Lecture 6.2

Last time:

- If F is a field and $x^2 - \alpha \in F[x]$ is irreducible, then

$$F(\sqrt{\alpha}) = F[x]/(x^2 - \alpha)$$

is a field extension of F of degree 2.

- Degree 2 field extensions in characteristic 2 must be constructed more carefully, e.g.

$$\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2 + x + 1) \quad \text{over } \mathbb{F}_2.$$

Ex 1 Consider the quintic polynomial

$$f(x) = x^5 + \quad \in \mathbb{Q}[x]$$

$f(x) = x - 1$ [illegible]

Since 1 is a root, we have:

$$x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1).$$

By a homework problem,

$$\zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = 0$$

where $\zeta = e^{2\pi i/5}$ is a 5th root of unity in $\mathbb{C}$.

In fact, $1, \zeta, \zeta^2, \zeta^3$ and ζ^4 are all of the roots of $f(x) = x^5 - 1$, so over $\mathbb{C}$,

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

But we don't need to go all the way to $\mathbb{C}/\mathbb{Q}$ to factor x^5-1.

Define "adjoint ζ^k for all $k \geq 1$"

$$\mathbb{Q}(\zeta) = \{ a_0 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3 + a_4\zeta^4 \mid a_i \in \mathbb{Q} \}$$
$$= \text{Span}_{\mathbb{Q}}\{1, \zeta, \zeta^2, \zeta^3, \zeta^4\}$$

Claim: $\mathbb{Q}(\zeta)$ is a field extension of $\mathbb{Q}$.

What is its degree?

Pf: Define a ring homomorphism

$$\varphi: \mathbb{Q}[x] \longrightarrow \mathbb{C}$$

$\varphi: \mathbb{Q}[x] \longrightarrow$

$$p(x) \longmapsto p(\zeta).$$

Thm: • $\operatorname{im}(\varphi) = \mathbb{Q}(\zeta)$.

• $\ker(\varphi) = (x^4+x^3+x^2+x+1)$

◦ irreducible b/c

• no linear factors over $\mathbb{Q}$

• quadratic factors have to be

$$(x-\zeta^j)(x-\zeta^k),$$
$$j \neq k$$

none are over $\mathbb{Q}$.

Therefore by the First Iso. Thm.,

Therefore $\mathbb{Q}[x]/(x^4+x^3+x^2+x+1) \cong \mathbb{Q}(\zeta)$.

Because $x^4+\dots+x+1$ is irreducible,

$\mathbb{Q}(\zeta)$ is a field. □

Finally, x^5-1 factors over $\mathbb{Q}(\zeta)$:

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

Def For any $n \geq 3$, let $\zeta_n = e^{2\pi i/n}$ be an nth root of unity generating the group μ_n. The field

$$\mathbb{Q}(\zeta_n) = \{a_0 + a_1\zeta_n + \ldots + a_k\zeta_n^k \mid a_j \in \mathbb{Q}\}$$

is called the **nth cyclotomic field extension** of $\mathbb{Q}$.

By construction, $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] \leq n$ but if there are any linear relations among the ζ^j, $0 \leq j \leq n$, then the degree is $< n-1$.

Lemma $\mathbb{Q}(\zeta_n)$ is, in fact, a field.

Pf: Let $\Phi_n(x)$ be the irreducible

factor of $f(x) = x^n - 1$ for which

$\Phi_n(\zeta) = 0$.

e.g. for $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$

Then as above, one can show

$$\mathbb{Q}[x]/(\Phi_n) \cong \mathbb{Q}(\zeta_n). \quad \square$$

In general, $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg(\Phi_n)$

which is an interesting number to

compute!

Exercise 1: prove that $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p-1$

when $p \geq 3$ is prime. Do you have a guess what $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ is for n composite?

Def Let $\alpha \in \mathbb{C}$ and consider the evaluation homomorphism

$$\varphi_\alpha : \mathbb{Q}[x] \longrightarrow \mathbb{C}$$
$$p(x) \longmapsto p(\alpha).$$

The kernel of φ_α is a principal ideal $\ker(\varphi_\alpha) = (p_\alpha)$ for some $p_\alpha \in \mathbb{Q}[x]$, called the minimal

polynomial of α over $\mathbb{Q}$. If $p_\alpha = 0$, meaning α is not a root of any element of $\mathbb{Q}[x]$, we say α is transcendental. Otherwise, α is algebraic.

Ex ② $\sqrt{2}$ is algebraic with minimal polynomial $x^2 - 2$.

③ $\frac{1-\sqrt{5}}{2}$ is algebraic since it's a root of $x^2 - x - 1$. Moreover, this polynomial is irreducible over $\mathbb{Q}$, so

it must be the minimal polynomial:

if $x^2 - x - 1 \in (p_\alpha) = \ker(\varphi_\alpha)$ then

$(x^2 - x - 1) \subseteq (p_\alpha)$ but $(x^2 - x - 1)$ is

a maximal ideal, forcing $(x^2 - x - 1) = (p_\alpha)$.

④ e, π, $\sqrt{\pi}$, etc. are transcendental,

but the proofs are hard.

⑤ $\cos\left(\frac{2\pi}{5}\right)$ turns out to be algebraic

(see HW 6).

Lemma Assume $\alpha \in \mathbb{C}$ is algebraic. Then

leading coefficient 1

|

there is a unique monic choice of $p_\alpha(x)$ generating $\ker(\varphi_\alpha)$.

Pf: If $p(\alpha) = 0$ for some $p \in \mathbb{Q}[x]$, let p_α be one of smallest degree.

Dividing through by the leading coefficient, we may assume p_α is monic.

Then $p_\alpha \in \ker(\varphi_\alpha)$ and the Polynomial Division Algorithm implies $(p_\alpha) = \ker(\varphi_\alpha)$.

Now suppose $q_\alpha \in \mathbb{Q}[x]$ is another

monic polynomial of smallest degree generating $\ker(\varphi_\alpha)$.

Then $p_\alpha - q_\alpha$ is a polynomial of strictly smaller degree and

$$p_\alpha(\alpha) - q_\alpha(\alpha) = 0 - 0 = 0,$$

a contradiction. □

Theorem (1) For any algebraic $\alpha \in \mathbb{C}$, the minimal polynomial p_α is irreducible over $\mathbb{Q}$.

(2) for every monic irreducible polynomial $p \in \mathbb{Q}[x]$, there is some algebraic $\alpha \in \mathbb{C}$ with $p_\alpha = p$.

Pf: (1) Suppose $p_\alpha = fg$ for some $f, g \in \mathbb{Q}[x]$. Then

$$0 = p_\alpha(\alpha) = f(\alpha)g(\alpha) \text{ in } \mathbb{C}$$

so $f(\alpha) = 0$ or $g(\alpha) = 0$, say $f(\alpha) = 0$.

Dividing by the leading coefficient, we may assume f is monic.

But p_α is the unique monic polynomial of smallest degree with α as a root,

so $f = p_\alpha$ and $g = 1$.

Therefore p_α is irreducible.

(2) Let $p \in \mathbb{Q}[x]$ be monic and irreducible. By the Fundamental Theorem of Algebra, p has a root $\alpha \in \mathbb{C}$ with minimal polynomial p_α. Then $p \in (p_\alpha)$, i.e. $p = p_\alpha f$ for some $f \in \mathbb{Q}[x]$ but p is irreducible and monic, so $p = p_\alpha$. □

Def A simple (algebraic) extension of

Def A simple (algebraic) extension of $\mathbb{Q}$ is an extension of the form

$$\mathbb{Q}(\alpha) = \bigcap_{\substack{\text{subfields} \\ \alpha \in K \subseteq \mathbb{C}}} K$$

for some (algebraic) $\alpha \in \mathbb{C}$.

Theorem Every simple algebraic extension $K/\mathbb{Q}$ is isomorphic to $\mathbb{Q}[x]/(p)$ for some p, which may be chosen to be the minimal polynomial of some $\alpha \in K$.

Pf: Let $K = \mathbb{Q}(\alpha)$ be a simple extension

and p_α the minimal polynomial of α.

Then $\varphi_\alpha : \mathbb{Q}[x] \longrightarrow \mathbb{C}$ has kernel (p_α)

and since this is a maximal ideal,

$\mathbb{Q}[x]/(p_\alpha)$ is a field.

If we can show $\operatorname{im}(\varphi_\alpha) = K$, the First Isomorphism Theorem will give us

$$\mathbb{Q}[x]/(p_\alpha) \cong K.$$

On one hand, $\alpha = \varphi_\alpha(x) \in \operatorname{im}(\varphi_\alpha)$,

so $K = \mathbb{Q}(\alpha) \subseteq \operatorname{im}(\varphi_\alpha)$.

On the other hand,

$$\operatorname{im}(\varphi_\alpha) = \{ f(\alpha) \mid f \in \mathbb{Q}[x] \}$$

$$= \{ a_0 + a_1\alpha + \dots + a_n\alpha^n \mid q_j \in \mathbb{Q} \}$$

$$\subseteq \mathbb{Q}(\alpha) \quad \text{by ring operations.}$$

So $\operatorname{im}(\varphi_\alpha) = K$. □

Corollary If $\mathbb{Q}(\alpha)/\mathbb{Q}$ and $\mathbb{Q}(\beta)/\mathbb{Q}$ are simple algebraic extensions with $p_\alpha = p_\beta$, then $\mathbb{Q}(\alpha) \cong \mathbb{Q}(\beta)$.

Remark: All of the above definitions and results hold if we replace $\mathbb{Q}$ by any

subfield $K \subseteq \mathbb{C}$. with essentially the same proofs.

Next time: field extension homomorphisms, classifying simple extensions.