Lecture 6.1

Last time:

- A **field extension** is a ring map $\varphi : F \longrightarrow K$ between fields, which is always injective. We write K/F.

- For any field extension K/F, K is an F-vector space.

- The **degree** of K/F is

$$[K : F] = \dim_F K.$$

Ex ① Let F be a field in which 2 does not have a square root, for example $F = \mathbb{Q}$. Then by previous results, $f(x) = x^2 - 2$ is irreducible, so $F[x]/(x^2-2)$ is a field. We will write

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

"F adjoin $\sqrt{2}$"

Formally,

$$F(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in F\}$$

$F(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in F\}$

where $\sqrt{2} = x + (x^2 - 2)$.

Multiplication is given by FOIL:

$$(a + b\sqrt{2})(c + d\sqrt{2}) = ac + ad\sqrt{2} + bc\sqrt{2} + 2bd$$

$$= (ac + 2bd) + (ad + bc)\sqrt{2}.$$

Exercise 1: Check this agrees with coset multiplication in $F[x]/(x^2 - 2)$.

In the field $F(\sqrt{2})$, 2 has a square root that it didn't before:

$$(\sqrt{2})^2 = (x + (x^2-2))^2 = x^2 + (x^2-2)$$

$$= 2 + (x^2-2)$$

since $x^2 - 2 \in (x^2-2)$.

Notice that we have a homomorphism

$$\varphi : F \hookrightarrow F(\sqrt{2})$$

$$a \longmapsto a = a + 0\sqrt{2}.$$

So $F(\sqrt{2})/F$ is a field extension

and we see that $[F(\sqrt{2}) : F] = 2$.

Compare this to $\mathbb{C}/\mathbb{R}$:

$$\mathbb{C} = \mathbb{R}[x]/(x^2+1)$$

$$= \{a+bi \mid a, b \in \mathbb{R}\}.$$

② More generally, a **quadratic extension** of F is a field extension $F(\sqrt{\alpha})/F$ where $\alpha \in F$, $\alpha \neq \beta^2$ and

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

$$= \{a+b\sqrt{\alpha} \mid a, b \in F\}.$$

Think: $F(\sqrt{\alpha})$ is the smallest field containing F and a square root of α.

By construction, $[F(\sqrt{\alpha}) : F] = 2$,

as long as $\alpha \neq \beta^2$ for any $\beta \in F$.

The process of constructing a field extension of F in which $x^2 - \alpha$ has a root is called **adjoining a (square) root of α**, or sometimes adjoining a root of $f(x) = x^2 - 2$.

(3) What happens if we adjoin a root of a different quadratic polynomial, say

$$f(x) = ax^2 + bx + c,$$

for $a, b, c \in F$?

If $b^2 - 4ac$ has a square root,

say $b^2 - 4ac = \beta^2$ for $\beta \in F$,

then $f(x)$ is reducible:

$$f(x) = \left(x - (2a)^{-1}(-b+\beta)\right)\left(x - (2a)^{-1}(-b-\beta)\right).$$

(the quadratic formula!)

In this case, $F[x]/(f)$ is <u>not</u>

a field.

However, if $b^2-4ac \neq \beta^2$ for any $\beta \in F$, then $f(x)$ is irreducible and

$$F(\beta) = F(\sqrt{b^2-4ac}) = F[x]/(f) = \{s+t\beta \mid s,t \in F\}$$

is a field extension of F with

$$[F(\sqrt{b^2-4ac}) : F] = 2.$$

Remark: we need to be able

to take 2^{-1} in the quadratic formula, so this discussion only makes sense if $\operatorname{char} F \neq 2$.

(4) A quadratic extension of $\mathbb{F}_2$ can be found by

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

Indeed, $f(x) = x^2+x+1$ is irreducible (check it!) so F is a field.

If $\varphi : \mathbb{F}_2[x] \longrightarrow F$

$$p(x) \longmapsto p(x) + (f)$$

is the quotient map, then

$$\varphi(f(x)) = 0$$

so it makes sense to say that

"$f(x) = x^2 + x + 1$ has a root in the field F".

Write $f(x) = (x - \alpha)(x - \beta)$ for $\alpha, \beta \in F$.

Claim: $F \cong \{a + b\alpha \mid a, b \in F\}$.

↑ multiplication by FOIL

Exercise 2: Prove it!

Hence $\mathbb{F}_2(\alpha) = \mathbb{F}_2[x]/(x^2 + x + 1)$ is a degree 2 (quadratic) field extension of $\mathbb{F}_2$.

But by definition, if $\mathbb{F}_2(\alpha)$ has dimension 2 as a vector space over $\mathbb{F}_2$,

$$|\mathbb{F}_2(\alpha)| = 4.$$

For this reason, we call $\mathbb{F}_2(\alpha)$ the field with 4 elements and write it $\mathbb{F}_4$.

Warning: $\mathbb{F}_4 \neq \mathbb{Z}/4\mathbb{Z}$ — we showed that $\mathbb{Z}/4\mathbb{Z}$ is not an integral domain, hence not a field.

Question: what about higher degree poly's?

Ex 5 Consider the quintic polynomial

$$f(x) = x^5 - 1 \in \mathbb{Q}[x].$$

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

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

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

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

$j \neq k$

have are over $\mathbb{Q}$.

Therefore by the First Iso. Thm.,

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

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

$\mathbb{Q}(\zeta)$ is a field. $\square$

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

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

D.C. For any $n \geq 3$, let $\zeta = e^{2\pi i/n}$

Def For any $n \geq 2$, let $\zeta_n \in \mathbb{C}$ 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, $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] < n$ 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 3: 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?

Next time: simple extensions.