§1.1. Field extensions.

Warmup: Given $\mathbb{R}$, what should $\mathbb{C}$ be?

$\mathbb{C} = \{a + bi : a, b \in \mathbb{R}, i^2 = -1\}$.

Idea: introduce relations $\Longrightarrow$ take a quotient.

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

So "i" here is x.

But we could have also written

$\mathbb{C} = \{a + bi : a, b \in \mathbb{R}, (-i)^2 = -1\}$.

which is "the" square root of -1?

Basic definitions.

Let K/F be a field extension. (i.e. let $F \subseteq K$ be fields.)

Then K is a vector space over F. (Check the axioms)

The degree of K/F, written $[K:F]$, is the dimension of this vector space. (Can be infinite.)

Ex. $[\mathbb{C} : \mathbb{R}] = 2$.

The characteristic of a field F is the smallest pos integer n with $n \cdot 1_F = 0_F$, if any such exists.
Write it $\mathrm{char}(F)$.

If none exists, say F has characteristic 0.

Claim. If F is any field, $\mathrm{char}(F) = 0$ or is prime.

Proof. If $n \cdot 1_F = 0_F$ with $n = rs$,
$(r 1_F) \cdot (s 1_F) = 0_F$, so $r 1_F = 0_F$ or $s 1_F = 0_F$.

(will stop writing 1_F and 0_F — just 1 and 0.)

S1.2

Note also that if $\mathrm{char}(F) = p$ then $p \cdot a = 0$ for all $a \in F$.

This is because

$$p \cdot a = p \cdot (1 \cdot a) = (p \cdot 1_a) \cdot a.$$

We always get a ring hom $\mathbb{Z} \longrightarrow F$

which is injective iff $\mathrm{char}(F) = 0$.

Examples. $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ is a field of char p.

(A comm ring with no nontrivial ideals is a field.)

$\mathbb{F}_p[x]$ is a ring w/ char p, so take its fraction field.

Constructing fields.

Prop. Let $\varphi : F \longrightarrow F'$ be a hom. of fields.

Then $\mathrm{Ker}(\varphi) = 0$ or F.

Proof. $\mathrm{Ker}(\varphi) \trianglelefteq F$.

Theorem. Let F be a field, and let $p(x) \in F[x]$ be an irreducible polynomial.

Then there exists an extension of F containing a root of $p(x)$.

Proof. Take $K := F[x]/(p(x))$.

$p(x)$ is irreducible, so $(p(x))$ is a maximal ideal

So K is a field.

Look at $F \hookrightarrow F[x] \xrightarrow{\pi} F[x]/(p(x))$

$\pi|_F$ is a field hom sending 1 to 1, so injective by above. Identify F w/ its image in K.

§1.3.

Let $\bar{x} = \pi(x)$, then

$$p(\bar{x}) = \overline{p(x)} \quad (\pi \text{ is a homomorphism})$$
$$= p(x) \pmod{p(x)} \text{ in } F[x]/(p(x))$$
$$= 0.$$

Indeed, can probably see how to get an extension containing all the roots.

Proposition. Let $p(x) \in F[x]$ be irred of deg n. $K = F[x]/(p(x))$.

Let θ be a root of p as constructed above, namely $\theta = x \pmod{(p(x))} \in K$.

Then, a basis for K/F is $1, \theta, \theta^2, \ldots, \theta^{n-1}$

So $[K:F] = n$ and

$$K = \{a_0 + a_1\theta + a_2\theta^2 + \cdots + a_{n-1}\theta^{n-1} \mid a_0, \ldots, a_{n-1} \in F\}.$$

(Also have $K = \{$polynomials in θ w/ coeffs in $F\}$.)
(This is by construction.)

Need to prove spanning and linear independence.

Suppose $g(\theta) = g(x) \pmod{(p(x))} \in K$.
Then since $F[x]$ is Euclidean, can write

$$g(x) = q(x)\,p(x) + r(x)$$
with $\deg r(x) < n$

and $g(x) \pmod{(p(x))} = r(x) \pmod{(p(x))}$
and so $g(\theta) = r(\theta)$ is an F-linear combo of $1, \theta, \theta^2, \ldots, \theta^{n-1}$.

51.4.

If ~~these~~ θ^i were not linearly independent, would have

$$b_0 + b_1\theta + \cdots + b_{n-1}\theta^{n-1} = 0 \quad \text{for some } b_i \in F$$

i.e. $b_0 + b_1 x + \cdots + b_{n-1}x^{n-1} \equiv 0 \pmod{p(x)}$

i.e. $p(x) \mid b_0 + b_1 x + \cdots + b_{n-1}x^{n-1}$ of smaller degree.

So the b_i are all zero.

Examples. 1. Take $F = \mathbb{Q}$, $K = \mathbb{Q}[x]/(x^2+1)$.

Like constructing $\mathbb{C}$, but not over $\mathbb{R}$.

2. Take $F = \mathbb{Q}$, $K = \mathbb{Q}[x]/(x^3-2)$

where $K = \{a + b\theta + c\theta^2 : a, b, c \in \mathbb{Q}, \theta^3 - 2 = 0\}$.

If this is a field, what is $\frac{1}{\theta}$?

Write $\frac{1}{\theta} = a + b\theta + c\theta^2$

$1 = a\theta + b\theta^2 + c\theta^3$

$= a\theta + b\theta^2 + 2c \implies c = \frac{1}{2}, a = 0, b = 0.$

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

Note that a quadratic polynomial is reducible $\iff$ has a root.

Claim. $x^2 + x + 1$ is irreducible.

Proof. $0^2 + 0 + 1 = 1 \neq 0$

$1^2 + 1 + 1 = 3 = 1 \neq 0.$

Write θ for a root.

So $\theta^2 = -\theta - 1 = \theta + 1$.

§1.5.

Example 4. Let $K = \mathbb{Q}[x]/(x^4 + x^2 + 1)$.

Try to repeat computations like above.
Eventually you will get pissed.

Theorem. "Most" polynomials $/\mathbb{Q}$ are irreducible.
Lots of proofs (go to Michael's talks.)

~~Examples~~

Def. Let K/F be a field extension with $a_1 \dots a_n \in K$.
Then $F(a_1, \dots, a_n)$ is, equivalently:
(1) The smallest subfield of K containing F and the a_i's.
(2) The field containing all polynomials in the a_i.

Example. Consider $\mathbb{Q}(i, \sqrt{2}) \subseteq \mathbb{C}$
$= \{ a + bi + c\sqrt{2} + di\sqrt{2} : a, b, c, d \in \mathbb{Q} \}$.
In fact, this is $\mathbb{Q}(i + \sqrt{2})$, the field extension can be generated by one element.

Example. Let $\rho = e^{2\pi i/3}$.
Consider $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\rho\sqrt[3]{2})$, $\mathbb{Q}(\rho^2\sqrt[3]{2})$.
These fields do not coincide.
For example $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$, not true of other two.

BUT:

§ 57.6

Thm. Let F = field, $p(x) \in F[x]$ irred.

In some extension field K, let α be a root of $p(x)$ (i.e. $p(\alpha) = 0$.)

Then,

$$F(\alpha) \cong F[x]/(p(x)).$$

i.e. up to isomorphism, only one way to adjoin roots of irred polys.

So, $\mathbb{Q}(\sqrt[3]{2}) \cong \mathbb{Q}(\rho\sqrt[3]{2})$ for example.

Proof. Consider the ring hom

$$\begin{array}{ccc} F[x] & \longrightarrow & F(\alpha) \\ x & \overset{\varphi}{\longmapsto} & \alpha \end{array}.$$

(i.e. identity on F, map x to α, and extend to polynomials).

Then, $p(x)$ is in the kernel, hence obtain a hom

$$F[x]/(p(x)) \xrightarrow{\varphi} F(\alpha).$$

Both sides are fields since $p(x)$ is irreducible.

Since $\varphi \neq 0$, φ is injective

Since $\alpha \in \mathrm{Im}(\varphi)$, by def of $F(\alpha)$, φ is surjective.

So done!

52.2.

So this means, for example,

$$\mathbb{Q}(\sqrt[3]{2}),\quad \mathbb{Q}(e^{2\pi i/3}\cdot\sqrt[3]{2}),\quad \mathbb{Q}(e^{-2\pi i/3}\cdot\sqrt[3]{2})$$

are algebraically indistinguishable.

Theorem. Given an isomorphism $F \xrightarrow{\varphi} F'$ of fields, $p(x) \in F[x]$ irred.

Let $p'(x) \in F'[x]$ be $\varphi(p(x))$.

(Note: φ induces an iso $F[x] \xrightarrow{\varphi} F'[x]$ also.)

Let α and β be roots of p and p' respectively (in some extension). Then: φ extends to an iso

$$\sigma : F(\alpha) \xrightarrow{\sim} F'(\beta)$$
$$\alpha \longrightarrow \beta.$$

Proof. That was a mouthful, but easy. Proof by picture!

$$\begin{tikzcd}
\alpha & F(\alpha) \arrow[rr, dashed, "\sigma"] \arrow[d, "\sim"] & & F'(\beta) & \beta \\
\bar{x} \arrow[u] & F[x]/(p(x)) \arrow[rr] & & F'[x]/(p'(x)) \arrow[u] & \bar{x} \arrow[u]
\end{tikzcd}$$

This is induced by $\varphi : F[x] \xrightarrow{\sim} F'[x]$ because $\varphi(p(x)) = p'(x)$ and hence $\varphi((p(x))) = (p'(x))$.

By construction, $\alpha \longrightarrow \beta$ and $\sigma|_F = \varphi$.

52.3.

We draw this picture too:

$$\begin{tikzcd} \sigma: & F(\alpha) \arrow[r, "\sim"] \arrow[d, dash] & F'(\beta) \arrow[d, dash] \\ \varphi: & F \arrow[r, "\sim"] & F' \end{tikzcd}$$

Algebraic extensions.

Def. Let K/F be a field extension.

$\alpha \in K$ is <u>algebraic</u> over F if it is the root of some polynomial in $F[x]$. Otherwise it is <u>transcendental</u>.

K/F is algebraic if every $\alpha \in K$ is algebraic $/ F$.

Prop. If $\alpha \in K$ is algebraic over F, there is a unique monic irred polynomial $\min_{\alpha, F}(x) \in F[x]$ with α as a root.

It is called the <u>minimal polynomial</u> of α / F.

Its degree is the degree of α / F.

Proof. Let $I \trianglelefteq F[x] = \{\text{polys } f \text{ with } f(\alpha) = 0\}$.

If α is algebraic, I is a nonzero ideal.

$F[x]$ is a PID, so I has a unique monic generator.

There's your minimal polynomial.

(Note: the proof in DF basically reproves that $F[x]$ is a PID.)

§2.4.

Cor. If α is algebraic over a field F, then

$$F(\alpha) \cong F[x] / (\min_\alpha(x))$$

and so $[F(\alpha) : F] = \deg \min_\alpha(x) = \deg \alpha$.

Example. The minimal polynomial for $\sqrt[3]{2} / \mathbb{Q}$ is $x^3 - 2$.

If p is prime, min poly for $e^{2\pi i/p}$?

It's a root of $x^p - 1$ which is not irreducible.

But $\frac{x^p - 1}{x - 1}$ is, so $e^{2\pi i/p}$ has degree $p-1$.

What about $\sqrt{2} + \sqrt{3}$?

Proposition. The elt. α is algebraic $\longleftrightarrow [F(\alpha) : F] < \infty$

Proof. $\longrightarrow$: α satisfies some polynomial in $F[x]$, so a min poly exists.

$\longleftarrow$ The elements $1, \alpha, \alpha^2, \alpha^3, \alpha^4, \ldots$ are F-linearly dependent.

That gives a polynomial satisfied by α.

Cor. Finite extensions are always algebraic.

~~52.7.~~ 52.5.

Example. Consider $L = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

what is its degree?

$$1 = 1$$

$$\sqrt{2} + \sqrt{3} = \sqrt{2} + \sqrt{3}$$

$$(\sqrt{2} + \sqrt{3})^2 = 5 + 2\sqrt{6}$$

$$(\sqrt{2}+\sqrt{3})^3 = 2\sqrt{2} + 3\sqrt{3} + 6\sqrt{3} + 9\sqrt{2}$$

$$= 11\sqrt{2} + 9\sqrt{3}.$$

$$(\sqrt{2} + \sqrt{3})^4 = (5 + 2\sqrt{6})^2 = 49 + 20\sqrt{6}.$$

Get a relation

$$(\sqrt{2} + \sqrt{3})^4 - 10(\sqrt{2} + \sqrt{3})^2 + 1 = 0$$

So $[L:\mathbb{Q}] = 4$ w/ min poly $x^4 - 10x^2 + 1$.

$1, \sqrt{2}+\sqrt{3}, (\sqrt{2}+\sqrt{3})^2, (\sqrt{2}+\sqrt{3})^3$ is a basis.

We see also that $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ is.

So $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{6})$ are all subfields of deg 2.

Moreover $L = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{2} + \sqrt{3}) = \dots$

We also have

$$x^4 - 10x^2 + 1 = (x - \sqrt{2} - \sqrt{3})(x - \sqrt{2} + \sqrt{3})$$
$$(x + \sqrt{2} - \sqrt{3})(x + \sqrt{2} + \sqrt{3}).$$

52.5 = 53.1.

Theorem. (degrees multiply)

If $F \subseteq K \subseteq L$ are fields then

$$[L:F] = [L:K][K:F].$$

Proof. First assume RHS is finite.

Consider bases for:

L/K $\quad \alpha_1, \dots, \alpha_m$

K/F $\quad \beta_1, \dots, \beta_n$.

Claim. The $\alpha_i \beta_j$ are a basis for L/F.

Spanning: For $x \in L$ we have

$x = a_1 \alpha_1 + \cdots + a_m \alpha_m$ $\quad$ (for $a_1, \dots, a_m \in K$)

$= (b_{1,1} \beta_1 + \cdots + b_{1,n}\beta_n)\alpha_1$

$+ \cdots + (b_{m,1}\beta_1 + \cdots + b_{m,n}\beta_n)\alpha_m$. So done.

(for $b_{i,j} \in F$)

Linear independence.

If the above expression is 0 for some choice of the $b_{i,j}$:

~~[illegible]~~ All $b_{i,1}\beta_1 + \cdots + b_{i,n}\beta_n = 0$ by linear indep of the α_i.

But then the $b_{i,j}$ are all zero by lin. indep of the β_i.

If $[L:K] = \infty$, inf. many elements LI over K.

They will certainly also be LI over F.

If $[K:F] = \infty$, K has inf many elements LI over F.

These elements are also in L.

52.6 = 53.2.

Cor. If L/F finite, and $F \subseteq K \subseteq L$ then
$[K:F] \mid [L:F]$.

Example. Let $L = \mathbb{Q}(\sqrt[5]{2})$.
Degree 5 over $\mathbb{Q}$ because $x^5 - 2$ is irreducible.
If $\mathbb{Q} \subseteq K \subseteq \mathbb{Q}(\sqrt[5]{2})$,
would have $[K:\mathbb{Q}] \mid 5$ so $= 1$ or 5.

But $[L:F] = 1 \Rightarrow L = F$, so this means $K = \mathbb{Q}$
or $K = \mathbb{Q}(\sqrt[5]{2})$.

That is, $\mathbb{Q}(\sqrt[5]{2})$ has no nontrivial proper subfields.

Example. $L = \mathbb{Q}(\sqrt[6]{2})$. $[L:\mathbb{Q}] = 6$.
L contains $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt[3]{2})$ as intermediate subfields.

(anything else ~ ?)

Since $\left.\begin{array}{l}[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}] = 3 \\ [\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2\end{array}\right\}$, $\begin{array}{l}[\mathbb{Q}(\sqrt[6]{2}):\mathbb{Q}(\sqrt[3]{2})] = 2 \\ [\mathbb{Q}(\sqrt[6]{2}):\mathbb{Q}(\sqrt{2})] = 3.\end{array}$

So, e.g. min poly of $\mathbb{Q}(\sqrt[6]{2}) / \mathbb{Q}(\sqrt{2})$ is $x^3 - \sqrt{2}$.
It's not a priori obvious that this irreducible.
But this «does» prove it.

§3.3

Lemma. $F(\alpha, \beta) = (F(\alpha))(\beta)$.

Proof. $\subseteq$: $F(\alpha, \beta)$ is the smallest field containging F, α, β.
$(F(\alpha))(\beta)$ contains F, α, β.

$\supseteq$: $F(\alpha, \beta)$ contains $F(\alpha)$ and β.
$(F(\alpha))(\beta)$ is the smallest field doing so.

Same story with $F(\alpha_1, \alpha_2, \dots, \alpha_n)$. Can adjoin one at a time.
If the α_i are all algebraic, then

$$[F(\alpha_1, \alpha_2, \dots, \alpha_n) : F] < \infty \text{ by "degrees multiply".}$$

Indeed, the $\alpha_1^{r_1} \alpha_2^{r_2} \cdots \alpha_n^{r_n}$ for $0 \le r_i < \deg_F(\alpha_i)$
span the extension.

They might not be linearly independent though, because we need not have

$$[F(\alpha_1, \alpha_2) : F] = [F(\alpha_1) : F][F(\alpha_2) : F].$$

Instead —

Prop. Let K/F field ext. with α algebraic $/F$.
Then

$$[K(\alpha) : K] \le [F(\alpha) : F].$$

Proof. Consider $g(x) = \min_{\alpha, F}(x)$.
Then $g(x) \in F[x] \subseteq K[x]$ with $g(\alpha) = 0$.
So, by construction, $\min_{\alpha, K}(x) \mid \min_{\alpha, F}(x)$ in $K[x]$.
Might or might not be equal.

~~Sec~~ 54.1

So:

~~Theorem~~ Cor. K/F is finite $\longleftrightarrow$ K is generated by a finite number of alg. elts over L.

Proof. $\longrightarrow$: Can choose a basis for K/F.

$\longleftarrow$: Just proved this.

Cor. If α, β algebraic $/F$, so are $\alpha \pm \beta$, $\alpha\beta$, $\frac{\alpha}{\beta}$ $(\beta \neq 0)$.

Proof. They all lie in $F(\alpha, \beta)$ which is finite $/F$. Finite extensions are algebraic.

Cor. Let L/F be arbitrary. Then $\{\alpha \in L : \alpha \text{ is algebraic} / F\}$ is a subfield of L.

Example. Consider $\mathbb{C}/\mathbb{Q}$ and let $\overline{\mathbb{Q}}$ be the subfield of algebraic numbers.

Since $\sqrt[n]{2} \in \overline{\mathbb{Q}}$ for all $n \in \mathbb{Z}^+$,

$$[\overline{\mathbb{Q}} : \mathbb{Q}] \geq [\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n \text{ for all } n.$$

So $[\overline{\mathbb{Q}} : \mathbb{Q}]$ is infinite.

~~[illegible]~~ 54.2

Thm. If K is algebraic $/F$ and L is algebraic $/K$, then L is algebraic $/F$.

Proof. If $\alpha \in L$, we have

$$a_n \alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1 \alpha + a_0 = 0 \quad (a_i \in K)$$

So α is finite over $F(a_n, a_{n-1}, \ldots, a_0)$ which is finite over F. So α is finite over F, hence algebraic.

Composita:

Def. If K_1 and K_2 are subfields of some field K, then the <u>compositum</u> K_1K_2 is the smallest subfield of K containing K_1 and K_2.

For example, if $K_1 = F(\alpha_1)$, $K_2 = F(\alpha_2)$,
then $K_1K_2 = F(\alpha_1, \alpha_2)$

and more generally if $K_1 = F(\alpha_1, \ldots, \alpha_n)$
$K_2 = F(\beta_1, \ldots, \beta_m)$

then $K_1K_2 = F(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m)$.

Example. The compositum of $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt[3]{2})$ is $\mathbb{Q}(\sqrt[6]{2})$.

(Prove in your head)

54.3.

Proposition. If $F \le K_1, K_2 \le K$ with K_1, K_2 finite then
$$[K_1K_2 : F] \le [K_1 : F][K_2 : F].$$

Proof (sketch). Same ideas as before. (Exercise!)

Indeed, if $[K_1 : F]$ and $[K_2 : F]$ are coprime we must have equality.

$$\begin{tikzcd}
 & K_1K_2 & \\
K_1 \arrow[ur, dash, "\le n"] & & K_2 \arrow[ul, dash, "\le m"'] \\
 & F \arrow[ul, dash, "m"] \arrow[ur, dash, "n"'] &
\end{tikzcd}$$

This diagram means, $m = [K_1 : F]$, $n = [K_2 : F]$.

By "degrees multiply", have $m \mid [K_1K_2 : F]$ and $n \mid [K_1K_2 : F]$.

Since they are coprime, $mn \mid [K_1K_2 : F]$.

Splitting fields:

Given F = field, $f \in F[x]$.

Then, an extension K/F is a splitting field for f if:

- f "splits completely" (factors into linear factors) in K
- This is not true of any subextension.

Example. The splitting field of $x^3 - 2 / \mathbb{Q}$ is
$$\mathbb{Q}(\zeta_3, \sqrt[3]{2}) = \mathbb{Q}(\sqrt{-3}, \sqrt[3]{2}).$$

54.4.

Theorem. They exist:

First of all, some extension K/F exists containing all roots of f.

Choose an irreducible $\deg \geq 2$ factor f' of f.

Take $F_1 = F[x]/(f')$.

Then f' has a root, write $f = (x - \alpha_1) \cdot f''$ in F_1.

Repeat over F_1, until f'' has been factored completely.

Labeling the roots $\alpha_1, \dots, \alpha_n$, $F(\alpha_1, \dots, \alpha_n)$ is the splitting field.

Example. Splitting field of $x^4 + 4$.

$$x^4 + 4 = (x^2 + 2x + 2)(x^2 - 2x + 2)$$

And the four roots are $\pm 1 \pm i$.

So splitting field is $\mathbb{Q}(i)$, deg $2/\mathbb{Q}$.

Example. Splitting field of $x^n - 1$ is $\mathbb{Q}(\zeta_n)$

$\zeta_n := e^{2\pi i/n}$.

The roots are $1, \zeta_n, \zeta_n^2, \dots, \zeta_n^{n-1}$.

Proposition. A splitting field of $f(x)$ of deg n/F has degree at most $n!$ over F.

Read the above proof carefully!

Induction $\Rightarrow$ split off one factor, have a deg $n-1$ factor left.

§4.5 = §5.1

A technical theorem.

Let $\varphi : F \xrightarrow{\sim} F'$ be an iso
$\qquad\quad f \longrightarrow f'$.

Let E and E' be splitting fields for f over F, f' over F'.

Then, φ extends to an iso $E \xrightarrow{\sim} E'$.

Proof. Induct on $n = \deg(f)$.

Can assume f has a factor $\underset{p}{\wedge}$ irred of $\deg \geq 2$. (else $E = F$, $E' = F'$)

Then let $\alpha \in E$ be a root of p
$\beta \in E'$ be a root of p'.

By previous theorem, can extend φ to an iso

$$\begin{array}{ccc} \varphi : F(\alpha) & \xrightarrow{\sim} & F'(\beta) \\ | & & | \\ \varphi : F & \xrightarrow{\sim} & F' \end{array}$$

sending $\alpha \longrightarrow \beta$.

Then, take $f_1 = f/(x-\alpha)$,
$f_1' = \varphi(f) = f'/(x-\beta)$

E and E' are the splitting fields for f_1 and f_1' over $F(\alpha)$ and $F'(\beta)$.

By induction, the top φ extends to $E \xrightarrow{\sim} E'$.

Cor. Any two splitting fields for $f \in F[x]$ are isomorphic.

§4.6 ≈ §5.2.

Def. A field $\bar{F}$ is an algebraic closure of F if $\bar{F}$ is algebraic $/F$ and if every $f \in F[x]$ splits completely over $\bar{F}$.

Def. A field K is algebraically closed if every $f \in K[x]$ splits completely over K.

Examples. $\mathbb{C}$, $\bar{\mathbb{Q}}$, $\bar{\mathbb{F}}_p$, ... (will study!!)

Note. We could have just demanded that every $f \in K[x]$ has a root in K; then apply ~~theorem~~ def. to $f/(x-a)$.

Proposition. Algebraic closures are algebraically closed.

Proof. Given $f(x) \in \bar{F}[x]$ with root a.

Then $\bar{F}(a)$ is alg. $/\bar{F}$, $\bar{F}$ alg. over F, so $F(a)$ alg. over F.

In particular a satisfies a polynomial over F, so $a \in \bar{F}$.

Theorem. Given F, there exists an algebraic closure $\bar{F}$.

Follows if we construct an alg. closed field containing F.

Proof. Uses Zorn's lemma.

For every nonconstant monic $f = f(x) \in F[x]$
associate an indeteminate x_f

Consider $F[\dots, x_f, \dots]$ (adjoin all the x_f)
and the ideal I gen by all the $f(x_f)$.

Claim. I is proper.
Proof. Otherwise have a relation

$$g_1 f_1(x_{f_1}) + \dots + g_n f_n(x_{f_n}) = 1.$$

Write $x_1 = x_{f_1}, \dots, x_n = x_{f_n}$, and $x_{n+1}, \dots, x_m$
other variables in the g_n.
(if any)

Get $g_1(x_1, \dots, x_m) f_1(x_1) + \dots + g_n(x_1, \dots, x_m) f_n(x_n) = 1$.

Let F' be a finite extension of F containing a root α_i
of each f_i.

In the equation above, plug in: $x_i = \alpha_i \quad (i = 1, \dots, n)$
$x_{n+1} = \dots = x_m = 0$.

Get $0 = 1$.

So: I is contained in a maximal ideal M. (Zorn's lemma)

Then $K_1 := F[\dots, x_f, \dots]/M$ is a field.
It contains an isomorphic copy of F.

Every polynomial f has a root.

So are we done?

55.4.

Obtain: K_1/F: every poly in F contains a root

K_2/K_1: every poly in K_1 contains a root

....

Does the madness ever stop?

Choose $K = \bigcup_{j=0}^{\infty} K_j$.

Given $f(x) \in K[x]$, we have $f(x) \in K_i[x]$ for some i. So it has a root in K_{i+1}.

So ~~K~~ K is algebraically closed, contains F, our alg. closure is

$\bar{F} := \{ a \in K : a \text{ is algebraic} / F \}$

Then, given $f \in F[x]$, splits into linear factors $x - a$ in $K[x]$.

Since each a is algebraic over F, in fact this is a splitting over $\bar{F}$.

<u>Theorem</u>. An algebraic closure is unique up to isomorphism.

Omitted / exercise. Same ideas. Use Zorn's lemma.

55.5. (=56.1)

Inseparability:

Consider the field $F = \mathbb{F}_2(t)$
rational functions over $\mathbb{F}_2$.

Then look at polynomials in $F[x]$.

Claim. $x^2 - t$ is irreducible in $F[x]$.

Proof. If it were reducible, would factor.
Could solve $\left(\frac{f(t)}{g(t)}\right)^2 = t$ in $\mathbb{F}_2[t]$

So $f(t)^2 = t \cdot g(t)^2$.

But parity of degrees is wrong.

So, consider the extension field $F(\sqrt{t})$.

Then $x^2 - t = (x - \sqrt{t})^2$.

This is weird. Never happens in characteristic 0!

Def. A polynomial $f \in F[x]$ is called separable if it does not have any multiple roots.

i.e. writing $f = (x - a_1)(x - a_2) \cdots (x - a_n)$ in $\overline{F}[x]$,

(or in $K[x]$ where K is a splitting field for F)

all the a_i are distinct.

Otherwise it is inseparable.

55.6. How to check?
(=56.2)

Prop. A polynomial $f \in F[x]$ has a multiple root a iff a is both a root of f and its <u>derivative</u> f'.

Here the derivative is <u>defined</u> using the power rule. No limits required! Sum, product rules still apply.

Example. Let $f(x) = x^p - 1 \in \mathbb{F}_p[x]$.

Then $f'(x) = p \cdot x^{p-1} = 0$. (Yes, this is weird.)

So any root of f is a multiple root.
In fact, $f(x) = x^p - 1 = (x-1)^p$, so
$\mathbb{F}_p$ <u>does not contain any nontrivial pth roots of unity</u>.

Proof of proposition.

If $f = (x-a)^2 g(x)$, then

$$D_x f = (x-a)^2 \cdot D_x g(x) + 2(x-a) \cdot g(x)$$

a is still a root.

Conversely, if $f = (x-a) g(x)$, then

$$D_x f = g(x) + (x-a) D_x g(x),$$ and

a is a root of this $\Longleftrightarrow$ a is a root of $g(x)$.

55.7 (=56.3)

More examples.

(1) $x^{p^n} - x$ over $\mathbb{F}_p$. Derivative is $p^n x^{p^n - 1} - 1$
$= -1$.

So derivative has no roots so polynomial is separable

(2) $x^n - 1$ has derivative nx^{n-1}.

Separable if and only if $\mathrm{char}(F) \nmid n$.

So, for example, $\mathbb{F}_7$ does have 8 distinct 8th roots of unity.

Prop. In characteristic 0, every irreducible polynomial is separable.

Proof. Let $f \in F[x]$ irred of degree n.
Then $D_x f(x)$ ~~fixed~~ of degree $n-1$.

$D_x f$ and f can't have any common factors in $F[x]$ (since f has no nontrivial factors).

But no common factors ~~o~~in $\bar{F}[x]$ either.
The Euclidean algo works over F!

Remark. In char $\neq 0$, can have $\deg(D_x f(x)) \neq n-1$.
This is what failed before.

But if $D_x f(x) \neq 0$, above proof works, f separable.

In particular, for f to be inseparable, in characteristic p, f must be a polynomial in x^p.

~~55.8~~.56-4.

Proposition. Let char(F) = p, $a, b \in F$,
Then $(a+b)^p = a^p + b^p$, $(ab)^p = a^p b^p$.

In other words, the map $x \longrightarrow x^p$ is a field homomorphism $F \to F$.

Proof. Use the binomial theorem,

$$\frac{p!}{i!(p-i)!} = 0 \text{ in } F \text{ for } 1 \le i \le p-1$$

b/c p doesn't divide the bottom.

Note $x \to x^p$ is injective also.
This map is called the Frobenius endomorphism of F.

If F is finite, then this is indeed an automorphism.

Proposition. An irreducible polynomial over a finite field is seperable.

Proof. Given $f(x) \in \mathbb{F}[x]$ irreducible.
If inseparable, then $f(x) = g(x^p)$ for some g.

But the coefficients of g are all pth powers.

So $g(x^p) = a_n^p (x^p)^n + a_{n-1}^p (x^p)^{n-1} + \cdots + a_0^p$

$= (a_n x^n + \cdots + a_0)^p$.

So $f(x) = (a_n x^n + \cdots + a_0)^p$, not irreducible.

Definition. A field K is called perfect if either:

(1) char(K) = 0
(2) $K = K^p$.

So, over a perfect field, every irred poly is separable.

§6.5.

Existence and uniqueness of finite fields:

Consider $x^{p^n} - x \in \mathbb{F}_p[x]$.

Separable with p^n distinct roots.

In its splitting field, these roots satisfy

$$(\alpha\beta)^{p^n} = \alpha\beta, \quad (\alpha^{-1})^{p^n} = \alpha^{-1}$$

$$(\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta.$$

So the set of roots is closed under field operations.

$\mathbb{F} := \{ \text{roots of } x^{p^n} - x \text{ in } \overline{\mathbb{F}_p} \}$ is a field, w/ p^n elts.

(Note also, every $\alpha \in \mathbb{F}_p$ is in $\mathbb{F}$.)

Why are they unique?

Suppose $\mathbb{F}'$ is some other field w/ p^n elements.

Since $|(\mathbb{F}')^\times| = p^n - 1$, $\alpha^{p^n} = \alpha$ for all $\alpha \in \mathbb{F}'$.

But then α is a root of $x^{p^n} - x$.

So $\mathbb{F}'$ is a splitting field for $x^{p^n} - x$, hence $\mathbb{F}' \cong \mathbb{F}$.

Write $\mathbb{F}_{p^n}$ for this field.

— See DF for a bit of extra structure theory.

More on cyclotomy.

Def. Write $\mu_n := \{n\text{th roots of unity in } \mathbb{C}\}$, a group.

You also see $\mu_n(F) = \{n\text{th roots of unity in } F\}$ (making μ_n a functor and a group scheme ... but never mind)

Then
$$\mathbb{Z}/n\mathbb{Z} \to \mu_n$$
$$a \to \zeta_n^a$$
where ζ_n is: $\begin{cases} e^{2\pi i/n} \\ \text{any primitive root of unity.} \end{cases}$

We clearly have $\mu_d \subseteq \mu_n \iff d \mid n$.

Definition. The nth cyclotomic polynomial $\Phi_n(x)$ is the one whose roots are the primitive roots of unity:
$$\Phi_n(x) = \prod_{\substack{\zeta \in \mu_n \\ \text{primitive}}} (x - \zeta) = \prod_{\substack{a \pmod n \\ (a,n)=1}} (x - \zeta_n^a).$$

By construction $\Phi_n(x)$ has degree $\varphi(n)$ (Euler φ-fn.)

So we have
$$x^n - 1 = \prod_{d \mid n} \prod_{\substack{\zeta \in \mu_d \\ \zeta \text{ primitive}}} (x - \zeta)$$
$$= \prod_{d \mid n} \Phi_d(x),$$
since every nth root of unity is a primitive dth root of unity for exactly one $d \mid n$. (minimal d s.t. $\zeta^d = 1$.)

~~56.7~~ 57.2

Cor. Note that we get $n = \sum_{d|n} \varphi(d)$.

(This says $\underline{n = 1 * \varphi}$ as a convolution of arith functions)

Example. $x^9 - 1 = \Phi_9(x)\,\Phi_3(x)\,\Phi_1(x)$.

$$\Phi_1(x) = x - 1,$$
$$\Phi_3(x) = \frac{x^3 - 1}{x - 1} = x^2 + x + 1.$$
$$\text{So } \Phi_9(x) = \frac{x^9 - 1}{x^3 - 1} = x^6 + x^3 + 1,$$

Proposition. $\Phi_n(x) \in \mathbb{Z}[x]$.

Cheating Proof. Its coefficients are algebraic integers and Galois-invariant.

Non-cheating proof. Induct on n,

$$x^n - 1 = \Big(\prod_{\substack{d|n \\ d<n}} \Phi_d(x)\Big) \cdot \Phi_n(x)$$

By long division, $\Phi_n(x) \in \mathbb{Q}[x]$.
But then the product is monic and in $\mathbb{Z}[x]$ by induction
So by Gauss' Lemma the product is def. / $\mathbb{Z}[x]$.

~~S6.8.~~ 57.3

Theorem. The cyclotomic polynomials are irreducible. (over $\mathbb{Z}[x]$)

Proof. If $\Phi_n(x) = f(x) \cdot g(x)$ in $\mathbb{Z}[x]$,

let $\begin{cases} \zeta \text{ be a primitive root of unity and a root of } f \\ p = \text{any prime not dividing } n. \end{cases}$

Then ζ^p is a root of f or g.

Claim. Can arrange so that ζ^p is a root of g.

Proof 1. Dirichlet's theorem on primes in progressions.

If $(a,n) = 1$ there is a prime $p \equiv a \pmod{n}$.

Proof 2. If ζ^p is a root of f for all primes p and roots ζ of $f \Rightarrow \zeta^a$ is a root of f for all $(a,n)=1$.

But then every primitive root of unity is a root of f.

So $f = \Phi_n$.

The meat. Suppose ζ^p is a root of g.

Then ζ is a root of $g(x^p)$ and f is the min poly of ζ.

So can write $g(x^p) = f(x)\, h(x)$ for some $h(x) \in \mathbb{Z}[x]$.

Reduce modulo p: $\bar{g}(x^p) = \bar{f}(x)\, \bar{h}(x)$ in $\mathbb{F}_p[x]$

But $\bar{g}(x^p) = (\bar{g}(x))^p$, so

$$\bar{g}(x)^p = \bar{f}(x)\, \bar{h}(x)$$

so $\bar{f}$ and $\bar{g}$ have a common factor in $\mathbb{F}_p[x]$.

~~Step~~ 57.4

Now $\Phi_n(x) = f(x)\, g(x)$

And so $x^n - 1$ has a multiple root over $\mathbb{F}_p$.

But we know this not to be the case!

Remark. This technique (reduce to a finite field) is very common in algebraic number theory!

57.5

Geometric Constructions.

Can you square a circle or trisect an angle?

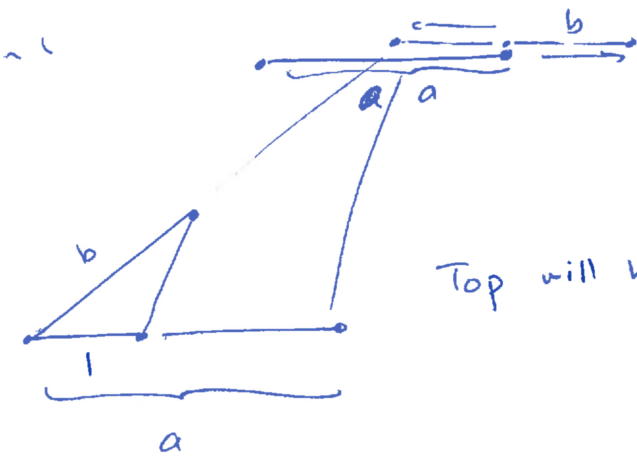
Suppose you have a line segment of length 1.

The constructible numbers (CC, say) are those real numbers x s.t. you can construct a line segment of length x. (and 0 and their negatives)

What can you get?

Addition + subtraction:

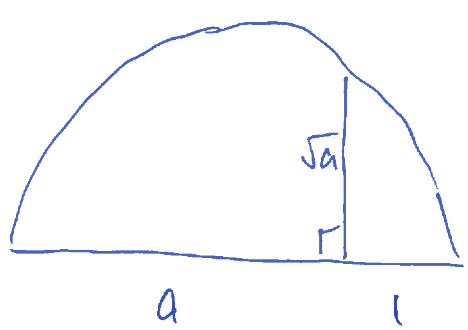
Multiplication:



Top will be ab.

Division:

Square roots:

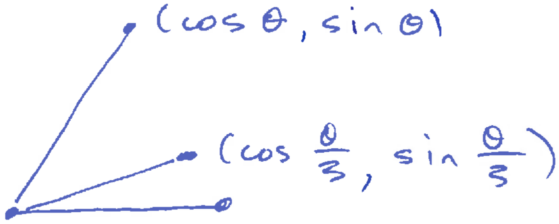


57.7 58.1

Squaring the circle:

$\sqrt{\pi}$ is not algebraic (not obvious, but true)

Trisecting an angle:



If $\cos\theta$ is constructible, is $\cos\frac{\theta}{3}$?

Triple angle formula: $\cos\theta = 4\cos^3\left(\frac{\theta}{3}\right) - 3\cos\left(\frac{\theta}{3}\right)$.

Take, say, $\theta = 60°$, $\cos\theta = \frac{1}{2}$.

Solve $\quad 4\beta^3 - 3\beta - \frac{1}{2} = 0$

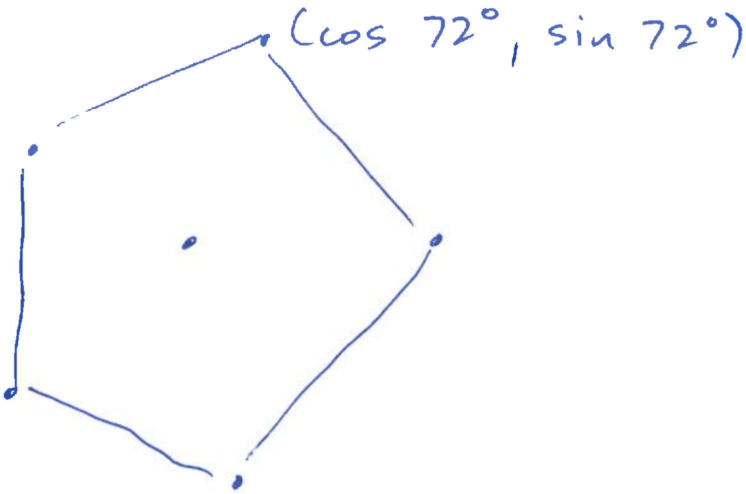
or (with $a = 2\beta$) $\quad a^3 - 3a - 1 = 0$.

Can check: This is irreducible, $[\mathbb{Q}(a) : \mathbb{Q}] = 3$

So no dice.

~~7.28~~. 58.2

Regular pentagons.



Are $\cos 72°$ and $\sin 72°$ constructible?

$$\cos(72°) = \tfrac{1}{2}(\zeta_5 + \zeta_5^{-1})$$
$$\sin(72°) = \tfrac{1}{2}(\zeta_5 - \zeta_5^{-1})$$

So we are asking if $\mathbb{Q}(\zeta_5)$ is constructible.

$[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = 4$ so it could be!

In fact, it is. How to see?

(1) The Gauss sum $\left(\sum_{n \in \mathbb{Z}/5} e^{2\pi i n^2/5} \right)$ equals $\sqrt{5}$.

(Muck around. You'll prove it)

So $\mathbb{Q}(\zeta_5)$ contains a quadratic subfield.

(2) In fact, if $a = 2\cos\left(\frac{2\pi}{5}\right)$, $a^2 + a - 1 = 0$.

Indeed, $\mathbb{Q}(a)$ is contained in $\mathbb{R}$, so must be a proper subfield of $\mathbb{Q}(\zeta_5)$! Quadratic if $a \notin \mathbb{Q}$.

(3) Look up a pentagon!

Edge length is $\sqrt{\frac{5 - \sqrt{5}}{2}}$.

5.8.3.

Galois theory.

Def. If K/F is a field extension,

$\mathrm{Aut}(K/F) = \{$ automorphisms $K \to K$ which fix $F\}$.

(i.e. $\sigma(x) = x$ for all $x \in F$.
Not just $\sigma(F) = F$.)

Then $\mathrm{Aut}(K/F)$ is a group, a subgroup of $\mathrm{Aut}(K)$.

Prop. Given K/F with $\begin{cases} \alpha \in K \text{ algebraic } / F \\ \sigma \in \mathrm{Aut}(K/F). \end{cases}$

Then $\sigma(\alpha)$ is a root of the min poly of α / F.

Proof. We have

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0 \quad \left(\begin{array}{l}\text{min poly of } \alpha, \\ a_i \in F.\end{array}\right)$$

Hit the equation with σ. It's an automorphism.

$$\sigma(\alpha)^n + \sigma(a_{n-1})\,\sigma(\alpha)^{n-1} + \cdots + \sigma(a_0) = 0.$$

But σ fixes all the a_i. so

$$\sigma(\alpha)^n + a_{n-1}\,\sigma(\alpha)^{n-1} + \cdots + a_0 = 0.$$

This means that $\mathrm{Aut}(K/F)$ acts on the set S of roots of this min poly, get a homomorphism

$$\mathrm{Aut}(K/F) \longrightarrow \mathrm{Sym}(S).$$

§8.4.

Example. $\mathbb{Q}(i)/\mathbb{Q}$.

$\mathrm{Aut}(\mathbb{Q}(i)/\mathbb{Q}) = \{$identity, complex conjugation$\}$

a cyclic group of order 2.

Example. $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$.

Let $\sigma \in \mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$.

Then σ is determined by its action on $\sqrt[3]{2}$.

$\sigma(\sqrt[3]{2})$ is a root of $x^3 - 2 = (x - \sqrt[3]{2})\underbrace{(x^2 + \sqrt[3]{2}x + \sqrt[3]{4})}$

Doesn't factor further in $\mathbb{Q}(\sqrt[3]{2})$

So $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = 1$.

Def. Let $H \subseteq \mathrm{Aut}(K)$ be a subgroup (or subset).

Then $\mathrm{Fix}(H)$, the fixed field of H, is

$$\mathrm{Fix}(H) = \{x \in K : \sigma(x) = x \text{ for all } \sigma \in H\}.$$

Then (the following are immediate):

(1) $\mathrm{Fix}(H)$ is indeed a subfield of K

(2) All this is inclusion-reversing:

$$F_1 \subseteq F_2 \subseteq K \implies \mathrm{Aut}(K/F_2) \subseteq \mathrm{Aut}(K/F_1)$$

$$H_1 \subseteq H_2 \subseteq \mathrm{Aut}(K) \implies \mathrm{Fix}(H_2) \subseteq \mathrm{Fix}(H_1).$$

58.5.

Example.

$\mathbb{Q}(i)/\mathbb{Q}$. What is $\mathrm{Fix}(\mathrm{Aut}(\mathbb{Q}(i)/\mathbb{Q}))$?

Set of elements in $\mathbb{Q}(i)$ fixed by complex conjugation.

So just $\mathbb{Q}$.

$\mathbb{Q}(\sqrt[3]{2})$. Since $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = 1$,

$$\mathrm{Fix}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \mathbb{Q}(\sqrt[3]{2}).$$

Now suppose that K is the splitting field for a polynomial $f \in F[x]$. Then the associated hom

$$\mathrm{Aut}(K/F) \longrightarrow \mathrm{Sym}(\text{Roots of } f)$$

is injective, because the action of any $\sigma \in \mathrm{Aut}(K/F)$ is determined by its action on the roots of f (the generators of K/F).

Indeed we can say more.

Prop. If K is the splitting field for some $f \in F[x]$, we have

$$|\mathrm{Aut}(E/F)| \leq [E:F]$$

with equality if f is separable$/F$.

58.6. Why is this true?

Ask how many $\sigma \in \mathrm{Aut}(K/F)$ extend the identity map $F \longrightarrow F$.

More generally: Given

$$\begin{tikzcd} \mathrm{Spl}(f) = E \arrow[d, dash] & \mathrm{Spl}(\varphi(f)) = E' \arrow[d, dash] \\ F \arrow[r, "\varphi"] & F' \end{tikzcd}$$

How many automorphisms extend φ?

Do one root at a time.

Let p be any irreducible factor of f, $p' = \varphi(f)$.

α: any root of p (in E), β: any root of p' (in E')

Then there is a unique extension τ

$$\begin{tikzcd} \tau : F(\alpha) \arrow[r, "\sim"] \arrow[d, dash] & F'(\beta) \arrow[d, dash] \\ F \arrow[r] & F' \end{tikzcd} \qquad \tau(\alpha) = \beta.$$

The number of maps $\tau : F(\alpha) \longrightarrow E'$ sending α to <u>some</u> root of p' is $[F'(\beta) : F'] = [F(\alpha) : F]$ provided all roots of p and p' are distinct.

(i.e. that <u>p is separable</u>)

Keep going, one root at a time, number of distinct automorphisms is $[E : F]$.

§9.1

Def. If K/F is finite, then K/F is <u>Galois</u> (equiv: K is Galois over F) if $|\mathrm{Aut}(K/F)| = [K:F]$. In this case write $\mathrm{Gal}(K/F)$ for $\mathrm{Aut}(K/F)$, the Galois group of K/F.

Cor. If K is the splitting field $/F$ of a separable polynomial f, then K/F is Galois.

Example. $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is Galois over $\mathbb{Q}$, the splitting field of $(x^2-2)(x^2-3)$.

(Verify that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \neq \mathbb{Q}(\sqrt{2})$. So degree 4.)

Any automorphism is determined by action on $\sqrt{2}, \sqrt{3}$:

$\sqrt{2} \to \sqrt{2}$	$\sqrt{2} \to -\sqrt{2}$	$\sqrt{2} \to \sqrt{2}$	$\sqrt{2} \to -\sqrt{2}$
$\sqrt{3} \to \sqrt{3}$	$\sqrt{3} \to \sqrt{3}$	$\sqrt{3} \to -\sqrt{3}$	$\sqrt{3} \to -\sqrt{3}$.
1	σ	τ	

Since $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$, $|\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})| = 4$.

So all these are in fact automorphisms.

Get $\sigma^2 = \tau^2 = 1$, and the right automorphism is $\sigma\tau$ or $\tau\sigma$.

So $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})) \cong C_2 \times C_2$.

<u>Fixed fields</u>:

$\{1\}$	$\mathbb{Q}(\sqrt{2}, \sqrt{3})$
$\{\sigma\}$	$\mathbb{Q}(\sqrt{3})$
$\{\tau\}$	$\mathbb{Q}(\sqrt{2})$
$\{\sigma\tau\}$	$\mathbb{Q}(\sqrt{6})$.

59.2 (= 60.1)

Example. Splitting field K of $x^3 - 2/\mathbb{Q}$.

Let $G = \mathrm{Gal}(K/\mathbb{Q})$.

Then $|G| = 6$.

We have $K = \mathbb{Q}(\sqrt[3]{2}, \rho\sqrt[3]{2}, \rho^2\sqrt[3]{2})$

and $K = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$

and $K = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$.

Note that the latter description lets us know $[K:\mathbb{Q}] = 6$.
(Divisible by 2 and 3.)

Claim. The Galois group $G \cong S_3$.

Why? $\mathrm{Gal}(K/\mathbb{Q}) \hookrightarrow \mathrm{Sym}(3)$
and the image has size 6!

To describe this, let

$$\sigma : \begin{cases} \sqrt[3]{2} \to \rho\sqrt[3]{2} \\ \rho \to \rho \end{cases} \qquad \tau : \begin{cases} \sqrt[3]{2} \to \sqrt[3]{2} \\ \rho \to \bar{\rho} = \rho^{-1} = \rho^2 \\ \qquad\qquad = 1 - \rho. \end{cases}$$

Then $G = \{1, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$.

Now compute $\sigma\tau$ and $\tau\sigma^2$!

Example. $x^p - 2$. (Do ...)

59.3 (= 60.2)

What are the fixed fields of all subgroups of G?

(Work out on board, and draw the picture.)

Example. $\mathbb{Q}(\sqrt[4]{2})$ is not Galois / $\mathbb{Q}$.

$\sqrt[4]{2}$ only has two conjugates over this field!

Example. $\mathbb{F}_{p^n} / \mathbb{F}_p$ is Galois, splitting field of $x^{p^n} - x$.

The map
$$\sigma : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n}$$
$$\alpha \longrightarrow \alpha^p$$

is an automorphism of $\mathbb{F}_{p^n}$ of order n.

Hence it generates $\mathrm{Gal}(\mathbb{F}_{p^n} / \mathbb{F}_p)$.

Example. Consider $F = \mathbb{F}_2(t)[x] / (x^2 - t)$ over $\mathbb{F}_2(t)$.

Then $|\mathrm{Aut}(F / \mathbb{F}_2(t))| = 1$, hence not Galois.

This is because $x^2 - t = (x - \sqrt{t})^2$ in this extension.

We'll aim to prove the F.T. of Galois theory.

Def. A (linear) character χ of a group G with values in a field L is a homomorphism

$$\chi : G \longrightarrow L^\times.$$

Example. You may have seen Dirichlet characters

$$\chi : (\mathbb{Z}/n\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$$

which are then defined as fns. $\chi : \mathbb{Z} \to \mathbb{C}$

by $\chi(a) = \begin{cases} \chi(a \bmod n) & \text{if } (a,n)=1 \\ 0 & \text{otherwise.} \end{cases}$

Def. Chars $\chi_1, \dots, \chi_n$ are linearly independent over L if they are such as fns. on G. No nontrivial rel'n

$$a_1 \chi_1 + \cdots + a_n \chi_n = 0 \qquad (a_i \text{ not all zero}) \; (a_i \in L)$$

as functions on G.

(It is okay if $a_1\chi_1(g) + \cdots + a_n\chi_n(g) = 0$ for some g.)

Theorem. If $\chi_1, \dots, \chi_n$ are distinct characters $G \to L^\times$ then they are linearly independent.

Proof. If not, choose a minimal dependence relation

$$a_1\chi_1 + \cdots + a_m\chi_m = 0$$

(reorder the χ_i if we have to).

60.4

Choose g_0 with $\chi_1(g_0) \neq \chi_m(g_0)$. Then,

$$a_1 \chi_1(g) + \cdots + a_m \chi_m(g) = 0 \qquad (*)$$

$$a_1 \chi_1(g_0 g) + \cdots + a_m \chi_m(g_0 g) = 0$$

and since the characters are multiplicative

$$a_1 \chi_1(g_0)\chi_1(g) + \cdots = 0.$$

Multiply $(*)$ by $\chi_m(g_0)$ and subtract.

$$a_1 (\chi_m(g_0) - \chi_1(g_0))\chi_1(g)$$
$$+ \cdots + a_m \underbrace{(\chi_m(g_0) - \chi_m(g_0))}_{\text{zero!}} \chi_m(g) = 0$$

This is a <u>nontrivial</u> $(a_1(\chi_m(g_0) - \chi_1(g_0)) \neq 0)$ dependence rel'n with fewer coeffs.

<u>Cor.</u> If $\sigma_1, \ldots, \sigma_n$ are distinct embeddings $K \hookrightarrow L$ (including automorphisms $K \to K$ of a field), then they are linearly independent.

(Yes, it's a special case — think about it!)

<u>Theorem.</u> Given a field K
a subgroup $G \subseteq \mathrm{Aut}(K)$
$F = \mathrm{Fix}(G)$.
Then K is Galois over F,
i.e. $[K : F] = |G|$.

60.5 = 61.1 .

Two claims : $[K:F] \geq |G|$ and $[K:F] \leq |G|$.

Claim. $[K:F] \geq |G| =: n$.

If not, choose a basis $w_1 \cdots w_m$ for K/F.

Have a system $\sigma_1(w_j) x_1 + \cdots + \sigma_n(w_j) x_n = 0$.

More equations than unknowns. $(x_i \in K.)$

So, can solve in the x_i; let $\beta_1 \cdots, \beta_n \in K$ be a solution.

If $a_1, \ldots, a_m \in F$ are arbitrary, they are fixed by all σ_i.

Multiply our system by $a_1, \ldots, a_m$ respectively:

$$\sigma_1(a_1 w_1)\beta_1 + \cdots + \sigma_n(a_1 w_1)\beta_n = 0$$

$$\vdots$$

$$\sigma_1(a_m w_m)\beta_1 + \cdots + \sigma_n(a_m w_m)\beta_m = 0$$

Add:

$$\sum_{i=1}^{n} \sigma_i(a_1 w_1 + \cdots + a_m w_m)\beta_i = 0$$

The w_i were a basis for K/F.

So $\sum_{i=1}^{n} \sigma_i(\alpha)\beta_i = 0$ for all $\alpha \in K$.

This means the σ_i are LD, contradicting previous cor.

61.2

Claim. $[K:F] \le |G| = n$.

Suppose instead that $n < [K:F]$.

Choose $n+1$ F-lin. indep. elts α_i of K, and look at

$$\sigma_1(\alpha_1)x_1 + \cdots + \sigma_1(\alpha_{n+1})x_{n+1} = 0$$
$$\vdots$$
$$\sigma_n(\alpha_1)x_1 + \cdots + \sigma_n(\alpha_{n+1})x_{n+1} = 0$$

Once again, has a solution $x_i = \beta_i \in K$

with: not all $\beta_i = 0$

not all $\beta_i \in F$: one of the automorphisms, say σ_1, is the identity

so first equation would contradict linear independence.

Choose a solution $(\beta_1, \ldots, \beta_{n+1})$ with the number r of nonzero β_i minimized. Reorder s.t. $\beta_1 \cdots \beta_r$ all nonzero. Can also assume WLOG that $\begin{cases} \beta_r = 1 & \text{(divide all } \beta_i \text{ by } \beta_r). \\ \beta_1 \notin F & \text{(some } \beta_i \notin F). \end{cases}$

So our system is

$$\sigma_i(\alpha_1)\beta_1 + \cdots + \sigma_i(\alpha_{r-1})\beta_{r-1} + \sigma_i(\alpha_r) = 0$$
$$(i = 1, 2, \ldots, n).$$

Choose an automorphism σ_{k_0} not fixing β_1.
Apply to previous eqns.

$$\sigma_{k_0}\sigma_j(\alpha_1)\sigma_{k_0}(\beta_1) + \cdots + \sigma_{k_0}\sigma_j(\alpha_{r-1})\sigma_{k_0}(\beta_{r-1})$$
$$(j = 1, \ldots, n) \qquad + \sigma_{k_0}\sigma_j(\alpha_r) = 0.$$

61.3 .

The kicker. The σ_i and the $\sigma_{k_0}\sigma_j$ $(i,j=1,\dots,n)$ are the same set of automorphisms, in a different order.

This is because $\begin{array}{l} G \longrightarrow G \\ g \longrightarrow g_0 g \end{array}$ is a bijection for any $g_0 \in G$.

Have the same system applied to the β_k and the $\sigma_{k_0}(\beta_k)$.

Subtract:

$$\sigma_i(\alpha_1)(\beta_1 - \sigma_{k_0}(\beta_1)) + \cdots + \sigma_i(\alpha_{r-1})(\beta_{r-1} - \sigma_{k_0}(\beta_{r-1}))$$

$$+ \sigma_i(\alpha_r)\underbrace{(1-1)}_{\text{Oops!}} = 0. \quad (i=1,\dots,n)$$

By hypothesis $\beta_1 - \sigma_{k_0}(\beta_1) \neq 0$ and this is a shorter nontrivial dependence relation — contrary to hypothesis!

Now we run with it.

Cor. For any finite extension K/F,

$$|\mathrm{Aut}(K/F)| \leq [K:F].$$

Proof. Let $F_1 = \mathrm{Fix}(\mathrm{Aut}(K/F))$ with $F \subseteq F_1$.

Then $\mathrm{Aut}(K/F) = \mathrm{Aut}(K/F_1)$,

$$|\mathrm{Aut}(K/F)| = [K:F_1] \leq [K:F].$$

(Indeed, $|\mathrm{Aut}(K/F)|$ divides $[K:F]$ by "degrees ...(think").)

Cor. Let G be any subgroup of $\mathrm{Aut}(K)$ with $F = \mathrm{Fix}(G)$. Then any automorphism of K fixing F is in G. (i.e. $\mathrm{Aut}(K/F) = G$.)

Proof. We have $|G| \leq |\mathrm{Aut}(K/F)|$ trivially

$|G| = [K:F]$ by previous theorem

$|\mathrm{Aut}(K/F)| \leq [K:F]$ by previous cor.

So equalities all around.

Cor. If $G_1 \neq G_2$ are finite subgroups of a field K, their fixed fields are distinct.

Proof. If they have the same fixed field then $G_1 \leq G_2$ and $G_2 \leq G_1$ by previous.

Theorem (1) An extension K/F is Galois if and only if K is the splitting field of some separable polynomial$/F$.

(2) If this is the case, then every irred $f \in F[x]$ which has a root in F is separable and has all its roots in K.

Proof. Splitting fields of sep polys are Galois.

So suppose K/F is Galois.

61.5 .

Claim. Every irred $p(x) \in F[x]$ with a root in K splits completely in K.

Proof of claim: Set $G = \mathrm{Gal}(K/F)$, α = root of p.

If $G = \{1, \sigma_2, \dots, \sigma_n\}$ write $\alpha = \alpha_1, \alpha_2, \dots, \alpha_r$ for the Galois conjugates of α, i.e. the distinct elements $\sigma_i(\alpha)$ as σ_i ranges over G.

Then any $\tau \in G$ permutes the α_i, so the poly

$$f(x) = (x-\alpha)(x-\alpha_2)\cdots(x-\alpha_n)$$

is fixed by all of G, hence is in $\mathrm{Fix}(G)[x]$
$= F[x]$.

Since p is the minimal poly of α/F, must have
$p(x) \mid f(x)$.

But we proved earlier that if $\sigma \in \mathrm{Gal}(K/F)$, $\sigma\alpha$ is a root of $\min_{\alpha, F}(x)$.

So p has all the α_i as roots so $p = f$.

So p is separable and has all roots in K, proving (2).

For (1), choose a basis $w_1, \dots, w_n$ for K/F
The min polys $p_i(x)$ are separable and split over K.

Let $g(x)$ = squarefree part of $\prod p_i(x)$
(remove any duplicate factors)

Then K is the splitting field for g.

What we've seen so far:

TFAE (a finite field ext K/F is Galois):

1. $[K:F] = |\mathrm{Aut}(K/F)|$
2. K is the splitting field of a separable polynomial$/F$
3. $\mathrm{Fix}(\mathrm{Aut}(K/F)) = F$
4. K is the splitting field of a collection of separable polynomials $/F$ (and is finite). "is normal".

Fundamental Theorem of Galois theory.

Let K/F be Galois w/ $G = \mathrm{Gal}(K/F)$. Then there is a bijection

$$\left\{ \begin{array}{c} \text{intermediate} \\ \text{fields} \\ K/E/F \end{array} \quad \begin{array}{c} K \\ | \\ E \\ | \\ F \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{subgroups} \\ \text{of } G \end{array} \quad \begin{array}{c} 1 \\ | \\ H \\ | \\ G \end{array} \right\}$$

$$E \longrightarrow \mathrm{Aut}(K/E)$$

$$\mathrm{Fix}(H) \longleftarrow H$$

satisfying:

(1) Inclusion reversing: If $\begin{array}{l} E_1 \longleftrightarrow H_1 \\ E_2 \longleftrightarrow H_2 \end{array}$

then $E_1 \subseteq E_2 \Longleftrightarrow H_2 \leq H_1$.

(2) Order preserving: $[K:E] = |H|$, $[E:F] = |G:H|$.

(3) K/E is always Galois, with $\mathrm{Gal}(K/E) = H$.

(4) E/F is Galois iff $H \trianglelefteq G$, and then $\mathrm{Gal}(E/F) \cong G/H$.

(5) Bijection of lattices: If $\begin{array}{l} E_1 \longleftrightarrow H_1 \\ E_2 \longleftrightarrow H_2 \end{array}$

then $E_1 \cap E_2 \longleftrightarrow \langle H_1, H_2 \rangle$, $E_1 E_2 \longleftrightarrow H_1 \cap H_2$.

Proof. Have done lots of this already.

* Fixed fields are unique.
  So the corr is injective $R \to L$.

* (3) is true, since K/E is ~~generated~~ the splitting field of the same poly.

* Saw inclusion reversing, and $F = \mathrm{Fix}(\mathrm{Gal}(K/F))$ for F Galois already.
  So map is surjective $R \to L$, hence get the bij.

* Get $|H| = [K:E]$ by original char. of Galois extensions.
  $[E:F] = |G:H|$ by taking quotients.

* Claim that every embedding $E \hookrightarrow \overline{F}$ is $\sigma|_E$ for $\sigma \in G$, and hence has image in K.
  If $\alpha \in E$ has min poly $m_\alpha(x)$ over F, all roots are in K.

  So use our "extend isomorphisms theorem"

$$\begin{tikzcd} K \arrow[r, "\sigma"] \arrow[d, dash] & K \arrow[d, dash] \\ E \arrow[r, "\tau"] & \tau(E) \end{tikzcd}$$

  Pick some σ extending τ, then $\tau = \sigma|_E$.

* The embeddings $E \hookrightarrow K$ are in bijection with the cosets σH of $H \leq G$:

  $\sigma|_E = \sigma'|_E$ if $\sigma(\sigma')^{-1}$ fixes E
  hence $\sigma(\sigma')^{-1} \in H$.

  So # of such embeddings is $[G:H] = [E:F]$.

The punchline:

E/F is Galois $\longleftrightarrow$ $|\mathrm{Aut}(E/F)| = [E:F]$, which is true if each embedding $E \hookrightarrow K$ is in fact an automorphism

Now, for $\sigma \in G$,

$$\mathrm{Gal}(K/\sigma(E)) = \sigma H \sigma^{-1} \quad \text{by definition}$$

and hence $\sigma(E) = \mathrm{Fix}(\sigma H \sigma^{-1})$.

This equals E for all σ iff $\sigma H \sigma^{-1} = H$ for all H.

* To prove (5),

if $H_1 = \mathrm{Gal}(K/E_1)$, $H_2 = \mathrm{Gal}(K/E_2)$

then certainly $H_1 \cap H_2 \subseteq \mathrm{Gal}(K/E_1 E_2)$.

(Any elt. of $E_1 E_2$ is an alg. combination of elts of E_1, E_2)

Conversely, $\mathrm{Gal}(K/E_1 E_2) \subseteq \begin{matrix} H_1 \\ H_2 \end{matrix}$ because $E_1 E_2 \supseteq \begin{matrix} H_1 \\ E_2 \end{matrix}$.

Claim about $E_1 \cap E_2$ is similar. QED!

See DF for lots of examples.

e.g. Compute a polynomial generating $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Look at $\sqrt{2} + \sqrt{3}$.

Has four Galois conjugates $\pm\sqrt{2} \pm \sqrt{3}$ in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Since $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$, can take

$$(x - (\sqrt{2} + \sqrt{3}))(x - (\sqrt{2} - \sqrt{3}))(x - (-\sqrt{2} + \sqrt{3}))(x - (-\sqrt{2} - \sqrt{3}))$$
$$= x^4 - 10x + 1.$$

Finite fields.

Saw before, for each prime power p^n, there is a unique field $\mathbb{F}_{p^n}$ of that order, with

$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$$

generated by the Frobenius automorphism $a \to a^p$.

For each $d \mid n$ there is a subfield of degree d, so

$$\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n} \iff d \mid n.$$

Moreover, if $\sigma = \mathrm{Frob}_p$, have a restriction map

$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \longrightarrow \mathrm{Gal}(\mathbb{F}_{p^d}/\mathbb{F}_p) \cong \frac{\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)}{\mathrm{Gal}(\mathbb{F}_{p^d}/\mathbb{F}_p)}$$

$$\sigma \longrightarrow \sigma|_{\mathbb{F}_{p^d}}.$$

Cool fact. x^4+1 is reducible (mod p) for every prime p, despite being irreducible $/\mathbb{Z}$.

Proof. $p=2$: $x^4+1=(x+1)^4$

$p = \text{odd} \Rightarrow p^2 \equiv 1 \pmod 8$.

So $x^8-1 \mid x^{p^2-1}-1$

and so $x^4+1 \mid x^{p^2-1}-1 \mid x^{p^2}-x$.

So, all roots of $x^4+1/\mathbb{F}_p$ live in $\mathbb{F}_{p^2}$, hence generate (at most) quadratic extensions!

So can't be irreducible. (That generates an integral basis...