Основные утверждения, содержащиеся в курсе «Алгебраические структуры» (лектор: Е. Е. Горячко)

Лемма о разбиениях на классы смежности.

Пусть G — группа и $H \le G$; тогда множества G/H и $H\backslash G$ — разбиения группы G.

Теорема Лагранжа. *Пусть G — группа, $|G| < \infty$ и $H \le G$; тогда $|H|$ делит $|G|$.*

Лемма о порядке элемента.

Пусть G — группа и $g \in G$; тогда $\operatorname{ord}(g) = |\langle g\rangle|$ и, если $|G| < \infty$, то $\operatorname{ord}(g)$ делит $|G|$.

Теорема об описании циклических групп.

1. Пусть G — группа, и $n \in \mathbb{N}$ и $G \cong (\mathbb{Z}/n)^+$, или $n = \infty$ и $G \cong \mathbb{Z}^+$; тогда группа G циклическая и $|G| = n$.

2. Пусть G — циклическая группа; обозначим через n величину $|G|$; тогда $n \in \mathbb{N}$ и $G \cong (\mathbb{Z}/n)^+$, или $n = \infty$ и $G \cong \mathbb{Z}^+$.

Первая теорема о подгруппах циклической группы.

Пусть G — циклическая группа, $d \in G$ и $G = \langle d\rangle$; обозначим через n величину $|G|$ и

1. пусть $l \in \mathbb{N}$ и, если $n < \infty$, то l делит n; обозначим через H подгруппу $\langle d^l\rangle$ группы G; тогда $\min\{a \in \mathbb{N} \mid d^a \in H\} = l$;

2. пусть $H \le G$ и, если $n = \infty$, то $H \ne \{1\}$; обозначим через l число $\min\{a \in \mathbb{N} \mid d^a \in H\}$; тогда $H = \langle d^l\rangle$ и, если $n < \infty$, то l делит n.

Вторая теорема о подгруппах циклической группы.

Пусть G — циклическая группа и $|G| < \infty$; обозначим через n число $|G|$ и

1. пусть $m \in \mathbb{N}$ и m делит n; обозначим через H подмножество $\{g \in G \mid g^m = 1\}$ группы G; тогда $H \le G$ и $|H| = m$;

2. пусть $H \le G$; обозначим через m число $|H|$; тогда m делит n и $H = \{g \in G \mid g^m = 1\}$.

Теорема о прямом произведении.

Пусть G — группа и $F, H \le G$; тогда следующие свойства эквивалентны:

- *$G = FH$, $F \cap H = \{1\}$ и $\forall f \in F, h \in H$ $(fh = hf)$;*
- *отображение, действующее из $F \times H$ в G по правилу $(f, h) \mapsto fh$ для любых $f \in F$ и $h \in H$, — изоморфизм групп.*

Теорема о разложении конечной циклической группы в прямое произведение.

Пусть $m, n \in \mathbb{N}$; тогда $\mathrm{C}_{mn} \cong \mathrm{C}_m \times \mathrm{C}_n$, если и только если $\gcd(m, n) = 1$.

Теорема об алгоритме Евклида.

Пусть R — евклидова область и $r, s \in R$; тогда

1. алгоритм Евклида находит такой $t \in R$, что $t \overset{|}{\sim} \gcd(r, s)$;

2. расширенный алгоритм Евклида дополнительно находит такие $u, v \in R$, что $t = ur + vs$.

Следствие из теоремы об алгоритме Евклида.

1. Пусть $n \in \mathbb{Z} \setminus \{0\}$; тогда $(\mathbb{Z}/n)^\times = \{a \in \mathbb{Z}/n \mid \gcd(a, n) = 1\}$.

2. Пусть K — поле и $f \in K[x] \setminus \{0\}$; тогда $(K[x]/f)^\times = \{a \in K[x]/f \mid \gcd(a, f) = 1\}$.

Китайская теорема об остатках.

Пусть $t \in \mathbb{N}_0$, $n_1, \ldots, n_t \in \mathbb{N}$ и числа $n_1, \ldots, n_t$ попарно взаимно просты.

Обозначим через n число $n_1 \cdot \ldots \cdot n_t$; тогда отображение, действующее из $\mathbb{Z}/n$ в $\mathbb{Z}/n_1 \times \ldots \times \mathbb{Z}/n_t$ по правилу $a \mapsto (a \bmod n_1, \ldots, a \bmod n_t)$ для любых $a \in \mathbb{Z}/n$, — изоморфизм колец.

Теорема Эйлера. *Пусть $n \in \mathbb{N}$, $a \in \mathbb{Z}$ и $\gcd(a, n) = 1$; тогда $a^{\phi(n)} \equiv 1 \pmod{n}$.*

Теорема о функции Эйлера.

1. Пусть $m, n \in \mathbb{N}$ и $\gcd(m, n) = 1$; тогда $\phi(mn) = \phi(m)\phi(n)$.

2. Пусть $n \in \mathbb{N}$; представим число n в виде $p_1^{\omega_1} \cdot \ldots \cdot p_t^{\omega_t}$, где $t \in \mathbb{N}_0$, $p_1, \ldots, p_t \in \mathbb{P}$, числа $p_1, \ldots, p_t$ попарно различны и $\omega_1, \ldots, \omega_t \in \mathbb{N}$; тогда $\phi(n) = n\big(1 - \frac{1}{p_1}\big) \cdot \ldots \cdot \big(1 - \frac{1}{p_t}\big)$.

Лемма о корнях многочлена.

Пусть R — область целостности и $f \in R[x] \setminus \{0\}$; тогда $|\{r \in R \mid f(r) = 0\}| \le \deg f$.

Теорема о цикличности.

Пусть R — область целостности, $G \le R^\times$ и $|G| < \infty$; тогда группа G циклическая.

Теорема о группах обратимых остатков.

1. Пусть $n \in \mathbb{N}$; представим число n в виде $p_1^{\omega_1} \cdot \ldots \cdot p_t^{\omega_t}$, где $t \in \mathbb{N}_0$, $p_1, \ldots, p_t \in \mathbb{P}$, числа $p_1, \ldots, p_t$ попарно различны и $\omega_1, \ldots, \omega_t \in \mathbb{N}$; тогда $(\mathbb{Z}/n)^\times \cong (\mathbb{Z}/p_1^{\omega_1})^\times \times \ldots \times (\mathbb{Z}/p_t^{\omega_t})^\times$.

2. Пусть $p \in \mathbb{P} \setminus \{2\}$ и $\omega \in \mathbb{N}$, или $p = 2$ и $\omega \in \{1, 2\}$; тогда $(\mathbb{Z}/p^\omega)^\times \cong \mathrm{C}_{p^{\omega-1}(p-1)}$.

3. Пусть $\omega \in \mathbb{N} \setminus \{1, 2\}$; тогда $(\mathbb{Z}/2^\omega)^\times \cong \mathrm{C}_2 \times \mathrm{C}_{2^{\omega-2}}$.

Критерий существования дискретного логарифма.

Пусть $n \in \mathbb{N}$; тогда следующие свойства эквивалентны:

- *существует дискретный логарифм по модулю n (то есть группа $(\mathbb{Z}/n)^\times$ циклическая);*
- *число n нечетное примарное, или число $\frac{n}{2}$ нечетное примарное, или $n \in \{1, 2, 4\}$.*

Теорема о разложении перестановки в произведение транспозиций.

Пусть $n \in \mathbb{N}_0$ и $u \in \mathrm{S}_n$; обозначим через l число $n - \kappa(u)$; тогда

1. существуют такие транспозиции $u_1, \ldots, u_l \in \mathrm{S}_n$, что $u = u_1 \cdot \ldots \cdot u_l$;

2. для любого $t \in \mathbb{N}_0$ из существования таких транспозиций $u_1, \ldots, u_t \in \mathrm{S}_n$, что $u = u_1 \cdot \ldots \cdot u_t$, следует, что $t \geq l$ и $t \equiv l \pmod 2$.

⋆ Теорема о гомоморфизме для структур.

Пусть σ — сигнатура, S, V — σ-структуры и $f \in \mathrm{Hom}(S, V)$; тогда $\mathrm{Im}\, f \leq V$, $\mathrm{Ker}\, f$ — конгруэнция на S, а также $S/\mathrm{Ker}\, f \cong \mathrm{Im}\, f$.

⋆ Теорема о свободных структурах.

Пусть σ — сигнатура, I — множество σ-тождеств, B — множество, $S \in \mathrm{Var}_I$ и $\alpha \in \mathrm{Map}(B, S)$; тогда отображение, действующее из $\mathrm{F}_I(B)$ в S по правилу ((Δ_I)-класс терма t) $\mapsto [t]_S(\alpha)$ для любого терма t над B, определено корректно и является единственным гомоморфизмом σ-структур, действующим из $\mathrm{F}_I(B)$ в S и для любого $b \in B$ отображающим (Δ_I)-класс терма b в $\alpha(b)$.

⋆ Лемма о делимости и главных идеалах.

Пусть R — коммутативное кольцо; тогда

1. для любых $r, s \in R$ выполнено (s делит r) $\Leftrightarrow$ $(r) \subseteq (s)$, $r \overset{|}{\sim} s \Leftrightarrow (r) = (s)$, $r \in sR^\times \Rightarrow r \overset{|}{\sim} s$;

2. для любых $r, s, t \in R$ выполнено $t \overset{|}{\sim} \gcd(r, s) \Leftrightarrow$ (идеал (t) — наименьший главный идеал кольца R, содержащий идеал $(r) + (s)$) и $t \overset{|}{\sim} \mathrm{lcm}(r, s) \Leftrightarrow (t) = (r) \cap (s)$.

⋆ Китайская теорема об остатках для областей главных идеалов.

Пусть R — область главных идеалов, $t \in \mathbb{N}_0$, $r_1, \ldots, r_t \in R$, элементы $r_1, \ldots, r_t$ попарно взаимно просты (то есть $\forall\, i, j \in \{1, \ldots, t\}$ $(i \neq j \Rightarrow \gcd(r_i, r_j) \overset{|}{\sim} 1)$). Обозначим через r элемент $r_1 \cdot \ldots \cdot r_t$; тогда отображение, действующее из $R/(r)$ в $R/(r_1) \times \ldots \times R/(r_t)$ по правилу $s + (r) \mapsto (s + (r_1), \ldots, s + (r_t))$ для любых $s \in R$, определено корректно и является изоморфизмом колец.

⋆ Теорема о главных идеалах.

1. Пусть R — коммутативное кольцо; тогда $\mathrm{Irr}(R) \subseteq \{r \in R \mid$ идеал (r) — максимальный нетривиальный главный идеал кольца $R\}$.

2. Пусть R — область целостности; тогда $\forall\, r, s \in R$ $(r \overset{|}{\sim} s \Leftrightarrow r \in sR^\times)$, $\mathrm{Irr}(R) = \{r \in R \mid$ идеал (r) — максимальный нетривиальный главный идеал кольца $R\}$ и $\mathrm{Prime}(R) \subseteq \mathrm{Irr}(R)$.

3. Пусть R — область главных идеалов; тогда $\mathrm{Prime}(R) = \mathrm{Irr}(R)$.

⋆ Теорема о факториальных областях.

Пусть R — область целостности; тогда R — факториальная область, если и только если любая неубывающая последовательность главных идеалов кольца R стабилизируется и $\mathrm{Prime}(R) = \mathrm{Irr}(R)$.

⋆ Теорема о включениях между классами колец.

1. Евклидовы области являются областями главных идеалов.

2. Области главных идеалов являются факториальными областями.

⋆ Теорема об описании однородных G-множеств. *Пусть G — группа и*

1. пусть C — класс сопряженности подгрупп группы G и $H \in C$, а также X — G-множество и $X \cong G/H$; тогда X — однородное G-множество и $\{\mathrm{St}_G(x) \mid x \in X\} = C$;

2. пусть X — однородное G-множество; обозначим через C множество $\{\mathrm{St}_G(x) \mid x \in X\}$; тогда C — класс сопряженности подгрупп группы G и для любых $H \in C$ выполнено $X \cong G/H$.

⋆ Лемма Бернсайда. *Пусть G — группа, X — G-множество, $|G| < \infty$; тогда $|X/G| = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}_X(g)|$.*

⋆ Теорема о внутренних автоморфизмах.

Пусть G — группа; тогда отображение conj_G, действующее из G в $\mathrm{Aut}(G)$ по правилу $g \mapsto$ (сопряжение слева при помощи элемента g) для любых $g \in G$, определено корректно и является гомоморфизмом групп, $\mathrm{Im}\,\mathrm{conj}_G = \mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$ и $\mathrm{Ker}\,\mathrm{conj}_G = \mathrm{Z}(G)$.

⋆ Теорема о простоте знакопеременных групп. *Группы A_n, где $n \in \mathbb{N} \setminus \{1, 2, 4\}$, просты.*

⋆ Лемма о независимых и порождающих подмножествах.

1. Пусть M — свободный модуль и B — базис модуля M; тогда B — максимальное независимое подмножество в M и минимальное порождающее подмножество в M.

2. Пусть V — векторное пространство, B — максимальное независимое подмножество в V или минимальное порождающее подмножество в V; тогда B — базис пространства V.

⋆ Теорема о бесконечном базисе. *Любые два базиса имеющего бесконечный базис модуля равномощны.*

⋆ Теорема о существовании базиса. *В любом векторном пространстве существует базис.*

⋆ Лемма Штейница о замене.

Пусть V — векторное пространство, C — независимое подмножество в V, D — порождающее подмножество в V и $|C| < \infty$; тогда существует такое подмножество D' в D, что $|C| = |D'|$ (и, значит, $|C| \leq |D|$) и $(D \setminus D') \cup C$ — порождающее подмножество в V.

⋆ Теорема о «поле разлома».

Пусть K — поле, $f \in \mathrm{Irr}(K[x])$, E — расширение поля K, $e \in E$ и $f(e) = 0$; тогда

1. $f = cf_e$, где $c =$ (старший коэффициент многочлена f);

2. отображение $\mathrm{eval}_{f,e}$, действующее из $K[x]/(f)$ в E по правилу $g + (f) \mapsto g(e)$ для любых $g \in K[x]$, определено корректно и является гомоморфизмом расширений поля K;

3. $\mathrm{Im}\,\mathrm{eval}_{f,e} = \{g(e) \mid g \in K[x] \ \wedge\ \deg g < \deg f\} = K(e)$ и $K[x]/(f) \cong K(e)$.

⋆ Следствие из теоремы о «поле разлома».

Пусть K — поле, $f \in K[x] \setminus \{0\}$, E и $\widetilde{E}$ — расширения поля K, $e \in E$, $f(e) = 0$ и f раскладывается в произведение многочленов степени 1 в кольце $\widetilde{E}[x]$; тогда структура расширения поля K на $\widetilde{E}$ продолжается до структуры расширения поля $K(e)$ (то есть $\mathrm{Hom}_K(K(e), \widetilde{E}) \neq \varnothing$).

⋆ Теорема о поле разложения.

Пусть K — поле и $f \in K[x] \setminus \{0\}$; тогда существует расширение поля K, являющееся полем разложения многочлена f над полем K, и любые два таких расширения изоморфны.

⋆ Теорема об описании конечных полей. *Пусть $p \in \mathbb{P}$ и*

1. пусть $n \in \mathbb{N}$, E — поле и $E \cong \mathrm{Spl}_{\mathbb{F}_p}(x^{p^n} - x)$; тогда $\mathrm{char}\,E = p$ и $|E : \mathbb{F}_p| = n$;

2. пусть E — поле, $\mathrm{char}\,E = p$ и $|E : \mathbb{F}_p| < \infty$; обозначим через n число $|E : \mathbb{F}_p|$; тогда выполнено $E \cong \mathrm{Spl}_{\mathbb{F}_p}(x^{p^n} - x)$.

⋆ Теорема о подполях конечного поля.

Пусть E — поле и $|E| < \infty$; обозначим через p число $\mathrm{char}\,E$ и через n число $|E : \mathbb{F}_p|$ и

1. пусть $l \in \mathbb{N}$ и l делит n; обозначим через F подмножество $\{e \in E \mid e^{p^l} = e\}$ поля E; тогда F — подполе поля E и $|F : \mathbb{F}_p| = l$;

2. пусть F — подполе поля E; обозначим через l число $|F : \mathbb{F}_p|$; тогда l делит n и выполнено $F = \{e \in E \mid e^{p^l} = e\}$.

Приложение

В списке основных утверждений курса имеются несколько однотипных теорем, смысл которых состоит в описании биекций между некоторыми множествами; ниже приведены *краткие концептуальные формулировки* этих теорем, в которых биекции выписаны явно. В этих формулировках используются следующие дополнительные обозначения (формулировки теорем даны после списка обозначений).

$\mathrm{Subgroups}(G)$	множество всех подгрупп группы G
$\mathrm{Divisors}(n)$	множество $\{l \in \mathbb{N} \mid l \text{ делит } n\}$, если $n \in \mathbb{N}$, и множество $\mathbb{N} \cup \{\infty\}$, если $n = \infty$
$\mathrm{Homogeneous}G\text{-}\mathrm{Sets}$	класс всех однородных G-множеств (G — группа)
$\mathrm{FiniteFields}_p$	класс всех конечных полей характеристики p ($p \in \mathbb{P}$)
$\mathrm{Subfields}(E)$	множество всех подполей поля E

Первая теорема о подгруппах циклической группы.

Пусть G — циклическая группа, $d \in G$ и $G = \langle d \rangle$; обозначим через n величину $|G|$.

Рассмотрим множество $\mathrm{Subgroups}(G)$ *и множество* $\mathrm{Divisors}(n)$*; следующие отображения определены корректно и являются взаимно обратными биекциями между этими множествами:*

$$\begin{aligned} \mathrm{Subgroups}(G) &\to \mathrm{Divisors}(n) \\ H &\mapsto \min\{a \in \mathbb{N} \mid d^a \in H\}; \end{aligned} \qquad \begin{aligned} \mathrm{Divisors}(n) &\to \mathrm{Subgroups}(G) \\ l &\mapsto \begin{cases} \langle d^l \rangle, & \text{если } l \in \mathbb{N}, \\ \{1\}, & \text{если } l = \infty. \end{cases} \end{aligned}$$

Замечание. Между формулировкой первой теоремы о подгруппах циклической группы из списка основных утверждений курса и ее формулировкой, приведенной выше, имеется следующее дополнительное отличие в том случае, когда $n = \infty$: в формулировке из списка основных утверждений идет речь о тех же биекциях, что и в приведенной выше формулировке, но для простоты записи из множества $\mathrm{Subgroups}(G)$ исключена подгруппа $\{1\}$, а из множества $\mathrm{Divisors}(\infty)$ исключена величина ∞.

Замечание. В обозначениях первой теоремы о подгруппах циклической группы (G — циклическая группа, $d \in G$, $G = \langle d \rangle$ и $H \leq G$) имеет место следующий факт: $\min\{a \in \mathbb{N} \mid d^a \in H\} = |G : H|$.

Вторая теорема о подгруппах циклической группы.

Пусть G — циклическая группа и $|G| < \infty$; обозначим через n число $|G|$.

Рассмотрим множество $\mathrm{Subgroups}(G)$ *и множество* $\mathrm{Divisors}(n)$*; следующие отображения определены корректно и являются взаимно обратными биекциями между этими множествами:*

$$\begin{aligned} \mathrm{Subgroups}(G) &\to \mathrm{Divisors}(n) \\ H &\mapsto |H|; \end{aligned} \qquad \begin{aligned} \mathrm{Divisors}(n) &\to \mathrm{Subgroups}(G) \\ m &\mapsto \{g \in G \mid g^m = 1\}. \end{aligned}$$

Замечание. Из теорем о подгруппах циклической группы можно вывести следующий факт.

Пусть G — циклическая группа, $d \in G$, $G = \langle d \rangle$, $|G| < \infty$ и $k \in \mathbb{Z}$, а также $y \in \mathbb{Z}$; тогда

1. $\mathrm{Im}\,\mathrm{pow}_{k,G} = \langle d^{\gcd(k,|G|)} \rangle$ *и* $|\mathrm{Im}\,\mathrm{pow}_{k,G}| = \frac{|G|}{\gcd(k,|G|)}$;

2. $\mathrm{Ker}\,\mathrm{pow}_{k,G} = \langle d^{\frac{|G|}{\gcd(k,|G|)}} \rangle$ *и* $|\mathrm{Ker}\,\mathrm{pow}_{k,G}| = \gcd(k,|G|)$;

3. используя соотношение Безу, представим число $\gcd(k,|G|)$ в виде $uk + v|G|$, где $u, v \in \mathbb{Z}$, тогда

$$\mathrm{pow}_{k,G}^{-1}(d^y) = \begin{cases} d^{\frac{uy}{\gcd(k,|G|)}}\,\mathrm{Ker}\,\mathrm{pow}_{k,G}, & \text{если } \gcd(k,|G|) \text{ делит } y, \\ \varnothing, & \text{если } \gcd(k,|G|) \text{ не делит } y. \end{cases}$$

⋆ Теорема об описании однородных G-множеств. *Пусть G — группа.*

Рассмотрим множество $\mathrm{Homogeneous}G\text{-}\mathrm{Sets}/{\cong}$ *классов изоморфизма всех однородных G-множеств и множество* $\mathrm{Subgroups}(G)/{\sim}$ *классов сопряженности всех подгрупп группы G; следующие отображения определены корректно и являются взаимно обратными биекциями между этими множествами:*

$$\begin{aligned} \mathrm{Homogeneous}G\text{-}\mathrm{Sets}/{\cong} &\to \mathrm{Subgroups}(G)/{\sim} \\ \begin{pmatrix} \text{класс изоморфизма} \\ G\text{-множества } X \end{pmatrix} &\mapsto \{\mathrm{St}_G(x) \mid x \in X\}; \end{aligned} \qquad \begin{aligned} \mathrm{Subgroups}(G)/{\sim} &\to \mathrm{Homogeneous}G\text{-}\mathrm{Sets}/{\cong} \\ \begin{pmatrix} \text{класс сопряженно-} \\ \text{сти подгруппы } H \end{pmatrix} &\mapsto \begin{pmatrix} \text{класс изоморфизма} \\ G\text{-множества } G/H \end{pmatrix}. \end{aligned}$$

⋆ Теорема об описании конечных полей. *Пусть $p \in \mathbb{P}$.*

Рассмотрим множество $\mathrm{FiniteFields}_p/{\cong}$ *классов изоморфизма всех конечных полей характеристики p и множество $\mathbb{N}$; следующие отображения определены корректно и являются взаимно обратными биекциями между этими множествами:*

$$\begin{aligned} \mathrm{FiniteFields}_p/{\cong} &\to \mathbb{N} \\ (\text{класс изоморфизма поля } E) &\mapsto |E : \mathbb{F}_p|; \end{aligned} \qquad \begin{aligned} \mathbb{N} &\to \mathrm{FiniteFields}_p/{\cong} \\ n &\mapsto (\text{класс изоморфизма поля } \mathrm{Spl}_{\mathbb{F}_p}(x^{p^n} - x)). \end{aligned}$$

⋆ Теорема о подполях конечного поля.

Пусть E — поле и $|E| < \infty$; обозначим через p число $\mathrm{char}\,E$ и через n число $|E : \mathbb{F}_p|$.

Рассмотрим множество $\mathrm{Subfields}(E)$ *и множество* $\mathrm{Divisors}(n)$*; следующие отображения определены корректно и являются взаимно обратными биекциями между этими множествами:*

$$\begin{aligned} \mathrm{Subfields}(E) &\to \mathrm{Divisors}(n) \\ F &\mapsto |F : \mathbb{F}_p|; \end{aligned} \qquad \begin{aligned} \mathrm{Divisors}(n) &\to \mathrm{Subfields}(E) \\ l &\mapsto \{e \in E \mid e^{p^l} = e\}. \end{aligned}$$