2. Вторая лекция, 9 апреля 2014 г.

2.1. **Максимальные и простые идеалы.**

Определение 2.1. Идеал $\mathfrak{m} \subset A$ называется максимальным, если он не содержится ни в каком большем идеале (не совпадающем со всем кольцом).

Определение 2.2. Идеал $\mathfrak{p} \subset A$ называется простым, если для любых двух элементов $a, b \in A$, таких, что $ab \in \mathfrak{p}$, верно, что либо $a \in \mathfrak{p}$, либо $b \in \mathfrak{p}$.

Пример 2.3. Простые идеалы в $\mathbb{Z}$ — это идеалы вида (p), где p простое. Они же являются и максимальными (проверьте это!).

Предложение 2.4. *1) Идеал $\mathfrak{p}$ прост тогда и только тогда, когда $A/\mathfrak{p}$ — область целостности.*
2) Идеал $\mathfrak{m}$ максимален тогда и только тогда, когда $A/\mathfrak{m}$ — поле.

Доказательство. 1) Пусть $\mathfrak{p}$ прост, $ab \in \mathfrak{p}$. Значит, a или b лежат в $\mathfrak{p}$. Рассмотрим их образы при отображении факторизации $A \to A/\mathfrak{p}$. Получим, что из $[ab] = [0]$ следует, что $[a] = [0]$ или $[b] = [0]$, что и означает, что $A/\mathfrak{p}$ целостное. Обратное утверждение доказывается точно так же.

2) Пусть $\mathfrak{m}$ максимален. Докажем, что всякий ненулевой элемент $[a] \in A/\mathfrak{m}$ обратим. Действительно, $a \notin \mathfrak{m}$. Рассмотрим идеал $a + \mathfrak{m} = \{ax + m \mid x \in A, m \in \mathfrak{m}\}$. Этот идеал содержит $\mathfrak{m}$ и не совпадает с ним (поскольку содержит ещё и a), значит, он совпадает со всем кольцом. Поэтому $1 = ax + m$ для некоторых $x \in A$,$m \in \mathfrak{m}$. Получаем, что в $A/\mathfrak{m}$ элемент $[x]$ есть $[a]^{-1}$, так как $[1] = [a][x] + [m] = [a][x]$. Обратное утверждение доказывается аналогично (проделайте это!). □

Следствие 2.5. *Всякий максимальный идеал прост.*

Упражнение 2.6. Приведите пример простого, но не максимального идеала.

Оказывается, что в кольцах главных идеалов верно и обратное к следствию 2.5. Это вытекает из следующей теоремы.

Теорема 2.7. *Пусть A — кольцо главных идеалов, $u \in A$ — необратимый элемент. Тогда $A/(u)$ является полем тогда и только тогда, когда u прост.*

Доказательство. Пусть u не прост: $u = vw$, где v и w необратимы. Тогда в $A/(u)$ получаем: $[v][w] = [u] = [0]$, причём $[v] \neq [0]$ и $[w] \neq [0]$ — значит, $A/(u)$ не область целостности, и тем более не поле.

Обратно, пусть u прост. Это значит, что для любого $x \notin (u)$ верно, что $(x, u) = 1$, следовательно, найдутся a и b, для которых $ax + bu = 1$. Значит, в $A/(u)$ получаем, что $[a][x] = [1]$, т.е. $[a]$ обратим. □

2.2. **Модули над кольцами: определение.** Как известно, векторное пространство — это множество V, снабжённое двумя операциями: сложением (относительно которого оно является абелевой группой) и умножением на элементы фиксированного поля $\mathbb{K}$. Что будет, если попробовать заменить в этом определении поле $\mathbb{K}$ на произвольное кольцо?

Например, всякая абелева группа является "векторным пространством над $\mathbb{Z}$": действительно: её элементы можно складывать между собой, а также умножать на целые числа по правилу $n \cdot g = g + \cdots + g$ (всего n слагаемых, с очевидными изменениями, если $n < 0$). Это мотивирует следующее

Определение 2.8. Пусть A — коммутативное ассоциативное кольцо с единицей. *Модуль* над кольцом A (или A-*модуль*) — это абелева группа, снабжённая действием кольца A, т.е. операцией $A \times M \to M$, удовлетворяющей следующим условиям:

(M1): $(ab)m = a(bm)$ для любых $a, b \in A$, $m \in M$;
(M2): $1 \cdot m = m$ для любого $m \in M$;
(D1): $(a + b)m = am + bm$ для любых $a, b \in A$, $m \in M$;
(D2): $a(m + n) = am + an$ для любых $a \in A$, $m, n \in M$.

Пример 2.9. Если $A = \mathbb{K}$ — поле, то M есть не что иное, как векторное пространство над $\mathbb{K}$.

Пример 2.10. Если $A = \mathbb{Z}$, то M — это просто абелева группа.

Пример 2.11 (очень важный!)**.** Пусть $A = \mathbb{K}[x]$, V — векторное пространство над $\mathbb{K}$, $\mathcal{A} \in \mathrm{End}(V)$ — линейный оператор на V. Тогда V является $\mathbb{K}[x]$-модулем, на котором действие кольца многочленов задано так:

$$(a_n x^n + \cdots + a_1 x + a_0) \cdot v = a_n \mathcal{A}^n v + \cdots + a_1 \mathcal{A} v + a_0 v.$$

Иными словами, x действует на V при помощи оператора $\mathcal{A}$. Отметим, что разные линейные операторы задают *разные* структуры модуля на V.

Пример 2.12. Всякое кольцо A является модулем над самим собой. Аксиомы (M1), (M2), (D1) и (D2) при этом следуют из определения кольца.

2.3. **Подмодули, фактормодули, гомоморфизмы.**

Определение 2.13. Пусть M — модуль над A. $N \subset M$ называется *подмодулем* в M, если $n + n' \in N$ и $an \in N$ для любых $a \in A$ и $n, n' \in N$.

Пример 2.14. Подмодули модулей из примеров 2.9 и 2.10 — это векторное подпространство и абелева подгруппа соответственно.

Пример 2.15. Подмодуль модуля из примера 2.11 — это *$\mathcal{A}$-инвариантное* подпространство $U \subset V$ (т.е. такое подпространство, для которого $\mathcal{A}u \in U$ для любого $u \in U$).

Пример 2.16. Подмодуль модуля из примера 2.12 — это идеал $I \subset A$.

По подмодулям можно брать факторы.

Определение 2.17. Пусть $N \in M$ — подмодуль. Рассмотрим отношение эквивалентности на M: $m \equiv m' \mod N$, если $m - m' \in N$. Множество классов эквивалентности $m + N = [m]$ называется *фактормодулем* и обозначается через M/N. Операции на M/N задаются обычным образом:

$$(m + N) + (n + N) = (m + n) + N; \qquad a(m + N) = am + N.$$

Упражнение 2.18. Проведите сами все необходимые проверки корректности.

Пример 2.19. Пусть A — кольцо, $I \subset A$ — идеал. Тогда A/I тоже является A-модулем.

Определение 2.20. Отображение A-модулей $f\colon M \to N$ называется *гомоморфизмом*, если

$$f(x + y) = f(x) + f(y); \qquad f(ax) = af(x)$$

для любых $x, y \in M$, $a \in A$.

Упражнение 2.21. Проверьте, что $\operatorname{Ker} f$ и $\operatorname{Im} f$ — подмодули в M и N соответственно.

Пример 2.22. Пусть $N \subset M$ — модуль и подмодуль. Отображение

$$\pi\colon M \to M/N, \qquad m \mapsto m + N$$

является сюръективным гомоморфизмом (=эпиморфизмом). Оно называется *эпиморфизмом факторизации*.

Соответственно, имеется и теорема о гомоморфизме:

Теорема 2.23 (о гомоморфизме модулей)**.** *Пусть $f\colon M \to N$ — гомоморфизм A-модулей. Тогда $\operatorname{Im} f \simeq M/\operatorname{Ker} f$. Более точно, отображение $\varphi\colon \operatorname{Im} f \to M/\operatorname{Ker} f$, при котором $b = f(a) \in \operatorname{Im} f$ отображается в $\pi(a) = a + \operatorname{Ker} f$, есть изоморфизм.*

Доказательство. Докажите эту теорему сами. □

2.4. **Системы порождающих. Конечно порождённые модули.** Пусть M — A-модуль, $S \subset M$ — произвольное подмножество. Рассмотрим *наименьший* подмодуль в M, содержащий S. Это

$$\langle S \rangle = \{a_1x_1 + \cdots + a_sx_s \mid x_i \in S, a_i \in A\}.$$

Если $\langle S \rangle = M$, то S называют *системой порождающих* модуля M. Если M допускает конечную систему порождающих, то он называется *конечно порождённым*.

Пример 2.24. $\mathbb{Q}$ как $\mathbb{Z}$-модуль не является конечно порождённым.

Пример 2.25. Конечно порождённые $\mathbb{K}$-модули — это в точности конечномерные векторные пространства.

E-mail address: esmirnov@hse.ru