Лекция 19

Идеалы и факторкольца. Часть 1

§ 2. Идеалы и факторкольца (продолжение)

Пример. Пусть $R = \mathrm{Mat}_n(F)$, где F — поле. Тогда $I = \left\{ \begin{pmatrix} * & & 0 \\ * & & \\ * & & \\ * & & \end{pmatrix} \right\}$ (звёздочки стоят в первом столбце) — левый, но не правый идеал.

Дальше рассматриваем только двусторонние идеалы, называя их просто идеалами.

Лемма 1. *Пусть I — идеал в кольце R. Тогда $I = R \Leftrightarrow I$ содержит обратимый элемент.*

□

- $\boxed{\Rightarrow}$

  $I = R \Rightarrow 1 \in I$, а 1 — обратимый элемент.

- $\boxed{\Leftarrow}$

  $a \in I$, $\exists\, b \in R : ab = ba = 1 \,\forall\, c \in R \; c \cdot 1 = c \in I \Rightarrow I = R$.

■

Следствие. В полях нет нетривиальных идеалов ($I = \{0\}$ и $I = R$).

Определение. Пусть R — коммутативное кольцо. Тогда с некоторым набором элементов $\{r_i \mid i \in \mathcal{I}\}$ связан идеал $I = \{h_1 r_{i_1} + \ldots + h_k r_{i_k}\}$. То, что это идеал, очевидно; более того, это наименьший идеал, содержащий все элементы $\{r_i\}$. Если множество $\mathcal{I}$ конечно, то есть набор элементов $\{r_1, \ldots, r_k\}$ конечен, то I обозначают $(r_1, \ldots, r_k)$ и называют идеалом, *порождённым* $\{r_1, \ldots, r_k\}$.

Определение. Идеал I называется *главным*, если $\exists\, r \in I$: $I = (r) = \{hr \mid h \in R\}$.

Определение. Кольцо R называется *кольцом главных идеалов*, если любой идеал в R — главный.

Предложение 1. *Кольца $\mathbb{Z}$ и $F[x]$, где F — поле, — кольца главных идеалов.*

□ Идеал является, в частности, подгруппой, а мы знаем, что в $(\mathbb{Z}, +)$ все подгруппы имеют вид $k\mathbb{Z}$, $k \in \mathbb{Z}_+$. Значит, любой идеал в $\mathbb{Z}$ имеет вид (k).

Пусть $I \subseteq F[x]$ — идеал, $f \in I$, $f \neq 0$, наименьшей степени. Тогда $(f) \subseteq I$. Обратно, $\forall\, g \in I$, по теореме о делении с остатком, $g = fq + r$, где $\deg r < \deg f$ ($\deg 0 \stackrel{\text{def}}{=} -\infty$) $\Rightarrow r = g - fq \in$ $\in I \Rightarrow r = 0 \Rightarrow I = (f)$. ■

Пример. Пусть $R = F[x,y]$, $I = (x,y) = \{a_{00} + a_{10}x + a_{01}y + a_{20}x^2 + a_{11}xy + \ldots \mid a_{ij} \in F, a_{00} = 0\}$. Предположим, что I — главный идеал, то есть $\exists f \in I$: $I = (f)$. Тогда, по определению, $f \mid x$, $f \mid y \Rightarrow f = \text{const} \neq 0$. Любая ненулевая константа обратима $\Rightarrow$ по лемме 1, $I = F[x,y]$. Получившееся противоречие показывает, что I — неглавный идеал.

Пусть теперь кольцо R не обязательно коммутативно.

Определение. Кольцо (алгебра) называется *простым (-ой)*, если в нём (ней) нет нетривиальных двусторонних идеалов, то есть нет двусторонних идеалов, кроме $\{0\}$ и R.

Определение. *Центром кольца (алгебры)* называется $Z(R) \stackrel{\text{def}}{=} \{a \in R \mid ab = ba \ \forall b \in R\}$.

Центр кольца — подкольцо, но, как правило, не идеал. Центр кольца — идеал $\Leftrightarrow$ кольцо коммутативно (центр — идеал $\Leftrightarrow$ идеал содержит единицу $\Leftrightarrow$ идеал — всё кольцо $\Leftrightarrow$ кольцо коммутативно).

Определение. F-алгебра A называется *центральной*, если $Z(A) = \{\lambda \cdot 1 \mid \lambda \in F\}$.

Теорема 1. Пусть F — поле. Тогда $\text{Mat}_n(F)$ — центральная простая алгебра над F $\forall n \in \mathbb{N}$.

□ Из первого семестра известно, что если $\mathcal{AB} = \mathcal{BA}$ $\forall \mathcal{B} \in \text{Mat}_n(F)$[23], то $\mathcal{A} = \lambda\mathcal{E}$, $\lambda \in F$, что доказывает центральность.

Пусть $I \subseteq \text{Mat}_n(F)$ — двусторонний идеал, $0 \neq \mathcal{A} = \sum\limits_{i,j} a_{ij}\mathcal{E}_{ij} \in I$. Тогда $\exists k,l \in \{1,\ldots,n\}$: $a_{kl} \neq 0 \Rightarrow \mathcal{E}_{st} = a_{kl}^{-1}\mathcal{E}_{sk}\mathcal{A}\mathcal{E}_{lt} \in I$ $\forall s,t \in \{1,\ldots,n\}$. Но матричные единицы — базис $\text{Mat}_n(F)$ как векторного пространства $\Rightarrow I = \text{Mat}_n(F)$. ■

Задача. Доказать, что любая алгебра размерности n над полем F изоморфна подалгебре в $\text{Mat}_n(F)$.

Определение. Пусть $I \subseteq R$ — двусторонний идеал в кольце R. На факторгруппе по сложению R/I определим умножение: $(a+I)(b+I) \stackrel{\text{def}}{=} ab + I$. Проверим корректность такого задания умножения: если $i,j \in I$, то

$$(a+i+I)(b+j+I) = (a+i)(b+j) + I =$$
$$= ab + \underbrace{aj}_{\in I} + \underbrace{bi}_{\in I} + \underbrace{ij}_{\in I} + I = ab + I.$$

Ассоциативность и дистрибутивность очевидны, есть единица $1 + I$. Итак, задано *факторкольцо* по идеалу I.

Пример.

1. $\mathbb{Z}/(n) \cong \mathbb{Z}_n$.
2. $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$. Действительно, если $f \in \mathbb{R}[x]$, $f(x) = (x^2+1)q(x) + r(x)$, тогда $f + (x^2+1)$[24] $= r + (x^2+1)$. При этом $\deg r < \deg(x^2+1) = 2$. Перемножим теперь два некоторых класса:

[23] Все матрицы здесь обозначены буквами в особом начертании, чтобы не путать их обозначения с обозначением самой алгебры.

[24] Здесь скобки стоят уже не для обособления множителя, как в разложении выше, а для обозначения главного идеала.

$$\begin{aligned}\left(ax+b+\left(x^2+1\right)\right)\left(cx+d+\left(x^2+1\right)\right) &= acx^2+(ad+cb)\,x+bd+\left(x^2+1\right)= \\ &= ac\,(-1)+(ad+cb)\,x+bd+\left(x^2+1\right)= \\ &= (ad+cb)\,x+(bd-ac)+\left(x^2+1\right).\end{aligned}$$

При переходе от первой строки ко второй мы воспользовались тем, что факторизуем $\mathbb{R}[x]$ по (x^2+1), то есть $x^2=-1$. Но именно так перемножаются комплексные числа.

Определение. *Гомоморфизмом колец* R и S называется отображение $\varphi\colon R\to S$, являющееся гомоморфизмом абелевых групп и такое, что $\varphi(ab)=\varphi(a)\,\varphi(b)\ \forall\, a,b\in R$ и $\varphi(1)=1$.

Лемма 2. *Если φ — гомоморфизм колец, то:*

1. $\operatorname{Ker}\varphi\subseteq R$ *— двусторонний идеал.*
2. $\operatorname{Im}\varphi\subseteq R$ *— подкольцо.*

Доказательство леммы тривиально.

Пример. Если $\varphi\colon R\to S$ — гомоморфизм колец, R — поле, то φ инъективно.

□ $\operatorname{Ker}\varphi$ — идеал $\Rightarrow \operatorname{Ker}\varphi=\{0\}$. ■

Теорема (о гомоморфизме). Пусть $\varphi\colon R\to S$ — гомоморфизм колец. Тогда отображение $\psi\colon \operatorname{Im}\varphi\to {}^{R}\!/_{\operatorname{Ker}\varphi}$, $b=\varphi(a)\mapsto a+\operatorname{Ker}\varphi$, является изоморфизмом колец, то есть $\operatorname{Im}\varphi\cong {}^{R}\!/_{\operatorname{Ker}\varphi}$.

□ ψ корректно определено и является изоморфизмом абелевых групп.

Остаётся проверить сохранение умножения. Пусть $b=\varphi(a)\in\operatorname{Im}\varphi$, $d=\varphi(c)\in\operatorname{Im}\varphi$. Тогда $bd=\varphi(ac)$, $\psi(bd)=ac+\operatorname{Ker}\varphi=(a+\operatorname{Ker}\varphi)\,(c+\operatorname{Ker}\varphi)=\psi(b)\,\psi(d)$. ■

Пример.

1. $\varphi\colon \mathbb{Z}[x]\to\mathbb{Z}_p[x]$, $a_0+a_1x+\ldots+a_nx^n\mapsto \overline{a_0}+\overline{a_1}x+\ldots+\overline{a_n}x^n\Rightarrow \operatorname{Ker}\varphi=p\mathbb{Z}[x]=(p)$, $\operatorname{Im}\varphi=\mathbb{Z}_p[x]\Rightarrow \mathbb{Z}_p[x]\cong {}^{\mathbb{Z}[x]}\!/_{p\mathbb{Z}[x]}$.
2. Пусть $R=\mathcal{F}(M,F)$, где M — произвольное множество, F — поле. С каждой точкой $m\in M$ связан гомоморфизм $\varphi_m\colon R\to F$, $f\mapsto f(m)$. Тогда $\operatorname{Ker}\varphi_m=\{f\in R\mid f(m)=0\}=I_m$, $\operatorname{Im}\varphi_m=F\Rightarrow F\cong {}^{R}\!/_{I_m}$.

Предложение 2. *Пусть F — поле, $f\in F[x]$. Тогда ${}^{F[x]}\!/_{(f)}$ — поле $\Leftrightarrow$ f неприводим.*

Это предложение мы докажем на следующей лекции.

Задача. Доказать, что ${}^{F[x]}\!/_{(f)}\cong F\Leftrightarrow f$ линеен.