Задачи по алгебраическим структурам (SE). 2

Задачи

(**4**) 17. а) Пусть G — группа; докажите, что следующие свойства эквивалентны:

- $\forall\, H \subseteq G\ \big((HH \subseteq H\ \wedge\ H \neq \varnothing)\ \Rightarrow\ H \leq G\big)$;
- порядки всех элементов группы G конечны.

б) Пусть G — группа, $H \trianglelefteq G$ и порядки всех элементов группы H и группы G/H конечны; докажите, что порядки всех элементов группы G конечны.

(**4**) 18. а) Пусть $p \in \mathbb{P} \setminus \{2\}$ и $\omega \in \mathbb{N}$, или $p = 2$ и $\omega = 2$; докажите, что $\{a \in \mathbb{Z}/p^\omega \mid a^2 = 1\} = \{1, -1\}$.

б) Пусть $\omega \in \mathbb{N} \setminus \{1, 2\}$; докажите, что $\{a \in \mathbb{Z}/2^\omega \mid a^2 = 1\} = \{1, -1, 1 + 2^{\omega-1}, -1 + 2^{\omega-1}\}$.

в) Пусть $n \in \mathbb{N}$; обозначим через t число $|\{p \in \mathbb{P} \mid p \mid n\}|$; докажите, что

$$|\{a \in \mathbb{Z}/n \mid a^2 = 1\}| = \begin{cases} 2^t, \text{ если } 2 \nmid n\ \vee\ (4 \mid n\ \wedge\ 8 \nmid n); \\ 2^{t-1}, \text{ если } 2 \mid n\ \wedge\ 4 \nmid n; \\ 2^{t+1}, \text{ если } 8 \mid n. \end{cases}$$

Комментарий к условию: равенство "$a^2 = 1$", где a — элемент кольца $\mathbb{Z}/p^\omega$, или $\mathbb{Z}/2^\omega$, или $\mathbb{Z}/n$, нужно понимать как равенство в соответствующем кольце (при переходе к кольцу $\mathbb{Z}$ это равенство превращается в сравнение по соответствующему модулю).

• В задаче 20 используется следующее обозначение: для любого числа $k \in \mathbb{Z}$ и любой группы G обозначим через $\mathrm{pow}_{k,G}$ отображение, действующее из G в G по правилу $g \mapsto g^k$ для любых $g \in G$ (то есть отображение $\mathrm{pow}_{k,G}$ — это *операция возведения в степень k в группе G*); в пункте а задачи 5 было доказано, что, если группа G абелева, то отображение $\mathrm{pow}_{k,G}$ — эндоморфизм группы G.

(**4**) 20. Пусть G — циклическая группа, $d \in G$, $G = \langle d \rangle$, $|G| < \infty$ и $k \in \mathbb{Z}$.

а) Докажите, что $\operatorname{Im} \mathrm{pow}_{k,G} = \langle d^{\gcd(k,|G|)} \rangle$ и $|\operatorname{Im} \mathrm{pow}_{k,G}| = \frac{|G|}{\gcd(k,|G|)}$.

б) Докажите, что $\operatorname{Ker} \mathrm{pow}_{k,G} = \langle d^{\frac{|G|}{\gcd(k,|G|)}} \rangle$ и $|\operatorname{Ker} \mathrm{pow}_{k,G}| = \gcd(k, |G|)$.

в) Пусть также $y \in \mathbb{Z}$; используя соотношение Безу, представим число $\gcd(k, |G|)$ в виде $uk + v|G|$, где $u, v \in \mathbb{Z}$, и, если $\gcd(k, |G|) \mid y$, то обозначим через x число $\frac{uy}{\gcd(k,|G|)}$; докажите, что

$$\mathrm{pow}^{-1}_{k,G}(d^y) = \begin{cases} d^x \operatorname{Ker} \mathrm{pow}_{k,G}, \text{ если } \gcd(k, |G|) \mid y; \\ \varnothing, \text{ если } \gcd(k, |G|) \nmid y. \end{cases}$$

• В вопросе 8 курса будет доказано, что по любому простому модулю p существует первообразный корень (то есть группа $\mathbb{F}_p^\times$ циклическая). Предположим, что это утверждение верно, и зафиксируем некоторый порождающий элемент d группы $\mathbb{F}_p^\times$, а также пусть $k \in \mathbb{Z}$; тогда, используя задачу 20 (в качестве G нужно взять группу $\mathbb{F}_p^\times$), мы получим, что имеют место перечисленные ниже факты.

⋆ $\operatorname{Im} \mathrm{pow}_{k,\mathbb{F}_p^\times} = \langle d^{\gcd(k,p-1)} \rangle$ и $|\operatorname{Im} \mathrm{pow}_{k,\mathbb{F}_p^\times}| = \frac{p-1}{\gcd(k,p-1)}$.

⋆ $\operatorname{Ker} \mathrm{pow}_{k,\mathbb{F}_p^\times} = \langle d^{\frac{p-1}{\gcd(k,p-1)}} \rangle$ и $|\operatorname{Ker} \mathrm{pow}_{k,\mathbb{F}_p^\times}| = \gcd(k, p-1)$.

⋆ Пусть также $y \in \mathbb{Z}$; используя соотношение Безу, представим число $\gcd(k, p-1)$ в виде $uk + v(p-1)$, где $u, v \in \mathbb{Z}$, и, если $\gcd(k, p-1) \mid y$, то обозначим через x число $\frac{uy}{\gcd(k,p-1)}$; тогда

$$\mathrm{pow}^{-1}_{k,\mathbb{F}_p^\times}(d^y) = \begin{cases} d^x \operatorname{Ker} \mathrm{pow}_{k,\mathbb{F}_p^\times}, \text{ если } \gcd(k, p-1) \mid y; \\ \varnothing, \text{ если } \gcd(k, p-1) \nmid y. \end{cases}$$

Эти факты используются во многих приложениях элементарной теории чисел (например, в дискретном преобразовании Фурье над конечными полями); далее в курсе эти факты будут использоваться для анализа степенных уравнений в кольцах остатков, а также в исследовании тестов на простоту.

(**5**) 21. Пусть G — группа и $|G| < \infty$.

а) Пусть также $g \in G$ и $k \in \mathbb{Z}$; докажите, что $\operatorname{ord}(g^k) = \frac{\operatorname{ord}(g)}{\gcd(k, \operatorname{ord}(g))}$.

б) Пусть также $f, h \in G$, $fh = hf$ и $\gcd(\operatorname{ord}(f), \operatorname{ord}(h)) = 1$; докажите, что $\operatorname{ord}(fh) = \operatorname{ord}(f)\operatorname{ord}(h)$.

в) Пусть также группа G абелева; обозначим через m число $\operatorname{lcm}(\{\operatorname{ord}(g) \mid g \in G\})$ (то есть наименьшее общее кратное порядков всех элементов группы G); докажите, что $\exists\, g \in G\ (\operatorname{ord}(g) = m)$.

• Пункт в задачи 21 будет использоваться в доказательстве того, что по любому простому модулю существует первообразный корень.

Указания к задачам

17. Это задача по теории групп (она не связана с кольцами); для того, чтобы ее решить, нужно понимать, что такое подгруппа, порядок элемента и факторгруппа. Пункты а и б независимы.

18. а), б) То, что $a^2 = 1$ в кольце остатков по некоторому модулю, равносильно тому, что число $a^2 - 1$ делится на этот модуль в кольце $\mathbb{Z}$.

в) Представим$^{(\star)}$ 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 $\omega_1, \ldots, \omega_t \in \mathbb{N}$ (здесь символ "t" имеет тот же смысл, что и в условии задачи). Сначала, используя китайскую теорему об остатках, свяжите число $|\{a \in \mathbb{Z}/n \mid a^2 = 1\}|$ с числами $|\{a \in \mathbb{Z}/p_1^{\omega_1} \mid a^2 = 1\}|, \ldots, |\{a \in \mathbb{Z}/p_t^{\omega_t} \mid a^2 = 1\}|$; затем используйте пункты а и б.

20. а) Сначала, используя пункт а задачи 7, докажите, что $|\operatorname{Im}\operatorname{pow}_{k,G}| = \frac{|G|}{\gcd(k, |G|)}$; затем используйте первую теорему о подгруппах циклической группы и следующее замечание к ней: для любой подгруппы H группы G выполнено $\min\{k \in \mathbb{N} \mid d^k \in H\} = |G : H| = \frac{|G|}{|H|}$.

б) Сначала, используя пункт а задачи 9 и вторую теорему о подгруппах циклической группы, докажите, что $|\operatorname{Ker}\operatorname{pow}_{k,G}| = \gcd(k, |G|)$; затем действуйте так же, как в пункте а.

в) Сначала докажите, что $d^{kx} = d^y$; затем используйте пункты а и б, а также "высокодуховную" лемму из доказательства теоремы о гомоморфизме для групп.

21. а) Используйте пункт а задачи 7. б) Сначала докажите, что $\langle f \rangle \cap \langle h \rangle = \{1\}$.

в) Представим$^{(\star)}$ число m 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 $\omega_1, \ldots, \omega_t \in \mathbb{N}$. Сначала, используя пункт а, для каждого числа $i \in \{1, \ldots, t\}$ постройте такой элемент g_i группы G, что $\operatorname{ord}(g_i) = p_i^{\omega_i}$; затем используйте пункт б.

Задачи′

(**2**) 3′. Пусть $H \leq \mathbb{C}^\times$ и $|H| < \infty$; обозначим через n число H; докажите, что $H = \mu_n$.

(**2**) 4′. Пусть G — группа и $|G| = \infty$; докажите, что $|\{H \subseteq G \mid H \leq G\}| = \infty$.

$^{(\star)}$Используем основную теорему арифметики (`http://en.wikipedia.org/wiki/Fundamental_theorem_of_arithmetic`).