7 Лекция 25.04

Теорема 9 (Кэли). *Всякая конечная группа G порядка n изоморфна подгруппе симметрической группы S_n.*

Доказательство. Рассмотрим действие $G \times G \to G$ левыми сдвигами. Это задает гомоморфизм $a : G \to S(G)$. Это действие свободно, следовательно эффективно, что в свою очередь значит, что $\ker a = \{e\}$. Тогда a инъективен. По теореме о гомоморфизме $G \cong G/\{e\} \cong \operatorname{Im} a \subseteq S(G) = S_n$. □

Кольца и поля

Определение 39. *Кольцо — множество $(R, +, \times)$, которое удовлетворяет следующим аксиомам:*

1. $(R, +)$ — *абелева группа.*
2. *дистрибутивность*
$$a(b + c) = ab + ac$$
$$(b + c)a = ba + ca$$
3. $(R, \times)$ — *ассоциативно*
4. $\exists 1 \in R, \forall a \in R : a \cdot 1 = 1 \cdot a = a$

Утверждение 5. $\forall a \in R : a \cdot 0 = 0 \cdot a = 0$.

Доказательство. $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0 \Leftrightarrow a \cdot 0 = 0$ □

Следствие 12. Если $|R| \geq 2$, то $0 \neq 1$.

Определение 40. *Кольцо R коммутативно, если умножение коммутативно, то есть $\forall a, b \in R : a \cdot b = b \cdot a$.*

Примеры колец

1. Числовые кольца — $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$
2. Вычеты $\mathbb{Z}_n$
3. $M_n(\mathbb{R})$, где R — кольцо
4. Многочлены $R[x], R[x_1, \ldots, x_n]$ — от одной и от многих переменных
5. Формальные степенные ряды $R[[x]] = \left\{\sum_{i=0}^{\infty} a_i x^i, a_i \in R\right\}$; справедливо $R[x] \subseteq R[[x]]$
6. Кольцо функций $F(M, R)$, где M — множество, R — кольцо. $F(M, R) = \{f : M \to R\}$. Введем операции
$$(f_1 + f_2)(m) := f_1(m) + f_2(m), (f_1 \cdot f_2)(m) := f_1(m) \cdot f_2(m)$$
Нулем и единицей будут 0 и 1 соответственно.

Определение 41. *В кольце R элемент $a \in R$ называется обратимым, если $\exists b \in R : ab = ba = 1$.*

Замечание 6. *Все обратимые элементы кольца образуют группу по умножению.*

Определение 42. *Элемент $a \in R$ $(a \neq 0)$ называется левым (соответственно правым) делителем нуля, если $\exists b \in R$ $(b \neq 0) : ab = 0$ (соответственно $ba = 0$).*

Замечание 7. *Все делители нуля необратимы. Если $ab = 0$, и a обратим, то $a^{-1}ab = (a^{-1}a)b = b = 0$, но $b \neq 0$.*

Определение 43. *Элемент $a \in R$ $(a \neq 0)$ называется нильпотентным, если $\exists m \in \mathbb{N} : a^m = 0$.*

Замечание 8. *Нильпотент является делителем нуля, так как $a \cdot a^{m-1} = 0$, но $a, a^{m-1} \neq 0$.*

Определение 44. *Элемент $a \in R$ называется идемпотентом, если $a^2 = a$.*

Определение 45. *Поле K — коммутативное кольцо и любой ненулевой элемент обратим.*

Пример. $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$ (где p простое) — поля.

Определение 46. *Подкольцо $(R', +, \times)$, где $R' \subseteq R$, определяется аналогично кольцу. Так же определяется подполе.*

Определение 47. *Алгебра — кольцо + векторное пространство над полем K. Оно задается как $(R, +, \times, \lambda)$, то есть можно умножать на скаляр $\lambda \in K$.*

Примеры алгебр

1. Поле K — алгебра над K.
2. $M_n(K)$ — алгебра над K, $\dim = n^2$
3. $K[x_1, \dots, x_n]$ — алгебра над K, $\dim = \infty$ (но счетная)
4. $F(M, K)$ – алгебра над K, $\dim = |M|$ (можно задать функции, которые в одной точке 1, а во всех остальных 0, и через них выразить все другие функции)

Определение 48. *Подалгебра — подкольцо + подпространство.*

Определение 49. *Идеал I кольца R — подмножество, которое удовлетворяет 2 свойствам:*

1. *подгруппа по сложению*
2. *$\forall a \in I, r \in R : ar \in I, ra \in I$ (это для двустороннего идеала; аналогично определяются односторонние идеалы)*

Замечание 9. *Идеалы — это аналог нормальных подгрупп (по ним можно факторизовать).*

Упражнение. $I = R \Leftrightarrow 1 \in I \Leftrightarrow$ в идеале есть обратимый элемент.

Как строить идеалы? Здесь и далее полагаем, что R коммутативно. Определим главный идеал элемента $r \in R$, где $(r) = \{ar \mid a \in R\}$.

Пример. Пусть $R = \mathbb{Z}$. Тогда $(k) = k\mathbb{Z}$, и все идеалы главные (так как любая подгруппа $\mathbb{Z}$ имеет вид $k\mathbb{Z}$).

Бывают ли неглавные идеалы? Рассмотрим $\mathbb{R}[x, y]$ кольцо многочленов, у которых свободный член нулевой. Обобщим понятие главного идеала. Пусть $S \subseteq R$ — идеал:

$$(S) = \{a_1 s_1 + \dots + a_n s_n \mid k \in \mathbb{N}, s_i \in S, a_i \in \mathbb{R}\}$$

Факторкольцо Факторкольцом называется $R/I = \{a + I, a \in R\}$. Определим сложение $(a+I)+(b+I) = (a+b)+I$ и умножение $(a+I)(b+I) = ab+I$. Определение корректно, потому что

$$((a+i)+I)((b+j)+I) = (ab+ib+aj+ij)+I, ib+aj+ij \in I$$

Нетрудно видеть, что $\mathbb{Z} = \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/(n)$. Также определим гомоморфизм $\varphi : R_1 \to R_2, \ker\varphi = \{a \in R \mid \varphi(a) = 0\}$ — идеал в R_1. Аналогично определим образ $\operatorname{Im}\varphi = \{\varphi(a) \mid a \in R_1\}$.

Теорема 10 (О гомоморфизме для колец)**.** $\operatorname{Im}\varphi \cong R_1/\ker\varphi$.