3 Поля

3.1 Расширение полей

Теорема 1. *Пусть F - поле, $P(X) \in F[X]$ - неприводим над F. Если α - корень$P(X)$ в некотором расширении E поля F, то $F(\alpha) \cong {}^{F[X]}/_{(P(X))}$. Кроме того, если $\deg P = n$, то $\forall$ элемент из $F(\alpha)$ единственным образом представим в слудеющем виде: $c_{n-1}\alpha^{n-1} + c_{n-2}\alpha^{n-2} + ... + c_1\alpha + c_0$*

Доказательство. Рассмотрим φ : $\left.\begin{array}{l} F[X] \to F(\alpha) \\ f(X) \to f(\alpha) \end{array}\right\} \Rightarrow \varphi$ - гомоморфизм колец $\Rightarrow Ker\ \varphi = (P(X))$
α - корень $P(X)$ в некотором расширении $F(\alpha) \Rightarrow P(\alpha) = 0 \Rightarrow P(X) \in Ker\ \varphi \Rightarrow (P(X)) \subset Ker\ \varphi$
$\left.\begin{array}{l} F[X] \text{ - кольцо главных идеалов} \\ P(X) \text{ - неприводим} \end{array}\right\} \Rightarrow (P(X))$ - максимальный в $F[X] \Rightarrow \forall$ другой идеал из $F[X]$ будет содержаться в $(P(X)) \Rightarrow Ker\ \varphi \subset (P(X))$
$\Rightarrow Ker\ \varphi = (P(X))$
Если $\left.\begin{array}{l} Im\ \varphi = F(\alpha) \\ Ker\ \varphi = (P(X)) \end{array}\right\} \Rightarrow {}^{F[X]}/_{Ker\ \varphi} \cong Im\ \varphi \Rightarrow {}^{F[X]}/_{(P(X))} \cong F(\alpha)$
$h(X) \in {}^{F[X]}/_{(P(X))} \Rightarrow h(x) + (P(X)) = c_{n-1}X^{n-1} + c_{n-2}X^{n-2} + ... + c_1X + c_0 + (P(X)) \overset{x=\alpha}{\longrightarrow} c_{n-1}\alpha^{n-1} + c_{n-2}\alpha^{n-2} + ... + c_1\alpha + c_0 + 0, c_i \in F$ □

Следствие 1. *Пусть F - поле, $P(X) \in F[X]$ - неприводим над F. Если α - корень $P(X)$ в некотором расширении E поля F и β - корень $P(X)$ в некотором расширении E' поля F, то $F(\alpha) \cong F(\beta)$*

Лемма 1. *Пусть F - поле, $P(X) \in F[X]$ - неприводим над F. Если α - корень $P(X)$ в некотором расширении E поля F. Если φ - изоморфизм полей: $F \to F'$ и β - корень $\varphi(P(X))$ в некотором расширении E' поля F', то $\exists$ изоморфизм: $F(\alpha) \to F'(\beta)$*

Доказательство. Так как $P(X)$ - неприводим над $F \Rightarrow \varphi(P(X))$ - неприводим над F'
Необходимо доказать: $\underbrace{{}^{F[X]}/(P(X))}_{f(\alpha)} \to \underbrace{{}^{F'[X]}/_{(\varphi(P(X)))}}_{F'(\beta)}$
$f(X) + (P(X)) \to \varphi(f(X)) + (\varphi(P(X)))$
По предыдущей теореме $F(\alpha) \cong F'(\alpha)$ □

Теорема 2. *Пусть $\varphi F \to F'$ - изоморфизм полей $f(X) \in F[X]$. Если E - поле разложения многочлена f над F и E' - поле разложения многочлена $\varphi(f)$ над F', то $\exists$ изоморфизм $E \cong E'$*

Следствие 2. *Любые два поля разложения одного многочлена изоморфны*

Корни неприводимых многочленов

Определение 1. *Пусть $f(X) = a_nX^n + ... + a_1X + a_0 \in F[X]$. Производной многочлена $f(X)$ называется многочлен $f'(X) = na_nX^{n-1} + ... + 2a_2X + a_1 \in F[X]$*

Лемма 2. *Пусть $f(X), g(X) \in F[X]$ и $\alpha \in F$. Тогда:*

1. $(f+g)' = f' + g'$
2. $(\alpha \cdot f)' = \alpha \cdot f'$
3. $(f \cdot g)' = f' \cdot g'$

Теорема 3. *Многочлен $f(X)$ над полем F имеет кратные корни в некотором расширении $\Leftrightarrow$ $f(X)$ и $f'(X)$ имеют общий множитель положительной степени в $F[X]$*

Теорема 4. *Пусть $f(X)$ - неприводим над полем F. Если $char\ F = 0$, то $f(X)$ не имеет кратных корней. Если $char\ F \neq 0$, то $f(X)$ имеет кратные корни, если $f(X) = g(X')$ для некоторого $g(X) \in F[X]$*

Определение 2. *Поле F называется совершенным, если* $\left[\begin{array}{l} char\ F = 0 \\ \left\{ \begin{array}{l} char\ F = P \\ F^p = \{\alpha^p \big| \alpha \in F\} = F \end{array} \right. \end{array} \right.$

Теорема 5. *Любое конечно поле является совершенным*

Теорема 6. *Если $f[X]$ - неприводимо над совершенным полем F, то $f(X)$ не имеет кратных корней*

Теорема 7. *Пусть $f(X)$ - неприводим над F. E - поле разложения $f(x)$ над F. Тогда все корни многочлена $f(X)$ в E имеют одинаковую кратность*

Следствие 3. *$f(X) = \alpha(X-\alpha_1)^n(X-\alpha_2)^n...(X-\alpha_m)^n$, где $\alpha_i \in E, \alpha \in F$*