Семинар 21

1 Повторение

Примеры колец: $\mathrm{M}_n(\mathbb{R})$, $\mathbb{R}[x]$, $\mathbb{Z}_n$.

Делители нуля. Утверждение о том, что 0 – поглощающий элемент в кольце. Целостное кольцо. Критерий целостности для нетривиального коммутативного кольца с единицей (закон сокращения).

Обратимые элементы в кольце. Мультипликативная группа кольца. Поле, примеры полей. Подкольцо. Подполя: примеры.

Алгоритм Евклида нахождения наибольшего общего делителя в кольце многочленов. Выражение для наибольшего общего делителя двух многочленов.

Определение гомоморфизма колец. Двусторонний идеал. Главный идеал. Примеры. Замечание, что $\mathbb{Z}$ — кольцо главных идеалов. Факторкольцо кольца по идеалу.

2 Задачи

Задача 1 из ДЗ.

Задача 1. Классы сопряжённости группы A_4:

$$\{\mathrm{id}\}, \quad \{(12)(34),\ (13)(24),\ (14)(23)\},$$

$$\{(123),\ (134),\ (142),\ (243)\}, \quad \{(132),\ (124),\ (143),\ (234)\}.$$

Из соображений делимости получаем, что единственная собственная нормальная подгруппа в A_4 – это V_4.

Для любой конечной группы G и её элемента $g \in G$ верен следующий факт:

$$|C_G(g)| \text{ делит } |G|.$$

Задача 1. Пусть U – это подгруппа $\mathbb{C}^\times$, состоящая из всех чисел, модуль которых равен 1. Для $n \in \mathbb{N}$ обозначим также через U_n подгруппу в U корней n-й степени из единицы. Доказать, что:

1. $\mathbb{R}/\mathbb{Z} \cong U$;

2. $U/U_n \cong U$;

3. $\mathbb{C}^\times/\mathbb{R}^\times_{>0} \cong U$.

Задача 2. Пусть

$$G = \mathrm{GL}_n(\mathbb{R}),\ P = \mathrm{SL}_n(\mathbb{R}),\ D = \{X \in G \mid \det X > 0\}.$$

Доказать, что:

1. $G/P \cong \mathbb{R}^\times$;

2. $G/D \cong \mathbb{Z}_2$.

Задача 3. Доказать, что подгруппа H группы G нормальна, если:

1. G абелева;

2. $G = S_4$, $H = V_4$.

Определим $\mathrm{GL}_n(\mathbb{Z})$ как множество всех невырожденных матриц g из $\mathrm{Mat}_n(\mathbb{Z})$ таких, что элементы g и g^{-1} – это целые числа. На самом деле

$$\mathrm{GL}_n(\mathbb{Z}) = \{g = (g_{ij}) \in \mathrm{Mat}_n(\mathbb{Z}) \mid \det(g) = \pm 1\}.$$

Задача 4. Будет ли нормальной подгруппой в группе $\mathrm{GL}_2(\mathbb{Z})$ множество H всех матриц вида

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

где числа a, d нечётны, а числа b, c чётны?

Задача 5. Доказать, что факторгруппа $\mathbb{R}^\times/\mathbb{Q}^\times$ не является циклической.

Пусть G – группа. Автоморфизмы из $\mathrm{Aut}(G)$, которые равны c_g для некоторого $g \in G$ (сопряжение элементом g), называются *внутренними*. Подгруппа всех внутренних автоморфизмов в $\mathrm{Aut}(G)$ (то есть образ гомоморфизма $c : G \to \mathrm{Aut}(G)$) обозначается $\mathrm{Inn}(G)$.

Центром группы G называется подмножество

$$Z(G) = \{g \in G \mid gx = xg\ \forall x \in G\} \subseteq G.$$

Заметим, что $g \in Z(G) \iff C_G(g) = \{g\}$.

Задача 6. Доказать, что $\mathrm{Inn}(G) \cong G/Z(G)$.

Определим также *централизатор* элемента $a \in G$:

$$Z_G(a) = \{g \in G \mid ga = ag\}.$$

Централизатор является подгруппой в G (не обязательно нормальной).

Задача 7. Найти центр группы $\mathrm{GL}_n(\mathbb{R})$.

Криптография с открытым ключом

Пусть G – конечная группа и $g \in G$ – элемент большого порядка.

Важный пример. $G = \mathbb{Z}_p^\times := (\mathbb{Z}_p \setminus \{\overline{0}\}, \cdot)$ при простом $p \in \mathbb{N}$. Оказывается, что такая группа всегда циклическая, то есть всегда существует натуральное число g такое, что g не делится на p и порядок $\overline{g}$ в группе $\mathbb{Z}_p^\times$ равен $p-1$.

Пример 1. Пусть $p = 7$.

Элемент g	Его степени (mod 7)
1	1
2	2, 4, 1
3	3, 2, 6, 4, 5, 1
4	4, 2, 1
5	5, 4, 6, 2, 3, 1
6	6, 1

Задача дискретного логарифмирования. Пусть задан элемент $h \in G$. Нужно найти такое $k \in \mathbb{N}$, что $h = g^k$. Несмотря на то, что для любого фиксированного $n \in \mathbb{N}$ можно "быстро" вычислить g^n (за $\mathrm{O}(n)$ умножений с помощью быстрого возведения в степень), найти нужное k – это долго ($\mathrm{O}(\mathrm{ord}(g))$).

Схема Диффи-Хеллмана. Всем участникам известны G и g. Каждый участник фиксирует $a \in \mathbb{N}$ $(1 < a < \mathrm{ord}(g))$, держит его в секрете, но всем сообщает g^a. Теперь пара участников A и B могут составить секретный общий ключ g^{ab}: A возводит $(g^b)^a$, B возводит $(g^a)^b$.

Схема Эль-Гамаля. Всем участникам известны G и g. Каждый участник фиксирует $a \in \mathbb{N}$ $(1 < a < \mathrm{ord}(g))$, держит его в секрете, но всем сообщает g^a. Если B хочет передать A сообщение $h \in G$, то он выбирает $k \in \mathbb{N}$ и сообщает всем пару $(g^k,\ h(g^a)^k)$. Только A может восстановить h: $h = (hg^{ak})(g^k)^{|G|-a}$.