Полугруппа и группа идеалов нетерова кольца

Пусть A — дедекиндово кольцо. Рассмотрим в кольце A два идеала: b и a. Предположим, что идеал a содержит идеал b. (В таком случае говорят, что b *делится на* a и пишут: $a|b$.) Тогда, как впервые показал Ван дер Варден, существует такой идеал c, что $ac = b$.

Назовем это нетривиальное утверждение *леммой Ван дер Вардена.* Ее виртуозное элементарное доказательство можно найти в знаменитой книге Ван дер Вардена "Алгебра". Мы ограничимся тем, что в Дополнении 1 докажем эту лемму в частном случае: когда A — дедекиндово кольцо целых поля алгебраических чисел K.

А пока, считая лемму доказанной, извлечем из нее полезные следствия.
Прежде всего докажем, что идеал c, о котором идет речь в лемме, однозначен. Точнее,

> *Лемма 1.* Пусть $b < a$. Кроме тривиального случая $a = b = 0$ идеал c, такой, что $ac = b$, определен однозначно.

Доказательство. В самом деле, пусть $ac = ac'$. Выберем ненулевой главный идеал $a_0A < a$. По лемме Ван дер Вардена, $a_0A = qa$ для некоторого идеала $q < A$. Но тогда $a_0Ac = qac = qac' = a_0Ac'$ или $a_0c = a_0c'$. Отсюда следует, что $c = c'$ (почему?) □

Из Леммы 1 мы выведем следующее важное утверждение.

> *Лемма 2.* Любой ненулевой идеал a дедекиндова кольца A однозначно представляется в виде произведения максимальных (читай, простых) идеалов.

Доказательство. Если идеал a максимален, то доказывать нечего. В противном случае, пусть $a \in m_1$, где m_1 — максимальный идеал. По лемме Ван дер Вардена $a = m_1a_1$ для некоторого идеала a_1. Затем, аналогично, $a_1 = m_2a_2$ и так далее. Так как $a < a_1 < a_2 \dots$ (почему?), то эта последовательность стабилизируется в силу нетеровости A. В итоге получаем разложение вида $a = m_1m_2 \dots m_k$ (не утверждается, что все m_i различны!). Докажем его однозначность (с точностью до перестановки множителей).

Действительно, если $m_1 \dots m_k = m'_1 \dots m'_\ell$, то $m'_1 \dots m'_\ell < m_1$ (почему?); пользуясь простотой m_1, получаем, что m_1 содержит один из идеалов m'_i, а потому с ним совпадает. Далее применяется индукция по $(k + \ell)$ и лемма 1 (восстановите конец доказательства). □

Лемма 2 означает, что абелева полугруппа (с единицей) по умножению ненулевых идеалов дедекиндового кольца A обладает свойством однозначного разложения на неразложимые множители (простые идеалы).

Разумеется, абелеву полугруппу с сокращением можно, следуя известной из теории групп конструкции, вложить в абелеву группу. Но можно поступить интереснее.

> *Определение.* Два ненулевых идеала a и b дедекиндового кольца A назовем *эквивалентными* ($a \sim b$), если найдутся такие ненулевые элементы x и y кольца A, что $xa = yb$.

Убедимся, что множество $\mathcal{C}\ell(A)$ классов эквивалентных идеалов образует абелеву группу по умножению.

Контрольный вопрос: что служит единицей в группе $\mathcal{C}\ell(A)$?

Не совсем понятно только существование обратного элемента: пусть (a) — класс ненулевого идеала a. Выберем в A ненулевой главный идеал $a_0A < a$. По лемме Ван дер Вардена существует такой идеал a^{-1}, что $aa^{-1} = a_0A$. Это означает, что $(a)(a^{-1}) = 1$ в группе $\mathcal{C}\ell(A)$.

Замечание. Эквивалентность дивизоров можно определить и так: $a \sim b$, если A-модули a и b изоморфны.
В самом деле, пусть $\varphi : a \longrightarrow b$ — изоморфизм A-модулей. Выберем ненулевой элемент $a_0 \in a$ и заметим, что с одной стороны, $\varphi(a_0a) = a_0\varphi(a)$, а с другой — $\varphi(a_0a) = \varphi(a_0)a$. Следовательно, $a_0b = \varphi(a_0)a$ и $a \sim b$ в смысле первого определения.

> *Упражнение.* Доказать, что если $(a) = (b)$ (в смысле первого определения), то A-модули a и b изоморфны.

Про группу классов $\mathcal{C}\ell(O_K)$ кольца целых O_K поля алгебраических чисел K известно, что она всегда конечна* (см. дополнение 2). Тривиальность группы $\mathcal{C}\ell(O_K)$ означает, что O_K — кольцо главных идеалов.

Замечания.

1) Даже в случае квадратичных расширений поля $\mathbb{Q}$ (т.е. расширений степени два) структура группы классов дивизоров изучена слабо, хотя и здесь имеются яркие результаты. Например, доказано, что существует всего 9 мнимых квадратичных расширений $K = \mathbb{Q}(\sqrt{m})$ с тривиальной группой классов: $m = -1, -2, -3, -7, -11, -19, -43, -67, -163$.

2) Группа $\mathcal{C}\ell(O_{\sqrt{-5}}) \simeq \mathbb{Z}_2$, а $\mathcal{C}\ell(O_{\sqrt{-23}}) \simeq \mathbb{Z}_3$.

3) Для положительных m еще Гаусс предположил, что $\mathcal{C}\ell(\mathbb{Q}(\sqrt{m}))$ равен 1 для бесконечно многих m, но до сих пор его гипотеза не доказана.

Продолжим изучение идеалов в дедекиндовых кольцах.

> *Лемма 3.* Для любого ненулевого идеала a дедекиндова кольца A факторкольцо A/a является кольцом главных идеалов (возможно, с делителями нуля!).

Доказательство. Пусть $x \mapsto \overline{x}, x \in A$ — каноническая проекция из A в A/a. Если $a = m_1^{e_1} \dots m_\ell^{e_\ell}$, то идеал a содержится в максимальных идеалах $m_1, \dots m_\ell$ и только в них (почему?). Поэтому в факторкольце A/a имеется лишь конечное число максимальных идеалов $\overline{m_1}, \dots, \overline{m_\ell}$.

*Концептуальное доказательство более общего утверждения можно найти, например, в книге И.Р.Шафаревича и З.И. Боревича *Теория чисел.*.

Более того, если $b|a$ (т.е. $a < b$), то $b = m_1^{f_1} \dots m_\ell^{f_\ell}$, причем $f_i \leqslant \ell_i$ (единственность разложения на множители). Следовательно, $\overline{b} = \overline{m_1}^{f_1}, \dots, \overline{m_\ell}^{f_\ell}$. Поэтому достаточно доказать, что идеал $\overline{m_1} = m_1(\mod a)$ является главным в факторкольце A/a. Для этого используем Великую Китайскую Идею (ВКИ). Прежде всего убедимся, что идеалы $m_i^{q_i}$ и $m_j^{q_j}$, $i \neq j$ взаимно просты: в самом деле, пусть $m_i^{q_i} + m_j^{q_j} \neq A$. Тогда существует максимальный идеал m, содержащий их сумму. Но в силу единственности разложения на простые (максимальные) множители m должен совпадать с m_i (т.к. ${m_i}^{q_i} \in m$) и одновременно с m_j (по той же причине). Противоречие.

Выберем теперь такой элемент $w \in m_1$, что $w \notin m_1^2$. Тогда, согласно ВКИ, существует такой элемент $y \in A$, что

$$\begin{aligned} y &\equiv w \mod m_1^2 \\ y &\equiv 1 \mod m_i, \;\; i = 2, \dots, \ell. \end{aligned}$$

Ясно, что идеал $a + yA$ содержится в идеале m_1, но не в m_1^2, и не содержится ни в одном из идеалов m_i. Но тогда $a + yA = m_1$ (почему?). Это показывает, что $\overline{m_1} = \overline{y}\overline{A}$, т.е. $\overline{m_1}$ — главный идеал факторкольца A/a. Теперь лемма полностью доказана. □

Дополнение 1.

Лемма Ван дер Вардена. Пусть O — кольцо целых поля алгебраических чисел K, a и b — его идеалы и $a|b$ (т.е. $b < a$). Тогда существует такой идеал $c < O$, что $ac = b$.

Доказательство.
На первом его этапе проделаем некоторую подготовительную работу. Рассмотрим множество $a^{-1} = \{x \in K \mid xa < O\}$. Легко проверить (сделайте это), что

а) множество a^{-1} является O-модулем;

б) $a^{-1} \geqslant O$;

в) a^{-1} — конечный $\mathbb{Z}$-модуль, а точнее решетка в K полного ранга. (Обратите внимание на то, что a^{-1} хотя и является O-модулем, но идеалом не является: если a — собственный идеал в O, то a^{-1} строго содержит O (почему?). O-модуль a^{-1} называется *дробным идеалом.*)

Докажем, что $a^{-1}a = O$.
Рассмотрим O-модуль $t = a^{-1}a$. Модуль t является идеалом.
В самом деле, $a^{-1}a < O$ и $Oa^{-1}a = Oaa^{-1} = aa^{-1}$.

Докажем, что $t = O$. Для этого выберем элемент $\alpha \in t^{-1}$. По определению, $\alpha a^{-1}a < O$, то есть $\alpha a^{-1} < a^{-1}$. Но a^{-1} — конечный $\mathbb{Z}$-модуль. Следовательно, элемент α цел над $\mathbb{Z}$. Значит, $\alpha \in O$. Итак, мы показали, что $O < t^{-1} < O$, то есть $t^{-1} = O$ и $t = O$ (почему?). Подготовительная работа закончена.

Рассмотрим O-модуль $c = a^{-1}b$. Ясно, что

а) $c < O$;

б) c — идеал;

в) $ac = aa^{-1}b = Ob = b$.$\square$

Дополнение 2.

Следуя одной важной идее Гурвица, докажем, что $|\mathcal{C}\!\ell(O)| < \infty$. Этот факт можно вывести элементарно из следующей леммы.

> *Лемма Гурвица о приближении.* Пусть O — решетка целых в поле K. Существует такое натуральное M (зависящее только от поля K), что для любого $x \in K$ существуют такие t, $0 < t \leqslant M$ и $\alpha \in O$, что
>
> $$|N(tx - \alpha)| < 1.$$

Замечание. Мы знаем. что $tx \in O$ для некоторого натурального t, но ограниченное множество таких t не может "обслуживать" все элементы поля K. Оказывается, что если мы ослабим наши требования: tx не обязательно попадает в решетку O, но находится недалеко от какой-то ее точки, то такому требованию для любого x можно удовлетворить с помощью конечного набора t.

Отложим на время доказательство леммы и выведем из нее нужное утверждение о конечности группы классов. Пусть I — идеал в O. Рассмотрим в I ненулевой элемент y с наименьшим значением $|N(y)|$, и пусть x — любой элемент из O. По лемме Гурвица для некоторого натурального t, $0 < t < M$ и некоторого $\alpha \in O$ имеем $|N(t\dfrac{x}{y} - \alpha)| < 1$ или $|N(tx - \alpha y)| < N(y)$.

Так как элемент $tx - \alpha y$ лежит в I, то $tx - \alpha y = 0$ ввиду выбора элемента y из I. Следовательно, $M!I < yO$ или $M!I\dfrac{1}{y} < O$. Но идеал $M!I\dfrac{1}{y}$ содержит главный идеал $M!O$ (почему?). А в дедекиндовом кольце имеется лишь конечное число идеалов, содержащих данный. Следовательно, среди идеалов, эквивалентных I, можно выбрать представителя из конечного множества идеалов, содержащих идеал $M!O$. Это показывает, что группа $\mathcal{C}\!\ell(O)$ конечна.

Набросок доказательства леммы Гурвица. Рассмотрим n-мерную $\mathbb{Z}$-решетку O в евклидовом пространстве $V = K \otimes \mathbb{R}$. Пусть $x \in K$. Тор $T = V/O$ компактен. Разобьем его на S "мелких" кусочков, евклидов диаметр каждого из которых < 1. Положим $M = S + 1$ и рассмотрим N точек $\{tx\}$, $t = 1, \ldots, N$ в пространстве V и их проекции $\{t\overline{x}\}$ на тор T. По принципу Дирихле какие-то две из наших точек $t_1\overline{x}$ и $t_2\overline{x}$ попадут в один "мелкий" кусочек. Но это значит, что $|(t_1 - t_2)x - \alpha| < 1$ для некоторого вектора α из решетки O (почему?).

Контрольный вопрос. Как в этом доказательстве заменить евклидово расстояние на расстояние в смысле функции N?

Проективные модули

Определения

Часто требуется построить отображение, представленное на коммутативной диаграмме:

$$\begin{tikzcd} & P \arrow[dl, "?"'] \arrow[d, "\varphi"] & \\ M' \arrow[r, "i"] & M \arrow[r, "j"] & 0 \end{tikzcd}$$

где M', M и P — модули над кольцом A, вертикальная и горизонтальные стрелки — заданные отображения, а наклонная стрелка со знаком ? показывает отображение, которое мы хотим найти (разумеется, все отображения суть морфизмы A-модулей).

Определение. Модуль P называется *проективным*, если эта проблема разрешима, при условии, что строка $M' \xrightarrow{i} M \xrightarrow{j} 0$ точна, т.е. $\operatorname{Im} i = M$.
Упражнение 1. Свободный модуль проективен.
(Напомним, что A-модуль называется свободным, если он обладает базисом.)

Другими словами, модуль P проективен, если для любого эпиморфизма $i : M' \to M$ и любого гомоморфизма $\varphi : P \to M$ существует такой гомоморфизм $? : P \to M'$, что $i\circ ? = \varphi$.

Есть и другие, не менее полезные, характеризации проективности.

Утверждение 1. Следующие условия на A-модуль P эквивалентны:

а) модуль P проективен;

б) всякая точная последовательность вида $0 \to M' \to M \to P \to 0$ расщепляется, или, по-другому, если $M/M' = P$, то $M = M' \oplus P$;

в) модуль P есть прямое слагаемое свободного модуля;

г) существуют такие элементы $e_i \in P$ и $f_i \in \operatorname{Hom}_A(P, A)$, что для любого $x \in P$

$$x = \sum f_i(x)e_i, \quad \text{где почти все} f_i(x) = 0.$$

(Эквивалентность условий а), б), в) была сформулирована в виде задач одного из "Листочков".)

Покажем, что из в) следует г). В самом деле, пусть P — прямое слагаемое свободного модуля S с базисом $\{s_i\}$. Рассмотрим проекцию $\pi : S \to P$ модуля S на прямое слагаемое P. По определению, любой элемент x из P однозначно представим в виде $x = \sum f_i(x)s_i$, где почти все $f_i(x)$ равны 0, а $f_i \in \operatorname{Hom}_A(P, A)$ (почему?).

Проецируя обе части этого равенства на P, получаем, что $x = \sum f_i(x)\pi(s_i)$. Это и есть утверждение г) с $e_i = \pi(s_i)$.

Покажем, что из г) следует в). В самом деле, пусть S — свободный A-модуль с базисом $\{s_i\}$. Рассмотрим два гомоморфизма A-модулей $\pi_1 : S \to P$ и $\pi_2 : P \to S$, заданных формулами: $\sum a_i s_i \overset{\pi_1}{\mapsto} \sum a_i e_i$ и $\sum f_i(x)e_i \overset{\pi_2}{\mapsto} \sum f_i(x)s_i$. Проверьте, что π_i — гомоморфизмы и что $\pi_1 \circ \pi_2 = \mathrm{id}$. Следовательно, $S = \operatorname{Ker}\pi_1 \oplus P$ (почему?).

Примеры проективных модулей

1) Пусть $e \in A$ — идемпотент кольца A, т.е. $e^2 = e$. Тогда умножение на элемент e есть оператор проецирования кольца A на его прямое слагаемое eA. Таким образом, идеал eA является проективным A-модулем (в кольце с нетривиальным идемпотентом есть делители нуля!).

2) Пусть A — дедекиндово кольцо с полем частных $R(A) = K$. Как мы знаем, любой ненулевой идеал $I \subset A$ обратим в том смысле, что существует такой A-модуль I^{-1}, что $II^{-1} = A$ (напомним, что $I^{-1} = \{x \in K \mid xI \subset A\}$) (без ущерба для понимания можно считать, что A — кольцо целых поля алгебраических чисел K). В частности, $1 = \sum f_i e_i$, где $e_i \in I$, а $f_i \in I^{-1} \subset K$. Но тогда $x = \sum (f_i x) e_i$, $x \in I$, и проективность идеала I обнаружена нами в виде условия г) с $f_i(x) = f_i x \subset A$ (!).

Таким образом, идеалы дедекиндова кольца суть проективные модули, и даже конечные проективные модули.

Отступление. Ввиду важности сделанного утверждения приведем его доказательство, не использующее обратимость ненулевого идеала I. Возьмем ненулевой элемент $i_0 \in I$. Тогда $i_0 A \subset I$ и, следовательно, $i_0 A = JI$ для некоторого идеала $J < A$ (ВдВ-теорема). Это равенство означает, что $i_0 = i_1 j_1 + \dots + i_\ell j_\ell$, где $i_k \in I$, а $j_s \in J$. Определим морфизмы A-модулей $I \to A^\ell$ и $A^\ell \to I$ формулами

$$i \mapsto (ij_1/i_0, \dots, ij_\ell/i_0), \;\; i \in I$$
$$(a_1, \dots, a_\ell) \mapsto a_1 i_1 + \cdots a_\ell i_\ell$$

Проверьте, что композиция указанных морфизмов тождественна на идеале I, что показывает его проективность и конечность.

Развивая успех, получим наше главное утверждение.

> *Теорема.* Любой конечный проективный модуль P над дедекиндовым кольцом A изоморфен прямой сумме идеалов, т.е.
>
> $$P \simeq I_1 \oplus I_2 \oplus \ldots \oplus I_s$$

Доказательство. Любой конечный проективный модуль P погружается в конечный свободный модуль A^k для некоторого k (задача из листочка!). Проекция P на k-тое слагаемое прямой суммы $A \oplus \cdots \oplus A$ — это гомоморфизм A-модулей $\varphi : P \to A$, ядро которого $\operatorname{Ker}\varphi$ лежит в A^{k-1}, а образ $\varphi(P)$ есть идеал $I_k < A$ (почему?). Следовательно, $P \simeq \operatorname{Ker}\varphi \oplus I_k$, и доказательство завершается с помощью индукции по k. □

Замечание. В доказательстве мы не использовали тот факт, что P вложено в A^k в виде прямого слагаемого. Любой конечный модуль M без кручения[†] можно погрузить в конечный свободный модуль (как?). Тогда наше рассуждение показывает, что конечный модуль без кручения над дедекиндовым кольцом есть прямая сумма идеалов. Следовательно, над дедекиндовыми кольцами нет разницы между конечными модулями без кручения и конечными проективными модулями (возможно, это еще раз убедит вас в естественности дедекиндовых колец).

[†]Говорят, что в A-модуле M *есть кручение*, если существует такой ненулевой элемент a кольца и такой ненулевой элемент m модуля, что $am = 0$.

Упражнение. Мы видели, что любой идеал кольца $O_{\sqrt{-5}}$ проективен. А когда он свободен?
Объясните, почему в кольце $O_{\sqrt{-5}}$ можно встретить проективные, но не свободные идеалы. Приведите пример такого идеала.

Проективные модули и расслоения

Пусть X — топологическое пространство, а k — поле вещественных или комплексных чисел. Семейство V векторных пространств с базой X определяется заданием

1) конечномерного векторного пространства V_x над полем k для каждой точки $x \in X$ (слой семейства над x)

2) топологии на несвязном объединении $V = \bigsqcup V_x$, которая индуцирует естественную топологию на каждом V_x и делает непрерывной естетственную проекцию $p : V \to X$.

   Сечением семейства $p : V \to X$ называется такое непрерывное отображение $s : X \to V$, что $ps(x) = x$ для всех $x \in X$.

Пример. Пусть W — векторное пространство. Семейство $V = X \times W$ с проекцией $p : V \to X$ на первый сомножитель называется *тривиальным семейством.* Семейство (V, p, X) называется *локально тривиальным*, если для каждой точки $x \in X$ найдется такая окрестность U, что $V|_U$ — тривиальное семейство.

Локально тривиальное семейство называется *векторным расслоением.*

Пример. Рассмотрим тривиальное семейство V над отрезком $X = [0, 1]$ с одномерным слоем $\mathbb{R}$. Склеим точки 0 и 1 базы и отождествим слои V_0 и V_1 над склеенными точками с помощью линейного преобразования $\varphi : \mathbb{R} \to \mathbb{R}$, $\varphi(x) = -x$. В итоге мы получим бесконечный лист Мебиуса — локально тривиальное семейство одномерных пространств над окружностью S^1. Любое сечение этого векторного расслоения задается вещественнозначной функцией $s(x)$ на отрезке $[0, 1]$ с условием $s(0) = -s(1)$. Тем самым, любое сечение обращается в нуль на базе S^1 (почему?). Отсюда следует, что лист Мебиуса не является тривиальным семейством (тривиальным векторным расслоением).

Обозначим через $\Gamma(V)$ множество всех сечений векторного расслоения $V \to X$. Сечения можно "поточечно" складывать и умножать на непрерывные функции, заданные на базе X. Если через $C(X)$ обозначить кольцо A непрерывных функций на базе X, то сечения $\Gamma(V)$ векторного расслоения $V \to X$ образуют $C(X)$-модуль относительно поточечного умножения, т.е.

$$(fs)(x) = f(x)s(x), \;\; f \in C(X), \;\; s \in \Gamma(V).$$

Можно доказать, что $C(X)$-модуль $\Gamma(V)$ над компактным хаусдорфовым пространством X проективен.

Пример. Для иллюстрации рассмотрим лист Мебиуса — нетривиальное локально-векторное расслоение $M \to S^1$ над окружностью, слоями которого являются прямые $\mathbb{R}$. Пространство сечений листа Мебиуса естественно отождествляется с вещественным векторным пространством непрерывных функций $s(x)$, заданных на отрезке $[0, 1]$ и удовлетворяющих условию $s(0) = -s(1)$.

Легко проверить, что пространство непрерывных сечений $\Gamma(M)$ является модулем над кольцом $A = C(S^1)$ непрерывных функций на окружности S^1, или, что то же самое, непрерывных функций $f(x)$ на отрезке $[0, 1]$ с условием $f(0) = f(1)$.

Покажем, что $\Gamma(M)$ — это проективный, но не свободный A-модуль.

> *Лемма.* Любые два сечения s_1 и s_2 листа Мебиуса линейно зависимы над кольцом A.

Доказательство. Заметим, что при нашем отождествлении пространства сечений $\Gamma(M)$ с функциями $s(x) \in C[0, 1]$, $s(0) = -s(1)$, произведение двух сечений есть функция из кольца $A = C(S^1)$. Поэтому $(s_1 s_2)s_2 - (s_2^2)s_1 = 0$ — искомая линейная зависимость. □

Следовательно, если модуль сечений $\Gamma(M)$ свободен над кольцом A, то $\Gamma(M) = As$. Это означало бы, что у всех сечений из $\Gamma(M)$ есть общий нуль на окружности, что, конечно, не так.

Однако, $\Gamma(M) \oplus \Gamma(M) \simeq A^2 = A \oplus A$.
В самом деле, пары сечений $(\sin \pi t, \cos \pi t)$ и $(-\cos \pi t, \sin \pi t)$ образуют свободный базис в $\Gamma(M) \oplus \Gamma(M)$, так как для любых сечений s_1 и s_2 система уравнений

$$\begin{pmatrix} \sin \pi t & -\cos \pi t \\ \cos \pi t & \sin \pi t \end{pmatrix} \begin{pmatrix} f_1 \\ f_2 \end{pmatrix} = \begin{pmatrix} s_1 \\ s_2 \end{pmatrix}$$

однозначно разрешима над кольцом непрерывных функций на окружности.

Литература

Э.Б.Винберг. *Курс алгебры.* Москва, Факториал, 2004
М. Атья. *Лекции по K-теории.* Москва, Мир, 1972
Книга для чтения по алгебре. Гостехиздат, 1936