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 $l = \min\{k \in \mathbb{N} \mid d^k \in H\}$;

2. пусть $H \le G$ и, если $n = \infty$, то $H \ne \{1\}$; обозначим через l число $\min\{k \in \mathbb{N} \mid d^k \in H\}$; 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 гомоморфизме для групп.

Пусть G, J — группы и $f \in \operatorname{Hom}(G, J)$; тогда $\operatorname{Im} f \le J$, $\operatorname{Ker} f \trianglelefteq G$ и $G/\operatorname{Ker} f \cong \operatorname{Im} f$.

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 $\gcd(m, n) = 1$.

Описание gcd и lcm в кольце $\mathbb{Z}$ в терминах идеалов.

Пусть $m, n \in \mathbb{Z}$; тогда $\gcd(m, n)\mathbb{Z} = m\mathbb{Z} + n\mathbb{Z}$ и $\operatorname{lcm}(m, n)\mathbb{Z} = m\mathbb{Z} \cap n\mathbb{Z}$.

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.

Лемма об обратимых остатках.

Пусть $n \in \mathbb{N}$ и $a \in \mathbb{Z}/n$; тогда $a \in (\mathbb{Z}/n)^\times \Leftrightarrow \gcd(a, n) = 1 \Leftrightarrow \langle a\rangle = (\mathbb{Z}/n)^+$.

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

Теорема о функции Эйлера.

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

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 $\varphi(n) = n\bigl(1 - \frac{1}{p_1}\bigr) \cdot \ldots \cdot \bigl(1 - \frac{1}{p_t}\bigr)$.

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 по модулю n.

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 фундаментальных транспозиций.

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

1. $\exists\, i_1, \ldots, i_l \in \{1, \ldots, n-1\}$ $(u = \sigma_{i_1} \cdot \ldots \cdot \sigma_{i_l})$;

2. $\forall\, t \in \mathbb{N}_0,\, i_1, \ldots, i_t \in \{1, \ldots, n-1\}$ $\big(u = \sigma_{i_1} \cdot \ldots \cdot \sigma_{i_t} \Rightarrow (t \geq l \wedge t \equiv l \pmod 2)\big)$.

Теорема об описании классов сопряженности в симметрических группах.

Пусть $n \in \mathbb{N}_0$; тогда отображение, действующее из множества классов сопряженности в группе S_n в множество разбиений числа n по правилу (класс сопряженности перестановки u) $\mapsto$ (цикловый тип перестановки u) для любых $u \in \mathrm{S}_n$, определено корректно и является биекцией.

⋆ 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 и $S/\mathrm{Ker}\, f \cong \mathrm{Im}\, f$.

⋆ Теорема о свободных структурах.

Пусть Σ — сигнатура, I — множество Σ-тождеств, B — множество; обозначим через S Σ-структуру $\mathrm{F}_I(B)$ и обозначим через σ отображение, действующее из B в S по правилу $b \mapsto$ (класс терма b) для любых $b \in B$; тогда для любой Σ-структуры $S' \in \mathrm{Var}_I$ и для любого отображения σ', действующего из B в S', существует единственный такой гомоморфизм $f \in \mathrm{Hom}(S, S')$, что $f\sigma = \sigma'$.

⋆ Китайская теорема об остатках для колец.

Пусть R — кольцо, $t \in \mathbb{N}_0$, $I_1, \ldots, I_t \trianglelefteq R$ и $\forall\, j, k \in \{1, \ldots, t\}$ $(j \neq k \Rightarrow I_j + I_k = R)$. Обозначим через I идеал $I_1 \cap \ldots \cap I_t$ кольца R; тогда отображение, действующее из R/I в $R/I_1 \times \ldots \times R/I_t$ по правилу $r + I \mapsto (r + I_1, \ldots, r + I_t)$ для любых $r \in R$, определено корректно и является изоморфизмом колец.

⋆ Лемма о делимости и главных идеалах.

Пусть R — коммутативное кольцо; тогда

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

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

⋆ 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 $\forall\, r, s \in R$ $(r \overset{\downarrow}{\sim} s \Leftrightarrow r \in sR^\times)$, $\mathrm{Irr}(R) = \{r \in R \mid$ идеал (r) — максимальный нетривиальный главный идеал кольца $R\}$ и $\mathrm{Prime}(R) \subseteq \mathrm{Irr}(R)$.

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

⋆ 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 $\mathrm{Irr}(R) = \mathrm{Prime}(R)$.

⋆ Теорема о включениях между классами колец.

Евклидовы области суть области главных идеалов; области главных идеалов факториальны.

⋆ 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 $C = \{\mathrm{St}_G(x) \mid x \in X\}$;

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 $|G \backslash X| = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}_X(g)|$.*

⋆ 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.*

⋆ Теорема о полупрямом произведении.

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

• $G = FH$, $F \cap H = \{1\}$ *и* $\forall\, h \in H\ (hFh^{-1} \le F)$*;*

• *существует такой гомоморфизм* $c \in \mathrm{Hom}(H, \mathrm{Aut}(F))$*, что отображение, действующее из* ${}^{c}(F \rtimes H)$ *в* G *по правилу* $(f, h) \mapsto fh$ *для любых* $f \in F$ *и* $h \in H$*, — изоморфизм групп.*

⋆ Описание гомоморфизмов между свободными модулями в терминах матриц.

Пусть R *— кольцо,* M*,* N*,* O *— свободные* R*-модули,* B*,* C*,* D *— базисы* R*-модулей* M*,* N*,* O*; тогда*

1. отображение, действующее из $\mathrm{Hom}(M, N)$ *в* $\mathrm{Mat}(C, B, R^{\mathrm{op}})_{\mathtt{cf}}$ *по правилу* $f \mapsto [f]_B^C$ *для любых* $f \in \mathrm{Hom}(M, N)$*, — изоморфизм абелевых групп;*

2. $\forall\, m \in M,\ f \in \mathrm{Hom}(M, N),\ g \in \mathrm{Hom}(N, O)\ \big([f(m)]^C = [f]_B^C\,[m]^B \ \wedge\ [gf]_B^D = [g]_C^D\,[f]_B^C\big)$.

⋆ 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,* $|C| \le |D|$*) и* $(D \setminus D') \cup C$ *— порождающее подмножество в* V*.*

⋆ Лемма о корнях многочлена.

1. Пусть R *— коммутативное кольцо,* $f \in R[x]$ *и* $r \in R$*; тогда* $f(r) = 0$*, если и только если* $x - r$ *делит* f*, и* r *— кратный корень многочлена* f*, если и только если* $f(r) = f'(r) = 0$*.*

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

⋆ Теорема о полиномиальных функциях.

Пусть R *— коммутативное кольцо; тогда отображение* subst_R*, действующее из* $R[x]$ *в* R^R *по правилу* $f \mapsto$ *(полиномиальная функция на* R*, определяемая многочленом* f*) для любых* $f \in R[x]$*, — гомоморфизм* R*-алгебр; пусть дополнительно* R *— область целостности; тогда* $|R| = \infty$ *и* $\mathrm{Ker}\,\mathrm{subst}_R = \{0\}$*, или* $|R| < \infty$*, структура кольца на* R *продолжается до структуры поля и* $\mathrm{Ker}\,\mathrm{subst}_R = (x^{|R|} - x)$*.*

⋆ Теорема о конечных подгруппах.

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

⋆ Теорема об алгебраических элементах.

Пусть K *— поле,* E *— расширение поля* K *и* $e \in E$*; тогда следующие свойства эквивалентны:*

• *существует такой многочлен* $f_e \in \mathrm{Irr}(K[x])$*, что отображение, действующее из* $K[x]/(f_e)$ *в* $K(e)$ *по правилу* $f + (f_e) \mapsto f(e)$ *для любых* $f \in K[x]$*, определено корректно и является изоморфизмом расширений поля* K*;* • $|K(e) : K| < \infty$*;* • e *— алгебраический элемент расширения* E*.*

⋆ Теорема о поле разложения.

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

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

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

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

⋆ Теорема о подполях конечного поля.

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

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

2. пусть F *— подполе поля* E*; обозначим через* r *число* $|F|$*; тогда* $r = p^l$*, где* $l \in \mathbb{N}$ *и* l *делит* n*, и* $F = \{e \in E \mid e^r = e\}$*.*