Часть 1. Гомоморфизмы колец

Аналогом подгрупп для колец являются подкольца, а аналогом нормальных подгрупп — идеалы.

Определение 1.1. Пусть A — произвольное кольцо. Подмножество $B \subset A$ называется подкольцом, если B — подгруппа в A относительно сложения и выполнены условия $1_A \in B$, $BB \subset B$.

Примеры 1.2.
1. Кольца $\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}$, не имеют нетривиальных подколец.
2. Кольцо $\mathbb{Z}$ является подкольцом в $\mathbb{Q}, \mathbb{R}$ и $\mathbb{C}$.
3. Кольцо R является подкольцом в кольцах $R[x]$ и $R[[x]]$.
4. Если R — коммутативное кольцо, а $f(x)$ — многочлен (формальный степенной ряд) с коэффициентами в R, то $R[f(x)]$ ($R[[f(x)]]$ соотв.) — покольцо в $R[x]$ ($R[[x]]$ соотв.).
5. Верхнетреугольные матрицы — подкольцо во всех матрицах.
6. Если A — кольцо, $S \subset A$ — подмножество, то $Z_S(A) := \{\, a \in A \mid \forall s \in S\ as = sa \,\}$ — подкольцо.
7. Если A — кольцо, то $Z(A) := Z_A(A) = \{\, a \in A \mid \forall s \in A\ as = sa \,\}$ — подкольцо (центр кольца A).

Определение 1.3. Пусть A — произвольное кольцо, а $I \subset A$ — подгруппа относительно сложения. Тогда I называется левым идеалом, если $AI \subset I$, и правым идеалом, если $IA \subset I$. Если же I является одновременно и правым и левым идеалом, то I называется двусторонним идеалом.

Двусторонние идеалы часто также называются просто идеалами.

Замечание 1.4. Заметим, что идеал (левый, правый или двусторонний) $I \subset A$ является подкольцом, только и если только $I = A$.

Замечание 1.5. Если кольцо A коммутативно, то всякий левый идеал является правым идеалом и, следовательно, двусторонним. Таким образом, в коммутативном случае все эти понятия эквивалентны.

Примеры 1.6.
1. Поле не имеет нетривиальных идеалов.
2. Всякая подгруппа (относительно сложения) в кольцах $\mathbb{Z}$ и $\mathbb{Z}/n\mathbb{Z}$ является идеалом.
3. Пусть A — кольцо и $a \in Z(A)$. Тогда $\{\, f(x) \in A[x] \mid f(a) = 0 \,\}$ — идеал.
4. Матрицы с нулевым первым столбцом образуют левый (но не правый!) идеал в кольце матриц. Аналогично, матрицы с нулевой первой строкой образуют правый (но не левый!) идеал. А нетривиальных двусторонних идеалов в кольце матриц (с коэффициентами в поле) просто нет!
5. Строго верхнетреугольные матрицы — двусторонний идеал в верхнетреугольных матрицах.
6. Если A — кольцо, $S \subset A$ — подмножество, то $AS := \{\, \sum_{i=1}^m a_i s_i \,\}$ — левый идеал, $SA := \{\, \sum_{i=1}^m s_i a_i \,\}$ — правый идеал, а $ASA := \{\, \sum_{i=1}^m a_i s_i a_i' \,\}$ — двусторонний идеал в кольце A (здесь $s_i \in S$, $a_i, a_i' \in A$). Говорят, что эти идеалы порождаются множеством S. Если же кольцо A коммутативно, то очевидно имеем $AS = SA = ASA$.

Определение 1.7. Ядром гомоморфизма колец $f : A \to B$ называется $\operatorname{Ker} f = \{\, a \in A \mid f(a) = 0 \,\}$. Образом гомоморфизма колец $f : A \to B$ называется $\operatorname{Im} f = \{\, b \in B \mid b = f(a),\ a \in A \,\}$.

Следующая лемма очевидно следует из определений.

Лемма 1.8. *Образ гомоморфизма колец $f : A \to B$ — подкольцо в B, а ядро — двусторонний идеал в A.*

Лемма 1.9. *Пусть $f : A \to B$ — гомоморфизм колец. Тогда f является мономорфизмом $\iff \operatorname{Ker} f = \{\, 0 \,\}$; f является эпиморфизмом $\iff \operatorname{Im} f = B$.*

Доказательство: аналогично утверждению о гомоморфизмах групп. □

Ясно, что всякое подкольцо $B \subset A$ является образом некоторого гомоморфизма колец. Покажем, что всякий двусторонний идеал является ядром некоторого гомоморфизма.

Пусть $I \subset A$ — идеал. Заметим, что так как аддитивная группа кольца A коммутативна, а I — подгруппа относительно сложения, то I — нормальная подгруппа, следовательно A/I является абелевой группой относительно операции сложения, заданной формулой

$$(a+I)+(b+I)=(a+b)+I. \tag{1.10}$$

Определим операцию умножения на классах смежности A/I следующим образом:

$$(a+I)(b+I) := ab+I. \tag{1.11}$$

Лемма 1.12. *Операция умножения* (1.11) *на A/I корректно определена.*

Доказательство: допустим $a'+I=a+I$, $b'+I=b+I$. Тогда $a'=a+m$, $b'=b+n$, $m,n\in I$. Следовательно $a'b'=(a+m)(b+n)=ab+mb+an+mn$, причем $mb\in IA\subset I$, $an\in AI\subset I$, $mn\in II\subset I$, следовательно $mb+an+mn\in I$ и $ab+I=a'b'+I$. □

Теорема 1.13. *Множество A/I с операциями сложения и умножения, заданными формулами* (1.10) *и* (1.11) *соотв. является кольцом. Более того, проекция $f: A\to A/I$, $a\mapsto a+I$ является эпиморфизмом колец, причем $\operatorname{Ker} f = I$.*

Доказательство: во-первых, A/I является абелевой группой относительно сложения по теореме о фактор-группе. Во-вторых, A/I является моноидом относительно умножения:

$$((a+I)(b+I))(c+I)=(ab+I)(c+I)=(ab)c+I=a(bc)+I=(a+I)(bc+I)=(a+I)((b+I)(c+I)),$$
$$(a+I)(1+I)=a\cdot 1+I=a+I, \quad (1+I)(a+I)=1\cdot a+I=a+I.$$

Наконец, умножение в A/I дистрибутивно:

$$((a+I)+(b+I))(c+I)=((a+b)+I)(c+I)=(a+b)c+I=(ac+bc)+I=(ac+I)+(bc+I)=(a+I)(c+I)+(b+I)(c+I).$$

Вторая часть теоремы очевидна. □

Кольцо A/I называется **факторкольцом** кольца A по идеалу I. Кольцо $\mathbb{Z}/n\mathbb{Z}$ является примером факторкольца.

Теорема 1.14. *Пусть $f: A\to B$ — гомоморфизм колец. Тогда $A/\operatorname{Ker} f\cong \operatorname{Im} f$* (канонический изоморфизм)*.*

Доказательство: пусть $I=\operatorname{Ker} f$. Определим отображение $\bar f: A/I\to \operatorname{Im} f$ формулой $\bar f(a+I)=f(a)$. Далее очевидно. □

Следствие 1.15. (*i*) *Если $f: A\to B$ — эпиморфизм колец, то $B\cong A/\operatorname{Ker} f$.* (*ii*) *Всякий гомоморфизм колец $f: A\to B$ раскладывается в композицию канонических эпиморфизма, изоморфизма и мономорфизма $A\to A/\operatorname{Ker} f\to \operatorname{Im} f\to B$.*

Часть 2. Модули

Определение 2.1. **Левым модулем** над кольцом A (или левым A-модулем) называется абелева группа M, на которой задано **линейное действие** кольца A, то есть отображение $A\times M\to M$, $(a,m)\mapsto am$, такое что

$$(ab)m=a(bm), \qquad 1m=m,$$
$$(a+b)m=am+bm, \qquad a(m+n)=am+an.$$

Аналогично определяются правые A-модули.

Примеры 2.2. 1. Всякая абелева группа является $\mathbb{Z}$-модулем.

2. Если A — кольцо, то всякий левый идеал является левым A-модулем, а всякий правый идеал — правым A-модулем. В частности, само кольцо A является модулем над собой.
3. Матрицы размера $n\times m$ являются левым модулем над кольцом матриц размера $n\times n$ и правым модулем над кольцом матриц размера $m\times m$.
4. Если U и V— абелевы группы, то множество $\operatorname{Hom}(U,V)$ гомоморфизмов из U в V является левым модулем над кольцом $\operatorname{End}(V)$ и правым модулем над кольцом $\operatorname{End}(U)$.
5. Пусть M и N — A-модули. Тогда правило $a(m,n)=(am,an)$ задает на прямом произведени абелевых групп $M\times N$ структуру A-модуля. Этот A-модуль называется **прямой суммой** модулей M и N и обозначается $M\oplus N$.

6. Пусть $\{ M_i \}_{i \in I}$ — произвольное семейство A-модулей. Тогда множество всех наборов $\{ (m_i)_{i\in I} \}$, где $m_i \in M_i$ и во всяком наборе $\{ (m_i) \}$ все элементы кроме конечного числа равны нулю, является A-модулем относительно действия $a(m_i) = (am_i)$. Этот A-модуль называется прямой суммой A-модулей M_i и обозначается $\bigoplus_{i\in I} M_i$.
7. Прямая сумма (конечная или бесконечная) A-модулей A называется свободным A-модулем.

Замечание 2.3. Если кольцо A коммутативно, то всякий левый A-модуль является правым A-модулем и наоборот.

Упражнение 2.4. Пусть M — левый A-модуль. Покажите, что $\forall a \in A$, $m \in M$ имеем $0m = 0$, $a0 = 0$, $(-a)m = -am$.

Лемма 2.5. *Структуры A-модуля на абелевой группе M находятся в биекции с гомоморфизмами колец $A \to \mathrm{End}(M)$.*

Доказательство: пусть M — A-модуль. Всякому элементу $a \in A$ сопоставим отображение $\rho(a) : M \to M$, $m \mapsto am$. Легко видеть, что $\rho(a) \in \mathrm{End}(M)$, и что $\rho : A \to \mathrm{End}(M)$ — гомоморфизм колец. Обратно, пусть $\rho : A \to \mathrm{End}(M)$ — гомоморфизм колец. Тогда ясно, что M является A-модулем относительно действия $am := \rho(a)(m)$. □

Пусть M — левый A-модуль. Абелева подгруппа $N \subset M$ называется A-подмодулем, если $AN \subset N$. Аналогично определяются подмодули в правых модулях.

Пусть M-левый A-модуль, а $S \subset M$ — произвольное подмножество его элементов. Тогда множество $AS := \{ \sum_{s\in S} a_s s \} \subset M$, где $a_s \in A$ и во всякой сумме все слагаемые кроме конечного числа равны нулю, является подмодулем. Если $AS = M$, то говорят, что S является множеством образующих для модуля M, или что A-модуль M порождается множеством S. Если у модуля M существует конечное множество образующих, то M называется конечно порожденным.

Определение 2.6. Подмножество $S \subset M$ называется линейно независимым, если $\sum_{s\in S} a_s s = 0 \Longrightarrow \forall s\ a_s = 0$. Множество образующих S называется базисом, если оно линейно независимо.

Лемма 2.7. *Если S — базис в M, то всякий элемент модуля M единственным образом представляется в виде суммы $\sum_{s\in S} a_s s$, в которой все слагаемые кроме конечного числа равны нулю.*

Доказательство: существование такого представления вытекает из того, что S-множество образующих, так что остается проверить единственность. Пусть $\sum_{s\in S} a_s s = \sum_{s\in S} b_s s$. Тогда $\sum_{s\in S}(a_s - b_s)s = 0$, следовательно $a_s = b_s$ при всех $s \in S$ в силу линейной независимости. □

Пусть M и N — A-модули. Гомоморфизм абелевых групп $f : M \to N$ называется гомоморфизмом A-модулей, если $f(am) = af(m)$ для всех $a \in A$, $m \in M$. Гомоморфизм A-модулей называется моно(эпи, изо, эндо, авто)морфизмом, если он является моно(эпи, изо, эндо, авто)морфизмом абелевых групп. Множество всех гомоморфизмов A-модулей $M \to N$ обозначается $\mathrm{Hom}_A(M, N)$, а множество всех эндоморфизмов A-модуля M обозначается $\mathrm{End}_A(M)$.

Теорема 2.8. *A-модуль M обладает базисом $\Longleftrightarrow$ M изоморфен свободному A-модулю.*

Доказательство: Пусть $M = \bigoplus_{i\in I} A$. Пусть $s_i \in M$ — элемент, все координаты кроме i-ой которого равны 0, а i-ая координата равна 1. Тогда легко видеть, что $S = \{ s_i \}_{i\in I}$ — базис в M. Обратно, пусть M — произвольный A-модуль с базисом S. Докажем, что он изоморфен прямой сумме $\bigoplus_{s\in S} A$. Определим отображение $f : \bigoplus_{s\in S} A \to M$ правилом $(a_s)_{s\in S} \mapsto \sum_{s\in S} a_s s$. Легко проверить, что f — гомоморфизм A-модулей, а из леммы 2.7 следует, что f — изоморфизм. □

Легко видеть, что множество $\mathrm{Hom}_A(M, N)$ является абелевой группой относительно операции поточечного сложения $(f + g)(m) = f(m) + g(m)$. Если же кольцо A-коммутативно, то множество $\mathrm{Hom}_A(M, N)$ обладает также структурой A-модуля относительно операций $(af)(m) = a(f(m))$. Действительно,

$$(af)(bm) = af(bm) = abf(m) = baf(m) = b(af)(m),$$

поэтому af является гомоморфизмом A-модулей, а остальные условия проверяются элементарно.