

3 Конечные поля (поле Галуа)

Предл. 1 Пусть F -поле и $\text{char } F = p > 0$. Тогда от-е $\varphi: F \rightarrow F$ по правилу $x^\varphi = x^p$ — гомоморфизм и $\text{Ker } \varphi = 0$. В частности, если $|F| < \infty$, то φ — автоморфизм.

Д-во $\forall x, y \in F$ $(xy)^\varphi = (xy)^p = x^p y^p = x^\varphi y^\varphi$ и $(x+y)^\varphi = (x+y)^p = \sum_{i=0}^p C_p^i x^i y^{p-i} = x^p + y^p = x^\varphi + y^\varphi$, т.к. $C_p^i \equiv 0(p)$, $i \neq 0, p$.
 $\text{Ker } \varphi = 0$, т.к. в F нет делителей нуля. \square

Опр 1 От-е φ из предл 1 наз-ся **эндоморфизмом** (т.е. гом-змом в себя) **Фробениуса**. В случае, если F конечно, говорят об **автоморфизме Фробениуса**.

Опр 2 Поле, состоящее из конечно числа элементов, наз-ся **полем Галуа** и обозч \mathbb{F}_q или $GF(q)$, где q — порядок поля, т.е. число его элементов.

Т. 1 (о полях Галуа) Пусть $F = \mathbb{F}_q$ — поле Галуа порядка q . Тогда

- 1) $q = p^n$ для некоего простого p и натурального n .
- 2) \forall простого p и натурального $n \exists$ поле Галуа \mathbb{F}_q , где $q = p^n$.
- 3) Все поля Галуа одного порядка изоморфны.
- 4) Группы $\text{Aut}(\mathbb{F}_q)$ автоморфизмов поля \mathbb{F}_q , $q = p^n$, — циклическая и порождается автом-ом Фробениуса $\varphi: x \mapsto x^p$.

Л-во: 1) Если $q = |F| < \infty$, то $\text{char } F = p > 0$ — простое и $\mathbb{F}_p = \mathbb{Z}_p = \{k \cdot 1 \mid k = 0, \dots, p-1\}$ — простое поле F . Т.к.

F конечно, то F — конеч. поле. пусть $\mathbb{F}_p \subset F$ и $|F:\mathbb{F}_p| = n$. Тогда $|F| = |\mathbb{F}_p|^{|F:\mathbb{F}_p|} = p^n$.

3) Пусть $|F| = q = p^n \Rightarrow$ порядок $|F^*|$ мультипл. группы поля F^* равен $q-1$. По т. Лагранжа $\forall a \in F^*: a^{q-1} = 1 \Rightarrow a^q = a \quad \forall a \in F$, т.е. все эл-ты поля F являются корнями уравнения $x^q - x \in \mathbb{F}_p[x] \Rightarrow F$ — поле разложения уравнения $x^q - x$ над $\mathbb{F}_p = \mathbb{F}_p$. В силу т. 11.1.7 (см. АН-71) поле F единственно с точностью до изоморфизма.

2) Пусть F — поле разложения уравнения $f(x) = x^q - x$ над \mathbb{F}_p , где $q = p^n$. Так $f'(x) = qx^{q-1} - 1 = -1$ над $\mathbb{F}_p \Rightarrow f(x)$ не имеет крат. корней (см. напр. упр 5.3.3 из [ВЛМ]).
Корни этого уравнения (их q штук) $\mathcal{L} = \{x \in F \mid x^q = x\}$
(Ф-ГБТ-3А Проб.)

— это невозв. точки аб-зла φ^n . Но тогда L — это
нормальное поле F (опять $(x-y)^{p^n} = x^{p^n} - y^{p^n}$ и т.п.).

Поскольку F — минимальное расширение поля \mathbb{F}_p ,
содержащее все корни мин-го $f(x)$, имеем $L = F$,
 $\Rightarrow |F| = q = p^n$.

Перед доказ-вом 4) Выведем следствие из п. 3)

Следствие Для любого p и $\forall n \in \mathbb{N}$ существуют мин-
мн-н $h(x) \in \mathbb{Z}_p[x] : \deg h = n$.

Д-во: $|F^*| = q-1 < p \Rightarrow F^* = \langle \alpha \rangle$ — циклическая (см.
т. 9.3.6 из АН-53) $\Rightarrow F = \mathbb{Z}_p(\alpha) \Rightarrow \exists h \in \mathbb{Z}_p[x] :$
 $\deg(h) = n$ и $h(\alpha) = 0$.

Вернемся к д-ву т-нн:

4) В ауг. прес. 1 $\varphi: x \mapsto x^p$ -абт-зм наса $F = \mathbb{F}_q = \mathbb{Z}_p(\alpha)$, где α из следствия. В частности, $\alpha^q = \alpha^p$. Т.к.

$F = \langle \alpha \rangle$, то φ однозначно опис-ся тем, куда он переборм α .

Имеет $\{\varphi, \varphi^2, \dots, \varphi^{n-1}, \varphi^n = \text{id}\} \subseteq \text{Aut}(F)$ (они различны т.к. $\alpha^{p^k} = \alpha^{p^l} \Leftrightarrow k \equiv l \pmod{n}$, проверьте!).

С группой сопр. см. лемму в 1-ве т. 7 из AN-71, число разл. автоморфизмов = числу корней в F мн-ва $h = m_\alpha$ из следствия, т.е. $\leq n$. \square

Следствие $|\text{Aut}(\mathbb{F}_{p^n})| = n$, в частности, $|\text{Aut}(\mathbb{Z}_p)| = 1$.

Пример Египет. неразр. над \mathbb{Z} мн-н с. 2 $h = x^2 + x + 1$, в этом $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$, где α - корень $h(x)$. С гр. сопр., \mathbb{F}_4 - поле разложения $x^4 - x = x(x-1)(x^2+x+1)$ над \mathbb{F}_2 .

Как замкнул эл-тн из $F = \mathbb{F}_4$. Умеем $F \cong \mathbb{F}_2[x]/(h)$
 $\Rightarrow \mathbb{F}_4 = \{0 + (h), 1 + (h), x + (h), x+1 + (h)\} = \{0, 1, \bar{x}, \bar{x}+1\}$
 Умеем $\bar{x}^2 = (x + (h))(x + (h)) = x+1 + (h) = \overline{x+1}$
 и $\bar{x}^3 = \overline{x+1} \bar{x} = \bar{1}$. В частности, $F^* = \langle \bar{x} \rangle$ и
 от-е $\varphi: a \mapsto a^2$ — единств. нетрив. авт-зм поля \mathbb{F}_4 .

Упр 1 Найдите неразл. мн-ки ст. 2 над \mathbb{F}_3 и
 ст. 3 над \mathbb{F}_2 и постройте поля корня 9 и 8.
 Найдите порождающие их мульт. группы и авт-змы.

Прем 2 Поле Галуэ хар-ки p содержит вместе
 с каждым своим эл-том ровно один корень p -ой
 степени из H_{p^n} .

Упр 2 А-те предл 2.

Предп 3 Пусть $K = GF(p^k)$ и $M = GF(p^m)$.

Тогда K изоморфизм по отношению поля $M \Leftrightarrow K \mid m$.

Упр 3 Д-те, предп 3.

Пусть $F = \bigcup_{n=0}^{\infty} GF(p^n)$, причем, если $k \mid m$, то мы считаем, что $GF(p^k)$ поглотит поле $GF(p^m)$. Оп-н операции на F по след. правилу, если $x \in GF(p^k)$ и $y \in GF(p^m)$, то $x, y \in GF(p^l)$, где $l = \text{НОК}(k, m)$ и $x+y, x \cdot y$ вычисляются как операции в $GF(p^l)$.

Упр 4 Д-те, что а) отн-но этих операций F -поле,

б) F -алгебраическое замыкание поля F_p .

(и в частности, само алгебр. замкнуто)