2. Лекция 2. Многочлены и конечные поля.

2.1. **Гомоморфизмы колец.**

Определение 2.1. Гомоморфизм колец $f : R_1 \to R_2$ это отображение, сохраняющее операции:

$$f(x+y) = f(x) + f(y) \quad f(xy) = f(x)f(y) \quad \forall x, y \in R_1$$

Если кольца R_1 и R_2 содержат единицу, обычно дополнительно требуют, чтобы $f(1) = 1$

Определение 2.2. Изоморфизм колец – это биективный гомоморфизм.

Определение 2.3. Ядро гомоморфизма $\operatorname{Ker} f = \{x \in R_1 \mid f(x) = 0\}$.

Определение 2.4. Образ гомоморфизма $\operatorname{Im} f = \{y \in R_1 \mid \exists\, x \in R_1 : f(x) = y\}$.

Несложно видеть, что ядро и образ – подкольца в R_1 и R_2 соответственно. Ядро связано с инъективностью следующим образом:

Предложение 2.5. Гомоморфизм f инъективен тогда и только тогда когда $\operatorname{Ker} f = \{0\}$.

2.2. **Характеристика поля.**

Пусть $\Bbbk$ – произвольное поле. Как мы видим по примеру $\mathbb{Z}/p\mathbb{Z}$, то в поле может существовать такое $n \geq 0$, что

$$\underbrace{1 + 1 + \ldots + 1}_{n \text{ раз}} = 0.$$

Такое число n называется *характеристикой поля* и обозначается через $\operatorname{char} \Bbbk$. Если такого n не существует, тогда говорят, что $\operatorname{char} \Bbbk = 0$.

Предложение 2.6. Характеристика поля либо ноль, либо простое число.

Доказательство. Пусть $\operatorname{char} \Bbbk = n = ab, a, b > 1$. Тогда

$$0 = \underbrace{(1 + \ldots + 1)}_{n} = \underbrace{(1 + \ldots + 1)}_{a}\underbrace{(1 + \ldots + 1)}_{b}$$

При этом оба множителя ненулевые, но в поле нет делителей нуля. □

Почему говорят, что $\operatorname{char} \Bbbk = 0$ в случае, когда это не простое число? Заметим, что для любого поля существует канонический гомоморфизм полей:

$$f : \mathbb{Z} \to \Bbbk, 1 \mapsto 1$$

По вышесказанному, $\operatorname{Ker} f = p\mathbb{Z}$ или $\operatorname{Ker} f = 0\mathbb{Z} = 0$.

2.3. **Прямое произведение колец.**

Пусть R_1, R_2 – кольца.

Определение 2.7. Множество $R_1 \times R_2 = \{(x, y) \mid x \in R_1, y \in R_2\}$ с покомпонентными операциями

$$(x_1, y_1) + (x_2, y_2) := (x_1 + x_2, y_1 + y_2)$$

$$(x_1, y_1) \cdot (x_2, y_2) := (x_1 x_2, y_1 y_2)$$

называется прямым произведением колец.

В случае счётного бесконечного числа множителей есть два определения: можно считать, что мы рассматриваем все элементы вида $(a_1, a_2, \ldots,)$, а можно считать, что начиная с некоторого номера N все $a_i = 0$. В первом случае получаем *прямое*, а во втором *декартово* произведение.

2.4. **Китайская теорема об остатках.** Пусть $n = n_1 \dots n_k$, и все n_i попарно взаимнопросты.

Теорема 2.8. $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_k\mathbb{Z}$

Доказательство. Рассмотрим отображение

$$f : [m]_n \mapsto ([m]_{n_1}, \dots, [m]_{n_k})$$

Тогда $\operatorname{Ker} f = 0$ (если $n_1 \mid m, \dots, n_k \mid m$, то $n \mid m$ так как все n_i попарно взаимнопросты) значит f инъективно. С другой стороны $|\mathbb{Z}/n\mathbb{Z}| = |\mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_k\mathbb{Z}|$. □

2.5. **Кольцо многочленов.** Пусть R коммутативное кольцо с единицей. Тогда определим кольцо многочленов с коэффициентами в R следующим образом:

$$R[x] = \{a_0 + a_1 x + \dots + a_n x^n \,|n \in \mathbb{Z}_{\geq 0}, a_i \in R\}$$

Легко видеть, что $R[x]$ – коммутативное кольцо с единицей (и не поле). Ниже мы будем по умолчанию рассматривать кольца многочленов с коэффициентами в произвольном поле $\Bbbk$. Однако

Примеры. Если $R = \Bbbk[y]$, то $R[x] = (\Bbbk[x])[y] = \Bbbk[x, y]$ – кольцо многочленов от двух переменных.

Факториально ли кольцо многочленов с коэффициентами в поле? Оказывается, что да. Причина та же самая, что и для целых чисел.

Определение 2.9. Пусть $f(x) = a_0 + a_1 x + \dots + a_n x^n, a_n \neq 0$. Тогда степень многочлена $\deg f = n$.

Ясно, что $\deg(fg) = \deg f \cdot \deg g$.

Предложение 2.10 (Деление с остатком)**.** Для любых $f, g \in \Bbbk[x]$ существуют единственные $q, r \in \Bbbk[x]$ такие, что

$$f = gq + r, \quad \deg r < \deg g$$

Следствие 2.11 (Теорема Безу)**.** (1) Пусть $f \in \Bbbk[x]$ и $c \in \Bbbk$ такое, что $f(c) = 0$. Тогда $x - c \mid f(x)$.

(2) В поле многочлен степени n имеет не более n различных корней.

Доказательство. 1) $f = (x - c)q + r$ причём $\deg r = 0$. Более того, $f(c) = 0 = r$.
2) Если c – корень, то $f(x) = (x - c)g(x)$, $\deg g = n - 1$. □

Определение 2.12. Пусть $f, g \in \Bbbk[x]$. Говорят, что $d \in \Bbbk[x]$ наибольший общий делитель (НОД) если:

(1) Старший коэффициент равен 1;
(2) $d \mid f, d \mid g$;
(3) d – максимальной степени со свойством (2).

Предложение 2.13. Наибольший общий делитель определён корректно.

Доказательство. Рассмотрим множество $I = \{fa + gb \,| a, b \in \Bbbk[x]\}$. Пусть $D \in I$ – многочлен минимальной степени. Тогда $I = \{D \cdot c \,| c \in \Bbbk[x]\}$ (иначе остаток от деления на D лежит в I и имеет меньшую степень). Тогда НОД(f, g) делит D. С другой стороны, D – общий делитель f, g. Значит, $\deg d = \deg D$, откуда следует, что $d = D \cdot \lambda, \lambda \in \Bbbk^\times$. □

Предложение 2.14 (Алгоритм Евклида и линейное представление НОД)**.** (1) НОД(f, g) = НОД$(f - g, g)$;

(2) Для любых $f, g \in \Bbbk[x]$ существуют $x, y \in \Bbbk[x]$ НОД$(f, g) = fx + gy$.

Следствие 2.15 (Факториальность)**.** Кольцо $\Bbbk[x]$ факториально.

2.6. **Вычеты по модулю многочлена.** Если $f \in \Bbbk[x]$ то можно рассмотреть множество $\Bbbk[x]/(f)$ – множество остатков при делении на f.

Предложение 2.16. Класс $[g]$ обратим тогда и только тогда когда НОД$(f, g) = 1$.

Доказательство. Аналогично доказательству для целых чисел. □

Следствие 2.17. $\Bbbk[x]/(f)$ – поле тогда и только тогда когда f - неприводим.

Примеры. (1) Многочлен $x^2 + 1$ неприводим в $\mathbb{R}[x]$. Поле

$$\mathbb{C} := \mathbb{R}[x]/(x^2 + 1)$$

называется полем комплексных чисел.

(2) Многочлен $x^2 - 2$ неприводим в $\mathbb{Q}[x]$, получаем поле

$$Q[x]/(x^2 - 2).$$

Несложно показать, что оно изоморфно подполю $\mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$ состоящему из чисел вида $a + b\sqrt{2}, a, b \in \mathbb{Q}$.

(3) Многочлен $x^2 + x + 1$ неприводим в $\mathbb{F}_{\not=}[x]$, получаем поле из четырёх элементов $\mathbb{F}_4 := \mathbb{F}_2[x]/(x^2 + x + 1)$.

(4) Если f – неприводимый многочлен степени n из $\mathbb{F}_p[x]$, то $\mathbb{F}_p[x]/(f)$ – поле из p^n элементов.

Заметим, что если бы мы знали, что существует неприводимый многочлен степени n, то построили бы конечное поле из p^n элементов.