Дискретные структуры

осень 2013

Александр Дайняк

www.dainiak.com

Поле: определение

Поле — это множество $\mathbb{F}$ с двумя бинарными ассоциативными *и коммутативными* операциями $+$ и $\cdot$, такими, что

- $\mathbb{F}$ является группой относительно $+$
  Нейтральный элемент этой группы обозначается 0.
- $\mathbb{F} \setminus \{0\}$ является группой относительно $\cdot$
  Нейтральный элемент этой группы обозначается 1.
- Операция $\cdot$ дистрибутивна относительно $+$:

$$\forall a, b, c \in F \quad a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

Примеры полей

Полями являются:

- Множества $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ относительно $+, \cdot$

Полями не являются:

- Множества $\mathbb{N}, \mathbb{Z}$
- Множество $\mathbb{R}^{n \times n}$ относительно сложения и умножения матриц

Примеры полей

Кроме $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ есть и другие бесконечные поля, например, поле дробно-рациональных функций, т.е.

$$\left\{ f \mid f = \frac{A(x)}{B(x)} \right\}$$

где $A(x)$ и $B(x)$ — многочлены с целыми коэффициентами, и $B(x) \not\equiv 0$.

Примеры свойств полей, выводимых из аксиом

Утверждение.
Если $\mathbb{F}$ поле, то для любого $a \in \mathbb{F}$ выполнено

$$a \cdot 0 = 0$$

Доказательство:

Обозначим $z := a \cdot 0$.

Имеем

$$z + z = a \cdot 0 + a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 = \mathrm{z}$$

Отсюда

$$z = 0 + z = (-z) + z + z = (-z) + z = 0$$

Примеры свойств полей, выводимых из аксиом

Утверждение.
Если $\mathbb{F}$ поле, то для любого $a \in \mathbb{F}$ выполнено

$$(-1) \cdot a = -a$$

Доказательство:

Обозначим $b \coloneqq (-1) \cdot a$.

Получаем

$$b + a = b + 1 \cdot a = (-1) \cdot a + 1 \cdot a = \big((-1) + 1\big) \cdot a = 0 \cdot a = 0$$

Поле: другое определение

Поле — это множество $\mathbb{F}$ с двумя бинарными ассоциативными операциями $+$ и $\cdot$ и двумя специальными элементами 0 и 1, такими, что

- $\forall a, b \quad a + b = b + a, \quad a \cdot b = b \cdot a$
- $\forall a, b, c \in \mathbb{F} \quad a \cdot (b + c) = (a \cdot b) + (a \cdot c)$
- $\forall a \in \mathbb{F} \quad 0 + a = a + 0 = a$
- $\forall a \in \mathbb{F} \setminus \{0\} \quad 1 \cdot a = a \cdot 1 = a$
- $\forall a, b \in \mathbb{F} \qquad \exists x: \quad a + x = b$
- $\forall a, b \in \mathbb{F} \setminus \{0\} \quad \exists x: \quad a \cdot x = b$

Поле: третье определение (для конечного поля)

Конечное поле — это множество

$$\mathbb{F} = \{a_1, \dots, a_n\}$$

с бинарными ассоциативными коммутативными операциями $+$ и $\cdot$ и элементами 0 и 1, такими, что

- $\forall a, b, c \in \mathbb{F} \quad a \cdot (b + c) = (a \cdot b) + (a \cdot c)$
- $\forall a \in \mathbb{F} \quad 0 + a = a + 0 = a$
- $\forall a \in \mathbb{F} \setminus \{0\} \quad 1 \cdot a = a \cdot 1 = a$
- $\forall a$ элементы $a + a_1, \dots, a + a_n$ все различны
- $\forall a \neq 0$ элементы $a \cdot a_1, \dots, a \cdot a_n$ все различны

Конечное поле $\mathbb{Z}_p$

Утверждение.
Для любого простого p множество $\mathbb{Z}_p$ образует поле относительно операций сложения и умножения по модулю p.

Доказательство:
То, что $(\mathbb{Z}_p, \oplus)$ и $(\mathbb{Z}_p \setminus \{0\}, \odot)$ — группы, доказано ранее.

Дистрибутивность умножения по модулю относительно сложения по модулю очевидна.

Многочлены: определение

Многочлен (*полином*) от переменных $x_1, \dots, x_m$ с коэффициентами из множества K — это конечная сумма *одночленов* (*мономов*) т.е. произведений вида

$$c \cdot x_{i_1}^{t_1} \cdot \dots \cdot x_{i_r}^{t_m}$$

где

$$c \in K$$
$$t_1, \dots, t_m \in \mathbb{N}_0$$
$$i_1, \dots, i_r \in \{1, \dots, m\}$$

Если $r = 0,$ то это *свободный член*.

Степени

Степень монома $T = c \cdot x_{i_1}^{t_1} \cdot \ldots \cdot x_{i_r}^{t_m}$ *— это*

$$\deg T \coloneqq t_1 + \cdots + t_m$$

Степень полинома P определяется так*:*

$$\deg P \coloneqq \max\{\deg T \quad | \quad T \text{ — моном } P\}$$

Степень *нулевого* (тождественно равного нулю) многочлена считается равной $-\infty$

Степени

Степень монома $T = c \cdot x_{i_1}^{t_1} \cdot \ldots \cdot x_{i_r}^{t_m}$ *по переменной* x_k — это показатель, с которым x_k входит в произведение T.
Обозначение:

$$\deg_{x_k} T$$

Степень полинома P *по переменной* x_k равна

$$\deg_{x_k} P := \max\{ \quad \deg_{x_k} T \quad | \quad T \text{ — моном } P \quad \}$$

Если $P \equiv 0$, то полагаем $\deg_{x_k} P := -\infty$.

Степени

Утверждение.

Если P' и P'' — многочлены, то

- $\deg(P' + P'') \leq \max\{\deg P', \deg P''\}$
- $\deg(P' \cdot P'') = \deg P' + \deg P''$

То же и для степеней по переменным:

- $\deg_{x_k}(P' + P'') \leq \max\{\deg_{x_k} P', \deg_{x_k} P''\}$
- $\deg_{x_k}(P' \cdot P'') = \deg_{x_k} P' + \deg_{x_k} P''$

Доказательство: прямая проверка.

Многочлены с коэффициентами из заданного множества

Если коэффициенты многочлена P от переменных $x_1, \dots, x_m$ берутся из множества K, то пишут

$$P \in K[x_1, \dots, x_m]$$

Если $\forall a, b \in K$ выполнено $(a + b), (a \cdot b) \in K$, то и множество $K[x_1, \dots, x_m]$ тоже замкнуто относительно сложения и умножения.

Чаще всего в качестве K рассматривают некоторое *поле*. Тогда обычно пишут

$$P \in \mathbb{F}[x_1, \dots, x_m]$$

Нормированные многочлены

Многочлен $P \in \mathbb{F}[x]$, у которого коэффициент при мономе старшей степени равен 1, называется *нормированным*.

Кратко будем называть нормированные многочлены *нормногочлеными*.

Очевидно, любой многочлен можно получить из некоторого нормногочлена умножением на константу.

Деление многочленов с остатком

Утверждение.
Для любых многочленов $P, Q \in \mathbb{F}[x]$ при $Q \not\equiv 0$ существуют и однозначно определены многочлены S и R, такие, что

- $P = Q \cdot S + R$
- $\deg R < \deg Q$

R — *остаток* от деления P на Q

Доказательство: всё аналогично делению целых чисел с остатком.

Пример деления многочленов «в столбик»

$$
\begin{array}{rl|l}
 & x^5 - 2x^4 + 5x + 3 & x^2 - 7 \\
- & x^5 - 7x^3 & \hline
 & & x^3 - 2x^2 + 7x - 14 \\
\hline
 & -2x^4 + 7x^3 + 5x + 3 & \\
- & -2x^4 + 14x^2 & \\
\hline
 & 7x^3 - 14x^2 + 5x + 3 & \\
- & 7x^3 - 49x & \\
\hline
 & -14x^2 + 54x + 3 & \\
- & -14x^2 + 98 & \\
\hline
 & 54x - 95 &
\end{array}
$$

Итог:

$$x^5 - 2x^4 + 5x + 3 = (x^3 - 2x^2 + 7x - 14) \cdot (x^2 - 7) + (54x - 95)$$

Вычисления по модулю многочлена

Если R — остаток от деления P на Q, будем писать

$$R = P \bmod Q$$

Если $P_1 \bmod Q = P_2 \bmod Q$, то пишем

$$P_1 \equiv P_2 \pmod{Q}$$

или

$$P_1 \overset{Q}{=} P_2$$

Вычисления по модулю многочлена

Утверждение.

Если $P_1 \overset{Q}{=} P_2$ и $P_3 \overset{Q}{=} P_4$, то

- $P_1 + P_3 \overset{Q}{=} P_2 + P_4$
- $P_1 \cdot P_3 \overset{Q}{=} P_2 \cdot P_4$
- $(P_1)^k \overset{Q}{=} (P_2)^k$ для любого $k \in \mathbb{N}$

Доказательство: упражнение.

Пример вычислений по модулю многочлена

Найдём остаток от деления многочлена

$$P \coloneqq (x^5 + 2x^3 + 4)^4 \cdot (x^3 + 3) + x$$

на многочлен $Q \coloneqq x^2 + 2$, где все многочлены принадлежат $\mathbb{Z}_5[x]$.

Решение:

$$x^5 + 2x^3 + 4 = (x^2 + 2)x^3 + 4 \overset{Q}{=} 4 \overset{\mathbb{Z}_5}{=} -1$$

$$x^3 + 3 = (x^2 + 2)x - 2x + 3 \overset{Q}{=} -2x + 3$$

Отсюда

$$P \overset{Q}{=} (-1)^4 \cdot (-2x + 3) + x = -x + 3 = 4x + 3$$

Малая теорема Безу

Утверждение.
Если $P \in \mathbb{F}[x]$ и $a \in \mathbb{F}$, то

$$P(a) = P \bmod (x - a)$$

Следствие.
Если a — корень многочлена $P \in \mathbb{F}[x]$, то P без остатка делится на $(x - a)$.

Неприводимые многочлены

Многочлен $P \in \mathbb{F}[x]$ называется н*еприводимым/неразложимым/простым* (*над* $\mathbb{F}$),
если не существует $Q, S \in \mathbb{F}[x]$, таких, что

$$P = Q \cdot S, \quad \deg Q \geq 1, \quad \deg S \geq 1$$

Примеры:

- $x^2 + x + 1$ простой над $\mathbb{R}$, так как если бы его можно было разложить на множители, то у него были бы корни в $\mathbb{R}$.
- $P = x^4 + 2x^3 + 3x^2 + 2x + 1$ не является простым над $\mathbb{R}$, так как $P = (x^2 + x + 1)^2$. Заметьте, что корней из $\mathbb{R}$ у P нет.

Неприводимые многочлены

Ещё примеры:

- $x^2 + x + 1$ простой над $\mathbb{Z}_2$, так как ни 0, ни 1 не являются его корнями (если вычисления выполнять по модулю 2)
- $x^2 + x + 1$ не является простым над $\mathbb{Z}_3$, так как

$$x^2 + x + 1 \overset{3}{=} x^2 + 4x + 4 = (x + 2)^2$$

Теорема о разложении

Теорема.
Любой многочлен $P \in \mathbb{F}[x]$ может быть единственным образом (с точностью до перестановки сомножителей) представлен в виде

$$P = c \cdot P_1 \cdot \ldots \cdot P_k$$

где $P_1, \ldots, P_k$ — простые нормногочлены (не обязательно различные).

Доказательство аналогично доказательству основной теоремы арифметики

Утверждения о делимости многочленов

Утверждения.

- Если $P_1 \cdot P_2$ делится на Q, и Q простой,
  то хотя бы один из многочленов P_1, P_2 делится на Q
- Если P делится на различные простые многочлены Q_1 и Q_2,
  то P делится на $Q_1 \cdot Q_2$

Доказательства аналогичны доказательствам аналогичных теорем арифметики

Поле: третье определение (для конечного поля)

Конечное поле — это множество

$$\mathbb{F} = \{a_1, \dots, a_n\}$$

с бинарными ассоциативными коммутативными операциями $+$ и $\cdot$ и элементами 0 и 1, такими, что

- $\forall a, b, c \in \mathbb{F} \quad a \cdot (b + c) = (a \cdot b) + (a \cdot c)$
- $\forall a \in \mathbb{F} \quad 0 + a = a + 0 = a$
- $\forall a \in \mathbb{F} \setminus \{0\} \quad 1 \cdot a = a \cdot 1 = a$
- $\forall a$ элементы $a + a_1, \dots, a + a_n$ все различны
- $\forall a \neq 0$ элементы $a \cdot a_1, \dots, a \cdot a_n$ все различны

Конечное поле $\mathbb{Z}_p[x]/Q$

Пусть p — простое число.

Пусть Q — простой многочлен из $\mathbb{Z}_p[x]$.

Через $\mathbb{Z}_p[x]/Q$ обозначим множество всех многочленов из $\mathbb{Z}_p[x]$, степень которых строго меньше $\deg Q$.

На множестве $\mathbb{Z}_p[x]/Q$ определим операции сложения и умножения:

$$P_1 \bigoplus P_2 \coloneqq (P_1 + P_2) \bmod Q$$
$$P_1 \odot P_2 \coloneqq (P_1 \cdot P_2) \bmod Q$$

Конечное поле $\mathbb{Z}_p[x]/Q$

Утверждение.
Множество $\mathbb{Z}_p[x]/Q$ является полем относительно введённых операций сложения и умножения многочленов по модулю Q.

Доказательство:

- Ассоциативность, коммутативность, дистрибутивность очевидна
- Существование нуля и единицы очевидно

Конечное поле $\mathbb{Z}_p[x]/Q$

Ещё нужно доказать, что:

- $\forall P, P_1, P_2 \in \mathbb{Z}_p[x]/Q$ если $P_1 \neq P_2$, то $P \bigoplus P_1 \neq P \bigoplus P_2$

Это так, т.к.

$$P \bigoplus P_1 = P \bigoplus P_2 \quad \Rightarrow \quad P + P_1 \overset{Q}{=} P + P_2 \quad \Rightarrow \quad P_1 \overset{Q}{=} P_2 \quad \Rightarrow \quad P_1 = P_2$$

Конечное поле $\mathbb{Z}_p[x]/Q$

Осталось доказать, что:

- $\forall P, P_1, P_2 \in \mathbb{Z}_p[x]/Q$ если $P_1 \neq P_2$ и $P \not\equiv 0$, то $P \odot P_1 \neq P \odot P_2$

Если $P \odot P_1 = P \odot P_2$, то

$$P \cdot P_1 \overset{Q}{=} P \cdot P_2 \quad \Rightarrow \quad P \cdot (P_1 - P_2) \overset{Q}{=} 0$$

Т.к. Q простой, то либо P делится на Q, либо $(P_1 - P_2)$ делится на Q.

По условию, $P \not\equiv 0$, а значит

$$(P_1 - P_2) \overset{Q}{=} 0 \quad \Rightarrow \quad P_1 \overset{Q}{=} P_2 \quad \Rightarrow \quad P_1 = P_2$$

Количество неприводимых многочленов над $\mathbb{Z}_p$

Теорема (доказательство — весной).
Количество неприводимых над $\mathbb{Z}_p$ нормногочленов степени n равно количеству непериодических циклических слов длины n в p-символьном алфавите.

Следствие.
При каждом p и при каждом $n \geq 2$ существует хотя бы один неприводимый над $\mathbb{Z}_p$ нормногочлен степени n.

Резюме

- Многочлены похожи на числа: их можно делить столбиком, определить простые многочлены и доказать аналоги теорем из арифметики
- Для любого простого p и любого $\alpha \in \mathbb{N}$ существует конечное поле порядка p^{α}.
  При $\alpha = 1$ это просто $\mathbb{Z}_p$,
  при $\alpha > 1$ это множество многочленов из $\mathbb{Z}_p[x]$ степени $\leq \alpha - 1$, сложение и умножение которых проводится по модулю некоторого простого многочлена Q, $\deg Q = \alpha$

Некоторые факты о конечных полях (без доказательства)

- Любое конечное поле изоморфно полю многочленов $\mathbb{Z}_p[x]/Q$ для некоторого простого числа p и многочлена Q, неприводимого над $\mathbb{Z}_p$.
- В любом конечном поле все ненулевые элементы образуют *циклическую* группу относительно умножения.