# Lecture # 12 (04/12/2025)

Recall from last time ...

- $f \in \mathbb{Z}[x]$. When is $f$ irreducible / $\mathbb{Q}$?

Useful: If $\exists$ $p$ prime s.t. $\deg f \bmod p = \deg f$ and $f$ is irred. / $\mathbb{F}_p$, then $f$ is irred. / $\mathbb{Q}$

- Theorem (Dedekind) Let $f(x) \in \mathbb{Z}[x]$ be monic & irreducible / $\mathbb{Q}$ of deg $n$. Pick a prime $p$ that does not divide $\Delta(f)$.

  Write $f \equiv \prod_{i=1}^{k} g_i \bmod p$ with each $g_i$ monic & irred and let $d_i = \deg g_i$. Then $G$ contains a cycle of type $(d_1, \cdots, d_k)$.

  (a product of $k$ - disjoint cycles of length $d_i$)

  $\rightsquigarrow$ When is $f$ / $\mathbb{F}_p$ irreducible?

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

$\Updownarrow$

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

AND

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

Recall that this splits!

$x^5 - x = x(x-1)(x-2)(x-3)(x-4) \mod 5$

"A more direct approach":

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

  Just plug-in $x = 0, 1, \ldots, 4$ 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 $x^4 + x^3 + 2x^2 + 2x + 2$ $/\mathbb{F}_3$

$p = 3$, $n = 4$

- $f$ divides $x^{3^4} - x$
- $\gcd(f, x^{3^2} - x) = 1$

no root $\Rightarrow$ no cubic factor

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

What are the quadratics $/\mathbb{F}_3$?

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

$\Rightarrow$ / $\mathbb{F}_3$ $f(X) \equiv x^3 + x^2 + X + 2$

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

---

## Hilbert's irreducibility theorem

For a field $K$ of 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 $f_1, \ldots, f_n \in K(t)[x]$ of deg $> 1$, $\exists$ infinitely many $b \in K$ s.t. none of the $f_i(b,x)$s has a root in $K$.

**Definition**

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 $\Psi_1, \ldots, \Psi_d$ defined in neighborhood $\mathcal{U}$ of $x_0$ such that $x \in \mathcal{U} \Rightarrow p(x,y) \in \mathbb{C}[y]$ has the $d$ distinct roots $\Psi_1(x), \ldots, \Psi_d(x)$.

② Given $n_0 \in \mathbb{Z}$ and

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

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

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

Assume that $\Psi(t)$ is <u>not</u> a Laurent polynomial. Then $\exists\ 0 < \alpha < 1$ s.t. for almost all $N \in \mathbb{N}$ we have that

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

$\rightsquigarrow$ We say that $\mathcal{B}(\Psi)$ is <u>sparse</u>.

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 $\Psi_1(t), \ldots, \Psi_d(t)$ (as in ①) such that $\Psi_1(t), \ldots, \Psi_d(t)$ are the roots of $f(b+t, x)$ $\forall\ |t| < \varepsilon$.

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

Then $M$ is sparse.

proof that $\mathbb{Q}$ is Hilbertian

Choose $f_1, \ldots, f_n \in \mathbb{Q}(t)[x]$ as in (ii) (page 4) & choose $b$ that works $\forall f_i$ as in ③

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

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 $\psi_i$ is rational, we have that $\psi_i \in \overline{\mathbb{Q}}(t)$. But the letting $\psi_i^\beta$ be the rational function obtained by applying $\beta \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ to the coeff. of $\psi_i$, we have that $\psi_i^\beta(q) = \psi_i(q) \quad \forall q \in \mathbb{Q}$ s.t. $\psi_i(q) \in \mathbb{Q}$.

if $\exists$ $\infty$ many such $q$s, $\psi_i^\beta = \psi_i \ \forall \beta \Rightarrow$

$\psi_i \in \mathbb{Q}(t) \Rightarrow \psi_i(t - b) \in \mathbb{Q}(t)$ is a root of $f(t, x)$ ?

* 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.

$\rightsquigarrow$ 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

$$f = f_1 \cdot \ldots \cdot f_m$$ with $f_i$ monic, irred. all distinct, conjugate / $L$

Now, $\exists\, \varphi_i \in M(t)$ s.t. letting $g_i(t,X) =$

$= f_i(t, X + \varphi(t))$ we have that

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

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

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

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