

Lecture # 12 (11/12/2024)

Recall $f(x) \in \mathbb{F}_p[x]$, $\deg f = n$ irred.



- f divides $x^{p^n} - x$

AND

- $\gcd(f, x^{p^{n/q}} - x) = 1 \quad \forall q \text{ prime divisor of } n$

example

$f(x) = x^3 + 4x^2 + x + 2$ is irreducible $\mathbb{F}_5$

$p = 5, n = 3$ (of course it suffices to check $\nexists$ roots)

- $x^{p^n} - x =$ product of all monic irred. pol. in $\mathbb{F}_p[x]$ of deg d for all $d \mid n$.

need $\underbrace{f \text{ divides } x^{p^3} - x}_{???}$ & $\gcd(f, x^5 - x) = 1$

Recall that this splits!

$$x^5 - x = x(x-1)(x-2)(x-3)(x-4) \pmod{5}$$

"A more direct approach":

- It is clear that $f(x)$ has no linear factors $/\mathbb{F}_5$.

Just plug-in $x = 0, 1, \dots, 4$ and check none of these are roots.

- Can it contain a quadratic factor? (monic)
No! Otherwise, it would contain a linear factor...

Still, note that
irred. quadratics $/\mathbb{F}_5$ must be factors of

$$x^{5^2} - x = x^{25} - x$$

$\exists$ 10 irred. quadratics $/\mathbb{F}_5$ we can list

these and check that none divide f ...

example $x^4 + x^3 + 2x^2 + 2x + 2 \quad / \mathbb{F}_3$

$$p=3, n=4$$

$$\bullet f \text{ divides } x^{3^4} - x$$

$$\bullet \gcd(f, x^{3^2} - x) = 1$$

no root $\Rightarrow$ no cubic factor

• a quadratic must divide $x^{3^2} - x$

Recall Take $f(x) \in \mathbb{Z}[x]$. Assume $\exists p$ prime s.t. $\deg f \bmod p = \deg f$ & f is irred. $\bmod p$. Then f is irred. $\bmod \mathbb{Q}$.

example $f(x) = x^3 + 7x^2 + 13x - 4$

$$\Rightarrow \bmod 3 \quad f(x) \equiv x^3 + x^2 + x + 2$$

$\nexists$ roots in $\mathbb{F}_3 \leadsto$ irreducible

Hilbert's irreducibility theorem

For a field K of $\text{char} = 0$, the following conditions are equivalent.

(i) For any $f = f(t, x) \in K(t)[x]$ irreducible,

$\exists$ infinitely many $b \in K$ s.t. $f_b = f(b, x) \in K[x]$ is irreducible.

(ii) For any finite collection of irreducible polynomials $f_1, \dots, f_n \in K(t)[x]$ of $\deg > 1$, $\exists$ infinitely many $b \in K$ s.t. none of the $f_i(b, x)$ s has a root in K .

Fields K satisfying (i) ($\Leftrightarrow$ (ii)) are called Hilbertian or are said to have the Hilbert property.

Today: We want to prove that $\mathbb{Q}$ is Hilbertian.

we follow "Groups as Galois groups: An introduction" by H. VolKlein.

(Chapter 1)

Our (sketch of the) proof will use the following intermediate results.

① Let $p(x, y) \in \mathbb{C}[x, y]$ be of $\deg d \geq 1$ in y and fix $x_0 \in \mathbb{C}$ such that $p(x_0, y)$ is separable of $\deg d$. Then $\exists$ holomorphic functions $\Psi_1, \dots, \Psi_d$ defined in neighborhood $\mathcal{U}$ of x_0 such that $x \in \mathcal{U} \Rightarrow p(x, y) \in \mathbb{C}[y]$ has the n distinct roots $\Psi_1(x), \dots, \Psi_d(x)$.

② Given $n_0 \in \mathbb{Z}$ and

$$\Psi(t) = \sum_{i=n_0}^{\infty} a_i t^i$$

a Laurent series $(/\mathbb{C})$ with a positive radius & around 0 of convergence, let

$$B(\Psi) := \{ b \in \mathbb{N}; \Psi(1/b) \in \mathbb{Z} \}.$$

Assume that $\Psi(t)$ is not a Laurent polynomial.

Then $\exists 0 < \alpha < 1$ s.t. for almost all $N \in \mathbb{N}$ we have that

$$\# B(\Psi) \cap \{1, \dots, N\} \leq N^\alpha$$

$\leadsto$ We say that $\mathcal{B}(\Psi)$ is sparse.

(3) If $f(t, x) \in \mathbb{Q}(t)[x]$ is irred. over $\mathbb{Q}(t)$ of $\deg_d > 1$ (in x). Then for almost all $b \in \mathbb{Z}$ the following hold.

a) $\exists \varepsilon > 0$ and $\Psi_1(t), \dots, \Psi_d(t)$ (as in (1)) such that $\Psi_1(t), \dots, \Psi_d(t)$ are the roots of $f(b+t, x) \quad \forall |t| < \varepsilon$.

b) If $\Psi_i \in \mathbb{C}(t)$ for some i , then $\exists$ only finitely many $q \in \mathbb{Q}$ s.t. $\Psi_i(q) \in \mathbb{Q}$

c) Let $M = \left\{ a \in \mathbb{N}; f(b + 1/a, x) \text{ has a root in } \mathbb{Q} \right\}$

Then M is sparse.

proof that $\mathcal{Q}$ is Hilbertian

Choose $f_1, \dots, f_n \in \mathbb{Q}(t)[x]$ as in (ii) (page 2/3)
& choose b that works $\forall f_i$

Let $A = \{a \in \mathbb{N}; \text{none of the } f_i(b + 1/a, x) \text{ has a root in } \mathbb{Q}\}$

and let $B = \mathbb{N} \setminus A$. Then, by (3) c),

B is a finite union of sparse sets, hence sparse. But then A must be infinite.

(A finite $\Rightarrow A$ sparse $\Rightarrow \mathbb{N}$ sparse $\exists$)



proof of (3) b)

First, note that for almost all $b \in \mathbb{Z}$, $f(b, x)$ is separable. So, we restrict to such b s.

If some Ψ_i is rational, we have that $\Psi_i \in \overline{\mathbb{Q}}(t)$. But the letting Ψ_i^β be the rational function obtained by applying $\beta \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ to the coeff. of Ψ_i , we have that $\Psi_i^\beta(q) = \Psi_i(q) \quad \forall q \in \mathbb{Q} \text{ s.t. } \Psi_i(q) \in \mathbb{Q}$.
 if $\exists \infty$ many such q s, $\Psi_i^\beta = \Psi_i \quad \forall \beta \Rightarrow$
 $\Psi_i \in \mathbb{Q}(t) \Rightarrow \Psi_i(t-b) \in \mathbb{Q}(t)$ is a root of $f(t, x) \quad \exists$

* to prove (3) c) we need (2).

* (2) (or a version of it) will be in the worksheet.

Proposition Let K be a Hilbertian field and L/K a field extension.

(i) If $[L:K] < \infty$, then L is Hilbertian.

(ii) If L/K is simple purely transcendental then L is Hilbertian.

→ Every f.g. extension of K is Hilbertian

proof Let M a Galois closure of L/K .
and G the corresp. Galois group.

(i) Take $f(t, x) \in L(t)[x]$ irred. monic in x .

In $M(t)[x]$ we can write

$$f = f_1 \cdots f_m \quad \text{with } f_i \text{ monic, irred.} \\ \text{all distinct, conjugate / } L$$

Now, $\exists \varphi_i \in M(t)$ s.t. letting $g_i(t, x) = f_i(t, x + \varphi_i(t))$ we have that

$$\tilde{g}_i(t, x) := \prod_{\sigma \in G} \sigma g_i \in K(t)[x] \text{ is irred.}$$

(If $M = L(\alpha)$, you may take $\varphi_i(t) = t^N + \alpha t^{N-1}$
 for some large $N = N(i)$)

Since K is Hilbertian $\exists$ infinitely many
 $b \in K$ s.t. $\tilde{g}_i(b, x)$ is irreducible.

But then each $g_i(b, x)$, hence each
 $f_i(b, x) = g_i(b, x - \varphi(b))$ is irreducible
 in $M[x]$. These are all distinct and
 conjugate $/L$ so their product $f(b, x)$
 is irred. in $L[x]$.

(Here, we consider only the b s that work $\forall i$)

Next time:

L/K alg. normal + separable

$$\text{Aut}(L/K) \longrightarrow \prod_{\substack{F/K \\ \text{finite} \\ \text{Galois}}} \text{Gal}(F/K)$$