Евклидовы Кольца

Определение 1. Целостное кольцо K называется *евклидовым*, если на нём есть *евклидова норма* $v : K \setminus 0 \to \mathbb{N}$, такая что $v(ab) = v(a)v(b)$ (для удобства положим $v(0) = 0$), и имеется деление с остатком: для каждого a, $b \in K$, $b \neq 0$, найдется $s, r \in K$, такие что

$$a = bs + r, \qquad v(r) < v(b).$$

Пример. Следующие кольца евклидовы:
любое поле F, $v(a) = 1$ для всех $a \neq 0$;
кольцо $\mathbb{Z}$, $v(n) = |n|$;
кольцо многочленов $F[x]$, $v(P) = 2^{\deg(P)}$;
кольцо формальных рядов $F[[x]]$, $v(F) = 2^{\operatorname{ord}(F)}$;
кольцо целых p-адических чисел $\mathbb{Z}_p$, $v(p^k a) = p^k$ для a не кратного p.

Предложение 1 *Равенство $v(x) = 1$ выполнено тогда и только тогда, когда x обратим.*

Доказательство: Если $v(x) = 1$, то деление с остатком даёт $1 = bx + r$ с $v(r) = 0$, откуда $r = 0$ и b — обратный к x.

Наоборот, заметим, что $0 \neq v(1) = v(1)v(1)$, откуда $v(1) = 1$. Тогда из $xb = 1$ следует $v(x)v(b) = v(1) = 1$, значит, $v(x) = v(b) = 1$.

Определение 2. Будем говорить, что $a \sim b$, если $a|b$ и $b|a$, то есть a/b — обратимый элемент K.

Тогда множество классов эквивалентности — полугруппа по умножению, частично упорядоченная по отношению делимости. Норма v постоянна на этих классах.

Определение 3. Наибольший общий делитель (a, b) — класс общих делителей a и b с наибольшей нормой.

Предложение 2 *Наибольший общий делитель единственен и делится на любой общий делитель.*

Доказательство: Легко увидеть, что результат приведённого ниже алгоритма Евклида делит любой общий делитель.

Пусть $a_1 = a$, $a_2 = b$. Чтобы получить a_{n+1} разделим a_{n-1} на a_n с остатком:

$$a_{n-1} = a_n s_{n-1} + a_{n+1}. \tag{1}$$

Так как $v(a_{n+1}) < v(a_n)$, рано или поздно получим $a_{k+1} = 0$. Тогда a_k будет общим делителем всех a_n (включая a и b), причём любой общий делитель a и b делится на него. Тем самым, в качестве (a, b) следует взять класс a_k.

Алгоритм Евклида родственен разложению в цепную дробь в следующем смысле. Норма естественным образом продолжается на кольцо частных (со значениями в $\mathbb{Q}$) по правилу $v(a/b) = v(a)/v(b)$. Деление с остатком строит взятие целой части в кольце частных $x = [x] + \{x\}$, где $[x] \in K$, $v(\{x\}) < 1$. Заметим, что в наших обозначениях $[a_n/a_{n+1}] = s_n$, $\{a_n/a_{n+1}\} = a_{n+2}/a_{n+1}$, а значит

$$\frac{a}{b} = \langle s_1, \dots, s_{k-1} \rangle = s_1 + \cfrac{1}{s_2 + \cfrac{1}{s_3 + \cfrac{1}{\dots s_{k-1}}}}$$

Заметим, что частичные цепные дроби $p_n/q_n = \langle s_1, \dots, s_n \rangle$ являются хорошими приближениями исходной дроби.

Упражнение 1 *Докажите, что* $p_n/q_n - p_{n-1}/q_{n-1} = (-1)^n/q_n q_{n-1}$.

Предложение 3 *Уравнение* $ax + by = c$ *имеет решение в* K *тогда и только тогда, когда* c *делится на* (a, b).

Доказательство: Ясно, что при наличии решения c делится на (a, b). Наоборот, достаточно найти решение для $c = a_k$ из алгоритма Евклида, в общем случае x и y достаточно будет умножить на $c/(a, b)$. В качестве таковогo достачочно вязть $x = (-1)^{k-1} q_{k-2}$, $y = (-1)^k p_{k-2}$.

Найдём общее решение этого уравнения. Пусть (x_0, y_0) и (x_1, y_1) — два решения, тогда для $x_+ = x_1 - x_0$, $y_+ = y_1 - y_0$ выполнено $ax_+ + by_+ = 0$. Поделив левую часть на представитель (a, b), можно сведём задачу к случаю $1 \in (a, b)$ (такие a и b называются *взаимно простыми*). Теперь общий вид решения

$$x = x_0 + kb/(a, b), \qquad y = y_0 - ka/(a, b)$$

легко получить из следующей леммы.

Лемма 1 *Если* $1 \in (a, b)$ *и* $b|ax$, *то* $b|x$.

Доказательство: Мы знаем, что найдутся α и β, такие что $\alpha a + \beta b = 1$. Умножая на x, получим $x = \alpha ax + \beta bx$, причём оба слагаемых правой части делятся на b.

Упражнение 2 *Когда уравнение* $a_1 x_1 + a_2 x_2 + \dots + a_n x_n = c$ *имеет решение? Придумайте алгоритм поиска его решений.*

Определение 4. Элемент $p \in K$ называется *простым*, если он не разлагается в произведение необратимых элементов.

Определение 5. Целостное кольцо K называется *факториальным*, если класс каждого элемента однозначно раскладывается в произведение классов простых множителей.

Теорема 1 *Всякое евклидово кольцо факториально.*

Доказательство: Во-первых, докажем, что разложение на простые множители существует. Проведём индукцию по $v(x)$. При $v(x) = 1$ мы знаем, что x — обратим. Теперь пусть x не простой, значит $x = x_1 x_2$, где $1 < v(x_i) < v(x)$. Тогда по предположению индукции x_i разлагаются в произведение простых множителей.

Для доказательства единственности снова проведём индукцию по $v(x)$. Заметим, что для простых p и q либо $1 \in (p, q)$, либо $p \sim q$. Если $x = p_1 \dots p_n = q_1 \dots q_m$, то по Лемме 1 один из q_i делится на p_1, значит, $q_i \sim p_1$. Сокращая равенство на p_1, пользуясь предположением индукции, легко завершим доказательство теоремы.

Иногда в каждом классе можно выбрать естественный представитель. Это упрощает формулировку теоремы.

Следствие 1 *Всякое натуральное число однозначно разлагается в произведение простых натуральных чисел.*

Следствие 2 *Пусть* F *— поле. Тогда всякий многочлен из* $F[x]$ *со старшим коэффициентом единица однозначно разлагается в произведение неразложимых многочленов со старшим коэффициентом единица.*

Предложение 4 *Если a — корень многочлена $P(x)$, то $P(x)$ делится на $x-a$.*

Доказательство: Остаток при делении $P(x)$ на $x-a$ является константой. Подставляя $x=a$, получим, что остаток равен $P(a)$.

Следствие 3 *Всякий многочлен из $\mathbb{C}[x]$ разлагается на линейные множители.*

Упражнение 3 *Всякий многочлен из $\mathbb{R}[x]$ разлагается на линейные и квадратичные множители.*

Следствие 4 *Всякий многочлен степени n над полем имеет не более n корней.*

Лемма 2 *Пусть x и y — элементы коммутативной группы порядка k и l, причём k и l — взаимно-просты. Тогда xy имеет порядок kl.*

Доказательство: В силу коммутативности $(xy)^{kl}=1$. Заметим, что если $x^a=y^b=z$, то порядок z является общим делителем k и l, следовательно $z=1$. Тем самым, если $(xy)^m=1$, то m кратно k и l, а значит и kl.

Теорема 2 *Мультипликативная группа любого конечного поля — циклическая.*

Доказательство: Пусть порядок мультипликативной группы поля равен n. Разложим n на простые множители $n=p_1^{d_1}\dots p_m^{d_m}$. Докажем, что для каждого i существует элемент порядка $p_i^{d_i}$, а значит по Лемме и порядка n. Для этого достаточно найти элемент порядка $kp_i^{d_i}$ и возвести его в степень k.

Предположим такого элемента нет, тогда по теореме Лагранжа порядок всякого элемента делит n, но не делится на $p_i^{d_i}$, значит, он делит n/p. Но тогда в поле имеется n корней уравнения $x^{n/p}-1=0$. Противоречие.

Но не всякое кольцо факториально.

Пример. Кольцо $\mathbb{Z}[\sqrt{-3}]$, составленное числами вида $a+b\sqrt{-3}$, где a, $b\in\mathbb{Z}$, не является факториальным:

$$4=2\cdot 2=(1-\sqrt{-3})\cdot(1+\sqrt{-3}).$$

Числа 2 и $1\pm\sqrt{-3}$ просты по следующей причине. Положим $N(z)=z\overline{z}$ для $z\in\mathbb{Z}[\sqrt{-3}]\subset\mathbb{C}$. Тогда $N(z)$ — неотрицательное целое число, $N(z_1z_2)=N(z_1)N(z_2)$ и $N(z)=1$ только для обратимых $z=\pm1$. Заметим, что $N(2)=N(1\pm\sqrt{-3})=4$ и $N(z)$ не принимает значение 2. Но значение N на простых делителях этих чисел должно быть делителем числа 4, откуда эти числа сами являются простыми.