Это означает, что поле F содержит в поле разложение многочлена $x^{p^n}-x$, $|F|=p^n$.

□

2.12.5.2 Объяснения к

▷ Почему в 2.12.4.1

$$x^{p^n} - x = \prod_{d|n} P_d(x)?\ P_d(x) = p_1(x) \cdot p_2(x) \cdot \ldots \cdot p_N(x),$$

где $p_i(x)$ — неразложимый степени d. Если $p_i(x)$ — неразложимый степени d, то $d \mid n$, так как является полем и в обратную сторону.

Пример 2.12.5.3 (Решётка подполей)**.**

▷ Решётка подполей поля: $F_{2^{12}} \simeq$ решётке натуральных делителей числа 12.

2.13 Квадратичные вычеты, закон взаимности Гаусса

ОПР 2.13.1 (Квадратичного вычета)**.**
Число a называется квадратичным вычетом *по модулю b, если уравнение $x^2 \equiv a (\mathrm{mod}\, b)$ разрешимо, в противном случае a называется* квадратичным невычетом.

Пример 2.13.1.1 (Квадратичного вычета)**.**

▷ $p = 7$, посмотрим $x (\mathrm{mod}\, 7)$ и $x^2 (\mathrm{mod}\, 7)$:

$x (\mathrm{mod}\, 7)$	0	1	2	3	4	5	6
$x^2 (\mathrm{mod}\, 7)$	0	1	4	2	2	4	1

(мы видим, что здесь выявляется некоторая симметрия, так как $x^2 = (-x)^2$).

ПРЕДЛ 2.13.2 (Совпадение числа квадратичных вычетов и невычетов)**.**

▷ Пусть
p — нечётное простое число.

▷ Тогда
Число квадратичных вычетов и квадратичных невычетов совпадает.

▷ **Доказательство**.

- Рассмотрим отображение $\varphi\colon \mathbb{Z}_p^* \to \mathbb{Z}_p^*$ (мультипликативная группа поля, то есть 0 надо выбросить) такое, что $\varphi\colon x \to x^2$, тогда φ — гомоморфизм, действительно: $(x \cdot y)^2 = x^2 \cdot y^2$.
- Рассмотрим его образ и ядро: $x \in \ker\varphi \Leftrightarrow x^2 \equiv 1 (\mathrm{mod}\, p) \Leftrightarrow x \equiv 1$ или $-1 (\mathrm{mod}\, p)$ (так как $(x^2 - 1) = (x-1) \cdot (x+1) = 0$), причём $1 \not\equiv -1 (\mathrm{mod}\, p)$, так как p — нечётное $\Rightarrow$ можем утверждать, что $|\ker\varphi| = 2$, поэтому $|\operatorname{Im}\varphi| \simeq_{\text{(изоморфен)}} |\mathbb{Z}_p^*/\ker\varphi| =_{\text{(фактор группы из смежных классов)}} |\mathbb{Z}_p^* : \ker\varphi| = |\mathbb{Z}_p^*|/|\ker\varphi| = (p-1)/2$. $\operatorname{Im}\varphi$ — это в точности множество квадратичных вычетов.

□

ОПР 2.13.3 (Символа Лежандра)**.**
Пусть a — целое число, p — простое, тогда символ Лежандра a по отношению p определяется так:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{если } a \text{ — квадратичный вычет по модулю } p; \\ -1, & \text{если } a \text{ — квадратичный невычет;} \\ 0, & \text{если } p \mid a. \end{cases}$$

(в первых двух случаях предполагается, что a и p взаимопросты).

Пример 2.13.3.1 (Символа Лежандра)**.**

▷ $\left(\frac{2}{7}\right) = 1$, $\left(\frac{5}{7}\right) = -1$, то есть если он $= -1$, то нет смысла искать решение.

ПРЕДЛ 2.13.4 (Формула Эйлера)**.**

▷ Если p — нечётное простое число и $(a,\, p) = 1$, то

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} (\mathrm{mod}\, p).$$

▷ **Доказательство**.

- Пусть $\psi\colon \mathbb{Z}_p^* \to \mathbb{Z}_p^*$ такое, что $\psi(a) = a^{\frac{p-1}{2}}$, это гомоморфизм, действительно: $(a \cdot b)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}}$. Если в абелевой группе $x = a^{\frac{p-1}{2}}$, то $x^2 = a^{p-1} \equiv 1 (\mathrm{mod}\, p)$ — по малой теореме Ферма (порядок $\mathbb{Z}_p^* = p - 1$, если возвести в степень по модулю p, получится 1), следовательно $x = 1$ или -1. Осталось доказать, что возможно и то и другое.
- Группа $\mathbb{Z}_p^*$ — циклическая, то есть $\mathbb{Z}_p^* =< g >$, порядок её: $|\mathbb{Z}_p^*| = p - 1 \Rightarrow \mathrm{ord}\, g = p - 1$, другими словами $g^{p-1} = 1$, но $g^{\frac{p-1}{2}} \neq 1 \Rightarrow$ он равен -1, поэтому мы можем утверждать, что $\mathrm{Im}\, \psi = \{1, -1\} \Rightarrow$ порядок образа равен двум.
- Теперь нас интересует порядок ядра: $|\ker \psi| = |\mathbb{Z}_p^*| / |\mathrm{Im}\, \psi| = \frac{p-1}{2}$. Пусть C — множество всех квадратных вычетов из $\mathbb{Z}_p^*$, тогда если $a \in C \Rightarrow a = x^2 \Rightarrow a^{\frac{p-1}{2}} = x^{p-1} \Rightarrow x \in \ker \psi \Rightarrow C \subset \ker \psi,\ |C| = \frac{p-1}{2} = |\ker \psi|$, следовательно мы можем заключить, что ядро ψ состоит в точности из квадратичного вычета $\ker \psi = C$. Поэтому $a \in C \Leftrightarrow \left(\frac{a}{p}\right) = 1$, с другой стороны $a \in \ker \psi \Leftrightarrow a^{\frac{p-1}{2}} = 1$, поэтому $a^{\frac{p-1}{2}} = \left(\frac{a}{p}\right)$.

□

Следствие 2.13.5 (Произведение символов Лежандра).

▷ $\left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) = \left(\frac{a \cdot b}{p}\right)$.

▷ **Доказательство**.

- $\left(\frac{a}{p}\right) = \psi(a)$, ψ — гомоморфизм (по теореме Лиувилля), а это, практически, и есть свойство гомоморфизма.

□

Следствие 2.13.6 (Символ Лежандра для (-1)).

▷ $\left(\frac{-1}{p}\right) = 1 \Leftrightarrow p = 4k + 1$, с другой стороны из -1 извлекается квадратный корень $\Leftrightarrow$ когда $= 1$.

▷ **Доказательство**.

- $\left(\frac{-1}{p}\right) =_{\text{(по формуле Эйлера 2.13.4)}} (-1)^{\frac{p-1}{2}} = 1 \Leftrightarrow \frac{p-1}{2}$ — нечётное $\Leftrightarrow p = 4k + 1$.

□

Теорема 2.13.7 (Закон взаимности Гаусса)**.**

▷ Пусть

p и q — различные нечётные простые числа.

▷ Тогда

$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \cdot \left(\frac{q}{p}\right)$.

▷ История

Некоторая теорема, которую Гаусс любил и дал ей несколько доказательств, она позволяет быстро считать символ Лежандра.

▷ **Доказательство**.

∘ Пусть L — поле, полученное из $\mathbb{Z}_p^*$ присоединением корня λ уравнения $x^q-1=0$, то есть $x^q=1$. Рассмотрим сумму Гаусса (которая упала с потолка):

$$\tau = \sum_{a\in\mathbb{Z}_q^*} \left(\frac{a}{q}\right)\cdot\lambda^a,$$

поймём, что τ лежит в поле $\mathbb{Z}_p$, имеем: $L\subset\mathbb{Z}_p$, когда $\tau\in\mathbb{Z}_p$? Ясно, что $\tau\in\mathbb{Z}_p \Leftrightarrow \tau^p=\tau$ (мы используем характеристику конечных полей). Так как $(x\pm y)^p = x^p \pm y^p$ в поле характеристики p (наше поле, так как $1\in\mathbb{Z}_p$ и $\underbrace{1+1+\ldots+1}_{p}=0$), тогда мы можем утверждать, что

$$\tau^p = \sum_{a\in\mathbb{Z}_q^*} \left(\frac{a}{q}\right)\cdot\lambda^{pa}$$

(так как p — нечётное). Сделаем замену $pa=b$, где $pa,\, b\in\mathbb{Z}_q^*$, тогда $a=p'\cdot b$, где p' — обратное к p по модулю q. Тогда

$$\tau^p = \sum_{b\in\mathbb{Z}_q^*}\left(\frac{p'b}{q}\right)\cdot\lambda^b =_{\text{(гомоморфизм)}} \left(\frac{p'}{q}\right)\cdot\sum_{b\in\mathbb{Z}_q^*}\left(\frac{b}{q}\right)\cdot\lambda^b = \left(\frac{p}{q}\right)\cdot\sum_{b\in\mathbb{Z}_q^*}\left(\frac{b}{q}\right)\cdot\lambda^b = \left(\frac{p}{q}\right)\cdot\tau,$$

таким образом $\tau^p = \left(\frac{p}{q}\right)\cdot\tau$ для суммы Гаусса, в частности $\tau^p=\tau \Leftrightarrow \left(\frac{p}{q}\right)=1$, таким образом $\tau\in\mathbb{Z}_p \Leftrightarrow \left(\frac{p}{q}\right)=1$.

∘ Вычислим:

$$\tau^2 = \left(\sum_{a\in\mathbb{Z}_q^*}\left(\frac{a}{q}\right)\cdot\lambda^a\right)\cdot\left(\sum_{b\in\mathbb{Z}_q^*}\left(\frac{b}{q}\right)\cdot\lambda^b\right) = \sum_{a\in\mathbb{Z}_q^*}\sum_{b\in\mathbb{Z}_q^*}\left(\frac{ab}{q}\right)\cdot\lambda^{a+b},$$

сделаем замену переменных $b=ac$, где $a,\, b,\, c\in\mathbb{Z}_q^*$, тогда

$$\left(\frac{ab}{q}\right) = \left(\frac{a^2c}{q}\right) = \left(\frac{a}{q}\right)^2\cdot\left(\frac{c}{q}\right) = \left(\frac{c}{q}\right),$$

но $a+b=a+ac=a\cdot(1+c)$ — по дистрибутивности, отсюда

$$\tau^2 = \sum_{a,\,c\in\mathbb{Z}_q^*}\left(\frac{c}{q}\right)\cdot\lambda^{a\cdot(1+c)} = \sum_{c=-1,\,a\in\mathbb{Z}_q^*}\left(\frac{-1}{q}\right)\cdot\lambda^{a\cdot 0} + \sum_{c\neq-1,\,a\in\mathbb{Z}_q^*}\left(\frac{c}{q}\right)\cdot\lambda^{a\cdot(1+c)} =$$

$$= \left(\frac{-1}{q}\right)\cdot(q-1) + \sum_{c\neq-1,\,c\in\mathbb{Z}_q^*}\left[\left(\frac{c}{q}\right)\cdot\sum_{a\in\mathbb{Z}_p^*}\lambda^{a\cdot(1+c)}\right] = \left(\frac{-1}{q}\right)\cdot(q-1) + \sum_{c\neq-1,\,c\in\mathbb{Z}_q^*}\left(\frac{c}{q}\right)\cdot(-1),$$

так как

$$0 = (\lambda^q-1)/(\lambda-1) = 1+\lambda+\ldots+\lambda^{q-1} = \sum_{a\in\mathbb{Z}_q^*}\lambda^{a\cdot(1+c)} + 1.$$

Поэтому

$$\tau^2 = \left(\frac{-1}{q}\right)\cdot(q-1) + \left(\frac{-1}{q}\right),$$

так как количество квадратичных вычетов и квадратичных невычетов по модулю q одинаково, то есть $\sum\limits_{c\in\mathbb{Z}_q^*}\left(\frac{c}{q}\right)=0$. В итоге $\tau^2 = \left(\frac{-1}{q}\right)\cdot q$, следовательно $\left(\frac{p}{q}\right)=1 \Leftrightarrow \left(\frac{\left(\frac{-1}{q}\right)}{p}\right)=1$, так как $x^2=\left(\frac{-1}{q}\right)\cdot q$ имеет решение $x=\tau$. Итак:

$$\left(\frac{p}{q}\right) = \left(\frac{\left(\frac{-1}{q}\right)}{p}\right) =_{\text{(формула Эйлера)}} \left(\frac{(-1)^{\frac{q-1}{2}}\cdot q}{q}\right) =_{\text{(мультипликативность)}} \left(\frac{-1}{p}\right)^{\frac{q-1}{2}}\cdot\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\cdot\left(\frac{q}{p}\right).$$

□

Теорема 2.13.8 (Символ Лежандра для (2))**.**

▷ Пусть

p — нечётное простое число.

▷ Тогда

$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

▷ **Доказательство**.

∘ Пусть поле L получается из $\mathbb{Z}_p$ присоединением корня λ многочлена $x^4+1=0$, то есть $\lambda^4=-1$ или $\lambda^2=-\lambda^{-2}$. Пусть $\omega=\lambda+\lambda^{-1}$, тогда $\omega^2=\lambda^2+2\cdot\lambda\lambda^{-1}+\lambda^{-2}$, другими словами $\omega=\sqrt{2}$, далее $\omega\in\mathbb{Z}_p \Leftrightarrow \omega^p=\omega \Leftrightarrow \lambda^p+\lambda^{-p}=\lambda+\lambda^{-1}$. Имеем:

$$\lambda^p+\lambda^{-p} =_{(\lambda^8=1)} \begin{cases} \lambda+\lambda^{-1}, & p=8k+1; \\ \lambda^{-1}+\lambda, & p=8k-1; \\ -\lambda^{-1}-\lambda, & p=8k+3; \\ -\lambda-\lambda^{-1}, & p=8k-3. \end{cases}$$

(так как $\lambda^2=-\lambda^{-2} \Rightarrow \lambda^3=-\lambda^{-1}$, $\lambda^{-3}=-\lambda$, здесь мы рассматриваем все случаи (остатки)). Таким образом $\left(\frac{2}{p}\right)=1 \Leftrightarrow \omega\in\mathbb{Z}_p \Leftrightarrow \omega^p=\omega \Leftrightarrow p=8k\pm1 \Leftrightarrow \frac{p^2-1}{8}=8k^2\pm2k \Leftrightarrow (-1)^{\frac{p^2-1}{8}}=1$, а что может быть ещё? Действительно: если $p=8k\pm3$, то $\frac{p^2-1}{8}=8k^2\pm6k+1$ — нечётное.

□

Пример 2.13.9 (Вычисления символа Лежандра)**.**

▷ Вычислим

$$\left(\frac{391}{479}\right)=\left(\frac{17\cdot23}{479}\right)=\left(\frac{23}{479}\right)\cdot\left(\frac{17}{479}\right)=_{(\text{все простые})}\left(\frac{479}{23}\right)\cdot(-1)^{\frac{23-1}{2}\cdot\frac{479-1}{2}}\cdot\left(\frac{479}{17}\right)\cdot(-1)^{\frac{17-1}{2}\cdot\frac{479-1}{2}}=$$
$$=-\left(\frac{19}{23}\right)\cdot\left(\frac{3}{17}\right)=_{(19=4k+1 \text{ и } 23=4k+1, \text{ но } 3\neq4k+1)}\left(\frac{23}{19}\right)\cdot\left(\frac{17}{3}\right)=\left(\frac{4}{19}\right)\cdot\left(\frac{2}{3}\right)=1\cdot(-1)=-1\Rightarrow$$

$\Rightarrow$ неразрешимо уравнение $x^2=399 (\mathrm{mod}\, 479)$.

2.13.10 Символ Якоби

Напомню: если p — простое число и нечётное, а число $a\,|\,0<a<p$, то по формуле Эйлера: $a^{\frac{p-1}{2}}\equiv\left(\frac{1}{p}\right)(\mathrm{mod}\, p)$, это свойство используется, как тест на не простоту (или простоту). Если это условие нарушается, то заведомо p — не простое. Здесь всё считается быстро, но если мы не знаем, простое ли p — это глобальная проблема.

Левую часть равенства легко считать, если представить $(p-1)/2$ в бинарном виде:

$$\frac{p-1}{2}=\sum_{i=0}^{k} n_i\cdot 2^i,\ n_i=0,1;\ \text{понятно } a^{\frac{p-1}{2}}=\prod_{i=0}^{k} a^{2^i\cdot n_i}(\mathrm{mod}\, p).$$

Таким образом всё сводится к последующему возведению в квадрат числа $a(a^2, a^4, \ldots)$ и последующему взятию остатков от деления на p.

Чтобы отсчитать правую часть равенства, необходимо обобщить символ Лежандра на случай непростого основания m. Это — *символ Якоби.*

ОПР 2.13.10.1 (Символа Якоби)**.**

Пусть $m=p_1\cdot p_2\cdot\ldots\cdot p_s$ — нечетное натуральное число, p_i — простые; тогда символ Якоби — *это*

$$\left(\frac{a}{m}\right):=\prod_{i=1}^{s}\left(\frac{a}{p_i}\right)$$

(раньше m было простым).

Заметим, что символ Якоби легко вычисляется без знания разложения m на простые множители, это связано со следующей теоремой 2.13.10.3.

Лемма 2.13.10.2 (Формулы по модулю (2))**.**

▷ Пусть

u и v — нечётные натуральные числа.

▷ Тогда

Утверждается, что:

- $\frac{uv-1}{2} \equiv \frac{u-1}{2} + \frac{v-1}{2} (\mathrm{mod}\, 2)$;
- $\frac{u^2v^2-1}{8} \equiv \frac{u^2-1}{8} + \frac{v^2-1}{8} (\mathrm{mod}\, 2)$.

▷ **Доказательство**.

- Используем как в определении: $m = p_1 \cdot p_2 \cdot \ldots \cdot p_s = u \cdot v$; пусть $u = 2u' + 1$, $v = 2v' + 1$, тогда сосчитаем левую часть:

$$\frac{uv-1}{2} = \frac{4 \cdot u'v' + 2 \cdot (u' + v') + 1 - 1}{2} \equiv u' + v' (\mathrm{mod}\, 2) \equiv \frac{u-1}{2} + \frac{v-1}{2} (\mathrm{mod}\, 2),$$

  вот и всё.
- Пусть $u = 4x + \alpha$, $v = 4y + \beta$; α, $\beta = \pm 1$; тогда $u^2 = 16x^2 + 8 \cdot x\alpha + 1$, $v^2 = 16y^2 + 8 \cdot \beta y + 1$, далее по модулю 16 имеем: $u^2v^2 - 1 \equiv 8 \cdot (\alpha x + \beta y) + 1 - 1 (\mathrm{mod}\, 16) \Rightarrow$ разделим на 8: $(u^2v^2 - 1)/8 = \alpha x + \beta y (\mathrm{mod}\, 2)$.
  Далее сосчитаем правую часть: $(u^2 - 1) \cdot (v^2 - 1) \equiv 8 \cdot (\alpha x + \beta y) (\mathrm{mod}\, 16)$, снова делим на 8 и снова получаем тоже.

□

Теорема 2.13.10.3 (Свойства символа Якоби)**.**

▷ Пусть

a и m — нечётные натуральные числа.

▷ Тогда

Выполнено:

- Закон взаимности:
$$\left(\frac{a}{m}\right) = (-1)^{\frac{m-1}{2} \cdot \frac{a-1}{2}} \cdot \left(\frac{m}{a}\right);$$
- $\left(\frac{-1}{m}\right) = (-1)^{(m-1)/2}$;
- $\left(\frac{2}{m}\right) = (-1)^{(m^2-1)/8}$.

▷ Пример

Подсчёт символа без разложения m:

$$\left(\frac{662}{2005}\right) =_{\text{(мультипликативность выполняется, ясно)}} \left(\frac{2}{2005}\right) \cdot \left(\frac{331}{2005}\right) = (-1)^{(2005^2-1)/8} \cdot \left(\frac{331}{2005}\right) = -\left(\frac{2005}{331}\right) =$$
$$= -\left(\frac{19}{331}\right) = \left(\frac{331}{19}\right) = \left(\frac{8}{19}\right) =_{\text{(мультипликативность)}} \left(\frac{2}{19}\right)^3 = (-1)^3 = -1.$$

▷ **Доказательство**.

- Пусть $m = p_1 \cdot p_2 \cdot \ldots \cdot p_s$, а $a = q_1 \cdot q_2 \cdot \ldots \cdot q_t$, где p_i и q_j — простые; тогда

$$\left(\frac{a}{m}\right) =_{\text{(определение и свойство мультипликативности символа Лежандра)}} \prod_i \left(\prod_j \left(\frac{q_j}{p_i}\right)\right) =_{\text{(закон взаимности Гаусса 2.13.7)}}$$
$$= (-1)^{\sum_i \left(\sum_j \frac{p_i - 1}{2} \cdot \frac{q_j - 1}{2}\right)} \cdot \prod \left(\frac{p_i}{q_j}\right) = (-1)^{\left(\sum_i \frac{p_i - 1}{2}\right) \cdot \left(\sum_j \frac{q_j - 1}{2}\right)} \cdot \left(\frac{m}{a}\right),$$

осталось заметить, что степень (-1) совпадает с начальной, то есть осталось доказать, что

$$\left(\sum_i \frac{p_i-1}{2}\right)\cdot\left(\sum_j \frac{q_j-1}{2}\right) = \frac{m-1}{2}\cdot\frac{a-1}{2} (\mathrm{mod}\, 2),$$

это следует из леммы 2.13.10.2.

- Сосчитаем:

$$\left(\frac{-1}{m}\right) = \prod_{i=1}^{s}\left(\frac{-1}{p_i}\right) =_{\text{(формула Эйлера)}} \prod_{i=1}^{s}(-1)^{(p_i-1)/2} = (-1)^{\sum_{i=1}^{s}(p_i-1)/2} =_{\text{(ввиду леммы, пункт 1.)}} (-1)^{(m-1)/2}.$$

- Имеем:

$$\left(\frac{2}{m}\right) = \prod_{i=1}^{s}\left(\frac{2}{p_i}\right) =_{\text{(закон Гаусса)}} \prod_{i=1}^{s}(-1)^{(p_i^2-1)/8} = (-1)^{\sum_{i=1}^{s}(p_i^2-1)/8} =_{\text{(лемма, пункт 2.)}} (-1)^{(m^2-1)/2}.$$

□