3. Лекция 3. Конечные поля и гауссовы числа.

3.1. **Конечные поля.**

Теорема 3.1. (1) Если $\mathbb{F}$ – конечное поле, то $|\mathbb{F}| = p^n$, где p – простое, $n \geq 1$.
(2) Существует поле $\mathbb{F}_{p^n}$ порядка p^n для любого простого p и $n \geq 1$.
(3) Любые два поля порядка p^n изоморфны.

Доказательство.

Предложение 3.2. Конечная подгруппа мультипликативной группы поля циклическая.

Доказательство. Пусть G – конечная подгруппа $\Bbbk^\times$, а n – максимальный порядок элемента в G. Покажем, что порядок любого элемента делит n. Отсюда будет следовать, что $n = |G|$, так как уравнение $x^n - 1 = 0$ имеет в поле не более n корней.

Лемма 3.3. Пусть $x, y \in G$ и $|x| = a, |y| = b$. Тогда в G существует элемент порядка $\text{НОК}(a, b)$.

Доказательство. 1) Предположим, что $\text{НОД}(a, b)$=1. Тогда $\text{НОК}(a, b) = ab$ и такой порядок имеет элемент xy. Действительно, $(xy)^{ab} = (x^a)^b \cdot (y^b)^a = 1$. Если $(xy)^k = 1$, причем $k < n$, то получим, что

$$x^r = y^s$$

для некоторых $r < a, s < b$. Но тогда $1 = y^{as}$, причем as не делится на b откуда $y^c = 1$, для некоторого $c < b$, что приводит к противоречию.
2) В общем случае пусть $d = \text{НОД}(a, b)$. Тогда существуют $a_1, a_2, l_1, l_2 \in \mathbb{Z}$ такие, что $a = l_1 a_1, b = l_2 b_1$, $\text{НОД}(l_1, l_2) = 1$, $\text{НОК}(a, b) = l_1 l_2$. Для этого отправим в l_1 все простые множители, которые входят в a в большей степени, чем в b. Тогда элементы x^{a_1} и y^{a_2} имеют взаимнопростые порядки l_1, l_2, а их произведение порядок $\text{НОК}(a, b)$. □

Из леммы следует предложение: если элемент имеет порядок m не делящий n, то $\text{НОК}(m, n) > n$, что приводит к противоречию. □

Заметим, что для поля характеристики p есть каноническое вложение поля $\mathbb{F}_p$ в $\mathbb{F}$ (*простое подполе*). Предложение показывает, что в конечном поле корректно определено следующее понятие:

Определение 3.4 (Минимальный многочлен элемента)**.** Минимальный многочлен $f \in \mathbb{F}_p[x]$ элемента $\alpha \in \mathbb{F}$ – это неприводимый приведённый многочлен минимальной степени такой, что $f(\alpha) = 0$.

Чтобы доказать пункт 1) теоремы заметим, что $\mathbb{F}_p[\alpha] = \{f(\alpha) \,|\, f \in \mathbb{F}_p[x]\}$ является подполем $\mathbb{F}$. Действительно, оно замкнуто относительно сложения и умножения по определению. С другой стороны, достаточно

$$\mathbb{F}_p[\alpha] = \{r(\alpha) \,|\, r - \text{произвольный остаток при делении на } m_\alpha(x)\}.$$

Отсюда следует, что любой элемент обратим (воспользуемся линейным представление НОД). Иными словами, $\mathbb{F}_p[\alpha] \simeq \mathbb{F}_p[x]/(m_\alpha(x))$. Так как $\mathbb{F}_p[\alpha]$ содержит ровно p^n элементов, то совпадает с $\mathbb{F}$.
2) Существование.

Предложение 3.5. Пусть $f \in \Bbbk[x]$ – многочлен. Тогда существует $\Bbbk \subset \mathbb{F}$ такое, что в $\mathbb{F}$ многочлен $\mathbb{F}$ раскладывается на линейные множители.

Доказательство. Пусть f имеет в $\Bbbk$ k корней и пусть g – неприводимый фактор f. Тогда в поле $\Bbbk[x]/(g)$ многочлен f имеет на один корень больше. Продолжая, получим поле требуемое. □

Построим поле $\mathbb{F}_{p^n}$ как подполе поля $\Bbbk$ разложения многочлена $x^{p^n} - x \in \mathbb{F}_p[x]$, а именно, мы утверждаем, что все его корни образуют поле. Действительно, если x, y – корни, то

$$(x+y)^{p^n} = ((x+y)^p)^{p^{n-1}} = (x^p + y^p)^{p^{n-1}} = \ldots = x^{p^n} + y^{p^n} \quad (xy)^{p^n} = xy.$$

Если $x \neq 0$ корень, то $x^{p^n-1} = 1$, а значит, элемент x обратим. Все остальные свойства поля следуют из того, что множество корней является подполем в $\Bbbk$. Осталось доказать, что корней ровно p^n, это следует из следующей леммы.

Лемма 3.6. Многочлен $f \in \Bbbk[x]$ не имеет кратных корней тогда и только тогда когда НОД$(f, f') = 1$. Здесь f' – (формальная) производная f.

3) Для доказательства единственности мы построим изоморфизм между любыми двумя полями $\mathbb{F}_1$ и $\mathbb{F}_2$ порядка p^n. Для этого выберем ξ – первообразный корень в $\mathbb{F}_1$ и пусть $m_\xi(x) \in \mathbb{F}_p[x]$ – минимальный многочлен. В $\mathbb{F}_1[x]$ и $\mathbb{F}_2[x]$ он раскладывается на линейные множители (так как делит $x^{p^n} - x$). Более того, все его корни – первообразные. Действительно, пусть a – корень $m_\xi(x)$ и a – не является первообразным. Тогда существует $m_a(x) \in \mathbb{F}_p[x]$ – минимальный многочлен элемента a, причем $m_a(x) \,|\, m_\xi(x)$. Но $m_\xi(x)$ неприводим. Пусть ξ_1 – корень $m_\xi(x)$ в $\mathbb{F}_2$. Мы утверждаем, что отображение $\psi : \mathbb{F}_1 \to \mathbb{F}_2, \xi^k \mapsto \xi_1^k, 0 \mapsto 0$ – изоморфизм полей. Очевидно, что ψ – биекция сохраняющая умножение. Пусть $\xi^i + \xi^j = \xi^k$. Нужно доказать, что $\xi_1^i + \xi_1^j = \xi_1^k$. Заметим, что $m_\xi(x) | x^i + x^j - x^k$, откуда получаем требуемое.

Если $\xi^i + \xi^j = 0$ и $\operatorname{char} \mathbb{F}_1 = 2$, то $\xi^i = \xi^j$ и получаем требуемое. Если $\operatorname{char} \mathbb{F}_1 \neq 2$, то $\xi^{i-j} = -1$, а значит $i - j = \frac{p^n-1}{2}$ и $\xi_1^{i-j} = -1$, что и требовалось доказать.

3.2. **Гауссовы числа.**

Определение 3.7. Гауссовы числа – это $\mathbb{Z}[i] = \{a + bi \,|\, a, b \in \mathbb{R}\} \subset \mathbb{C}$.

Так как гауссовы числа – подкольцо в $\mathbb{C}$, то они являются областью целостности.

Определение 3.8. Нормой Гауссова числа $z = a+bi$ называется целое положительное число $N(z) = z\bar{z} = a^2 + b^2$.

Предложение 3.9. Для любых $z_1, z_2 \in \mathbb{Z}[i]$ существует q, r такие, что $z_1 = qz_2 + r, N(r) < N(z_2)$.

Доказательство. В качестве неполного частного можно взять ближайшую к z_1 точку в решётке кратных z_2. □

Ясно, что $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.

Определение 3.10. *Наибольшим общим делителем* чисел $a, b \in \mathbb{Z}[i]$ называется $d \in \mathbb{Z}[i]$ такой, что:

(1) d общий делитель a, b;
(2) d – обладает наибольшей нормой среди всех общих делителей.

Предложение 3.11. НОД определён корректно.

Доказательство. Аналогично кольцу многочленов. □

Отсюда следует, что в $\mathbb{Z}[i]$ есть алгоритм Евклида, линейное представление НОД, лемма Евклида и основная теорема арифметики.

Теорема 3.12. Кольцо $\mathbb{Z}[i]$ факториально.

3.3. **Простые Гауссовы числа.**

Теорема 3.13. Гауссово числа $z = a+bi$ простое, тогда и только тогда когда выполнено одно из следующих условий

- z ассоциировано с $p = 4k + 3$;
- $N(a + bi) = p$, где $p = 4k + 1$ или $p = 2$ – простое.

Доказательство.

Лемма 3.14. Уравнение $x^2 = -1$ разрешимо в $\mathbb{F}_p$ тогда и только тогда когда $p = 2$ или $p = 4K + 1$.

Доказательство. Пусть $\exists\, a \in \mathbb{F}_p, p \neq 2$ такой, что $a^2 = -1$. Тогда $a^4 = 1$. Так как $\mathbb{F}_p^\times$ циклическая, то это $4 \mid p-1$. Обратно, если $4 \mid p-1$ то в циклической группе существует элемент порядка 4. □

- Пусть $p = 4k + 1$. Тогда $\exists\, a \in \mathbb{Z}$ такой, что $p|x^2 + 1 = (x - i)(x + i)$. Но тогда $p = \pm 1$.
- Пусть $p = 4k + 3$, не простое, тогда $p = (a + bi)q = p = (a - bi)\bar{q}$. Значит $p = (a + bi)(a - bi)c$, где $c = \pm 1$. Тогда $p^2 = a^2 + b^2$, но у суммы квадратов не может быть остаток 3 по модулю 4.
- Если $N(a + bi) = p$, то $a + bi$ – простое, так как норма 1 только у обратимых элементов.
- Пусть $a, b \neq 0$ и $N(a + bi) = n_1 \cdot n_2 = (a + bi)(a - bi)$, где $n_1, n_2 \in \mathbb{Z}_{>1}$. Если $a + bi$ простое, то $a - bi$ – тоже, а значит получаем два различных разложения на простые множители, что противоречит факториальности.

□

Отсюда получаем, что простые числа вида $4k + 1$ представимы в виде суммы двух квадратов целых чисел, а вида $4k + 3$ – нет.

Действительно, если $p = 4k + 1$, то $p = (a + bi)(a - bi) = a^2 + b^2$. Если $p = 4k + 3$, то очевидно не представимо. Более того, если a, b представимы в виде суммы двух квадратов, то ab – тоже, так как для комплексных чисел $|z_1 z_2| = |z_1||z_2|$.

Следствие 3.15. Натуральное число представимо в виде суммы двух квадратов если в разложение на простые множители простые числа вида $p = 4k + 3$ входят в чётных степенях.

Верно и обратное, но здесь мы это не доказываем (задача в листочке).

□