Principal ideal domain, every ideal looks like $(h(x))$

Suppose $\mathbb{F}$ is a field & $f: \mathbb{C}[x] \to \mathbb{F}$ is a ring homomorphism. Then either

→ ① f is injective $(\ker(f) = (0))$

→ ② $\ker(f) = (x-\alpha)$, $\alpha \in \mathbb{C}$ (namely $\ker(f)$ is maximal).

Pf: In $\mathbb{C}[x]$, we've shown in class maximal ideals are the same as $(x-\alpha)$, $\alpha \in \mathbb{C}$. So if $\ker(f) = (x-\alpha)$, then we're done. Assume $\ker(f) \neq (0)$ & since its not maximal, we have $\ker(f) = (h(x)g(x))$ w/ h, g irreducible & $\deg(h), \deg(g) \geq 1$.

$\ker(f) = (h(x)g(x))$ & $\underbrace{h(x), g(x)}_{\deg h < \deg h + \deg g} \notin \underbrace{(h(x)g(x))}_{\text{has degree } (\deg h + \deg g)} = \ker(f)$.

$(h(x))$ has elements whose degree is ($\geq$) larger than $\deg h$, $\deg g$

Lets apply f to $h(x)g(x)$:

$$0 = f(h(x)g(x)) = \underbrace{f(h(x))}_{=0} \cdot \underbrace{f(g(x))}_{=0} \in \mathbb{F}$$

or since $\mathbb{F}$ has no zero divisors.

Since $\mathbb{F}$ is a field

$\Rightarrow h(x)$ or $g(x) \in \ker(f) = (h(x)g(x))$ ↯.

$\Rightarrow \ker(f) = 0$. (Works for $\mathbb{F}$ an integral domain)

Abstract symbols

$$ev: \mathbb{F}_q[X] \longrightarrow \mathrm{Fun}(\mathbb{F}_q, \mathbb{F}_q)$$

$$f(x) \longmapsto \phi \in \mathrm{Fun}(\mathbb{F}_q, \mathbb{F}_q)$$

b

s.t. $\phi(a) = f(a) \quad \forall a \in \mathbb{F}_q$

$q=7$: $x^6 + 5x + 1 \in \mathbb{F}_7[x]$

$$(\underset{0}{1}, \underset{1}{5}, \underset{2}{0}, \underset{3}{0}, \underset{4}{0}, \underset{5}{0}, \underset{6}{1})$$

ϕ:

0	1	2	3
$ev_0(f)$	$ev_1(f)$	$ev_2(f)$	$ev_3(f)$

$$\chi_a(x) = \begin{cases} 1 & x = a \\ 0 & x \neq a \end{cases}$$

$g(a) \neq 0.$

$\downarrow$

$f(x) = g(x)\, g(a)^{-1}$

$f(b) = 0$ iff $x - b \mid f(x)$

$f(b) = 0 \ \forall b \neq a$ iff $\prod_{b \neq a} (x - b) \mid f(x)$

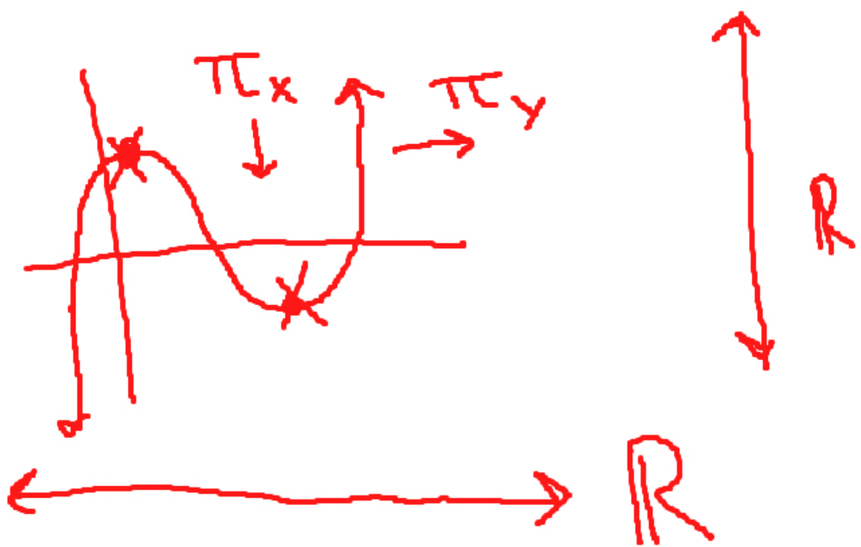
$\mathbb{F}_q$

$$g(x) = \prod_{b \neq a} (x - b), \quad g(a) = \prod_{b \neq a} (a - b) \neq 0$$

$\uparrow$ $\uparrow$ $\cap$ $\mathbb{F}$.

Q: → Special case of Bezout's Thm

→ Ramification points of Riemann surfaces



Ex: Let $L = V(ax+by+c) = \{(x,y) : \underbrace{ax+by+c=0}\} \subseteq \mathbb{C}^2$,

& let $f \in \mathbb{C}[x,y]$ be a degree d irreducible poly.

Show that $V(f) \cap L$ has at most d points, unless $V(f) \supseteq L$. $(\Leftrightarrow (f) \subseteq (ax+by+c) \Leftrightarrow ax+by+c \mid f)$

Sol: So I want to do an even more specialized version which will illuminate the approach.

Take $a=c=0$, $b=1$ $\Rightarrow$ $L = V(y) = \{(x,0)\}$

Let $f(x,y) = \sum_{j=0}^{d} f_j(y) x^j$ where $f_j(y)$ is a polynomial in y of degree $\leq d-j$.

What is $V(y)$? $V(y) = \{(x,0)\}$
$= \{(x,y) : y=0\}$

$V(f) \cap L = V(f) \cap V(y) \iff$ Solutions to

$$\underbrace{\sum_{j=0}^{d} f_j(0) x^j = 0}_{\text{has } \leq d \text{ roots}}$$

$V(f) = \{(x,0) : \sum_{j=1}^{d} f_j(0) x^j = 0\}$

In particular, $f_j(0) \in \mathbb{C}$.

$$0 = \sum_{j=0}^{d} f_j(0)\, \overset{f(x)}{\overset{\shortparallel}{x^j}} \in \mathbb{C}[x]$$ of $\deg \leq d$ (i.e. if $f_j(0) \neq 0$, is of degree d, $\deg(f) = \max_{f_j(0) \neq 0} j$).

We know every polynomial over $\mathbb{C}$ with degree $e \leq d$ has e roots, hence

$$|V(f) \cap L| = e = \deg(f) \leq d.$$

$\square$

For general case, use a similar argument

but w/ $y = -\frac{a}{b}x - \frac{c}{b}$ instead of 0.

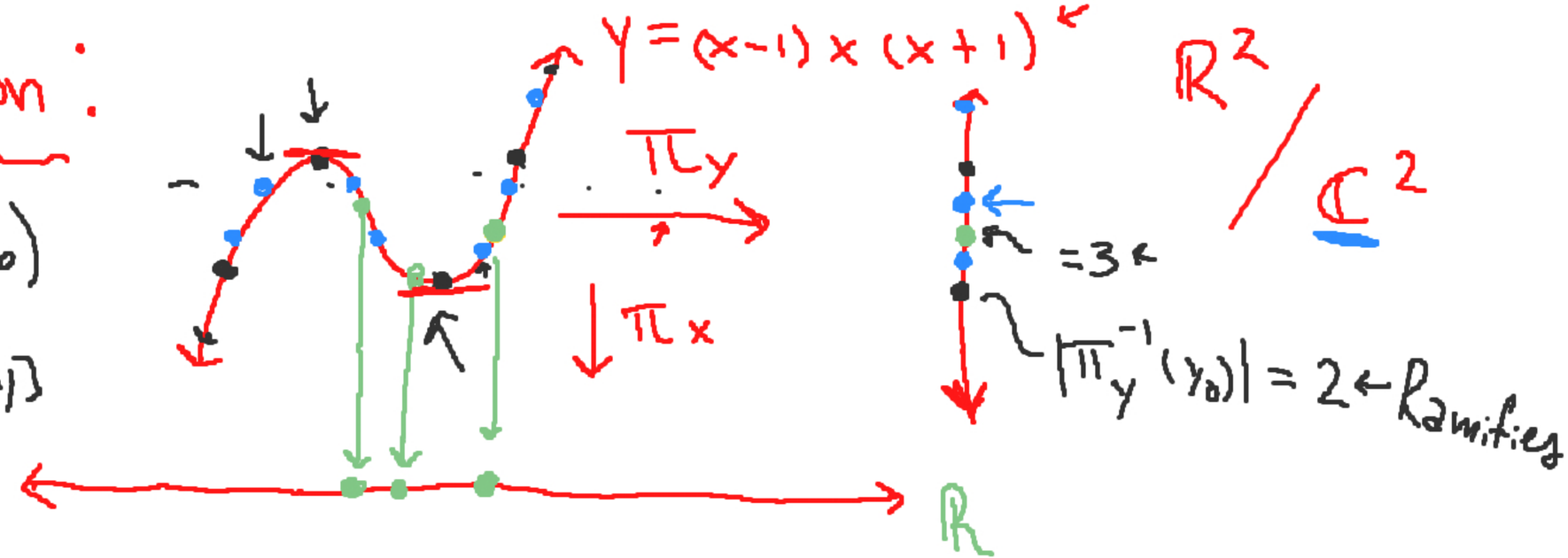
Ramification:

(Thm 11.9.16)

$f(x,y) \in \mathbb{C}[x,y]$

$\shortparallel$

$O \xrightarrow{\pi} \mathbb{C}$



Ramification points are where the preimage of the projection is not "full"

Ex: Does the following Riemann surface have ramification points? If so, where?

(a) $f(x,y) = y^2 - x^3 + x^2 + x = 0$ ← The set of (x,y) making this true is called a <u>Riemann surface</u>

Sol: Need to check if f & $\frac{\partial f}{\partial y}$ share any roots.

$$\frac{\partial f}{\partial y}(x,y) = 2y = 0 \iff y = \underline{0} \quad \left(\text{only root of } \frac{\partial f}{\partial y}\right)$$

$y=0$ is only root of $\frac{\partial f}{\partial y}$, lets plug into $f(x,y)=0$.

$$f(x,0) = -x^3 + x^2 + x = 0 = -(x^3 - x^2 - x) = -x(x^2 - x - 1)$$

Quadratic formula $\Rightarrow$ $x = \frac{1 \pm \sqrt{5}}{2} = \varphi, \bar{\varphi}$ (Golden ratio) $= \frac{1+\sqrt{5}}{2}$

$$f(x,0) = -x(x-\varphi)(x-\bar{\varphi}) = 0$$

$\Rightarrow$ roots are $0, \varphi, \bar{\varphi}$. $\Rightarrow$ $\frac{\partial f}{\partial y}$ & f share the roots

$(0,0), (\varphi,0), (\bar{\varphi},0)$.

<u>Claim:</u> $0, \varphi, \bar{\varphi}$ are ramification points.

<u>Claim</u>: f ramifies @ $0, \varphi, \overline{\varphi}$.

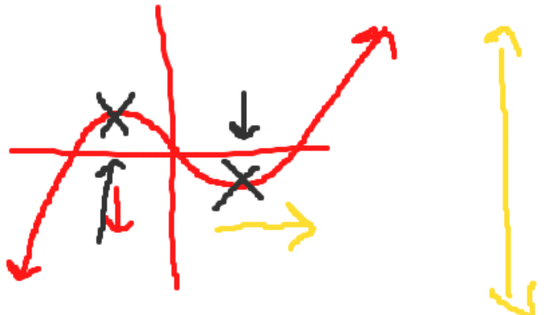
$$\pi^{-1}(0) = \{(0,y) : y^2 - 0\cancelto{0}{(0-\varphi)}(0-\overline{\varphi}) = 0\} = \{(0,y) : y^2 = 0\}$$
$$= \{(0,0)\}$$

$$\pi^{-1}(\varphi) = \{(\varphi,y) : y^2 - \varphi\cancelto{0}{(\varphi-\varphi)}(\varphi-\overline{\varphi}) = 0\} = \{(\varphi,0)\}$$

$$\pi^{-1}(\overline{\varphi}) = \{(\overline{\varphi},y) : y^2 - \overline{\varphi}\cancelto{0}{(\varphi-\overline{\varphi})}(\overline{\varphi}-\overline{\varphi}) = 0\} = \{(\overline{\varphi},0)\}$$

Since these are each of size 1 (<2), these are ramification points.

Ex: $f(x,y) = y - \overset{x^3-x}{x(x-1)(x+1)} = 0$



does not ramify as a projection to complex x-plane since

$$\frac{\partial f}{\partial y} = 1 \neq 0 \implies f \;\&\; \frac{\partial f}{\partial y} \text{ can never}$$

share a root, so no ramification. $\left(x = \pm\frac{\sqrt{3}}{3}\right)$ take $\frac{\partial f}{\partial x} = 0$

Sidebar: As a projection to complex y-plane, it does ramify

Q:

- Irreducible polys in $\mathbb{F}_p[x]$ using "Sieve of Eratosthenes"

- Example of poly $f(x)$ which is irreducible over $\mathbb{Q}$ (in $\mathbb{Q}[x]$) but reducible mod every prime

Sieve of Eratosthenes: An algorithm to find all prime numbers up to a given limit, $L \in \mathbb{Z}_{>0}$.

(Around 2000 or more years old)

How: Write all numbers up to L & starting at 2 (first prime), cross out all multiples of 2 up to L. Then cross out all multiples of 3, then all multiples of 5 & so on. List remaining at the end will be all primes less than L.

$\underline{L=30}$: $1\ 2\ 3\ \cancel{4}\ 5\ \cancel{6}\ 7\ \cancel{8}\ \cancel{9}\ \cancel{10}\ 11\ \cancel{12}\ 13\ \cancel{14}\ \cancel{15}$

$\cancel{16}\ 17\ \cancel{18}\ 19\ \cancel{20}\ \cancel{21}\ \cancel{22}\ 23\ \cancel{24}\ \cancel{25}\ \cancel{26}\ \cancel{27}\ \cancel{28}\ 29\ \cancel{30}$

$\Rightarrow$ The set of primes ≤ 30 is

$$\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29\}$$

* If $\mathbb{F}$ is a field, $\mathbb{F}[x]$ is a PID *

Lets try to find all irreducible (= prime) polys in $\mathbb{F}_2[x]$ of degree ≤ 4. $\mathbb{F}_2 = \{0,1\}$

$$\overbrace{1}^{1},\ \overbrace{x,\ x+1}^{2},\ \overbrace{\cancel{x^2},\ x^2\cancel{+1},\ x^2\cancel{+x},\ x^2+x+1}^{4=2^2},\ \cancel{x^3},\ \overset{(x+1)^3}{\overset{\shortparallel}{\cancel{x^3+1}}},\ \cancel{x^3+x},$$

$$x^3+x+1,\ \cancel{x^3+x^2},\ x^3+x^2+1,\ \cancel{x^3+x^2+x},\ \cancel{x^3+x^2+x+1},\ \cancel{x^4},\ \cancel{x^4+1},\ \cancel{x^4+x},$$

$$x^4+x+1,\ \cancel{x^4+x^2},\ x^4+x^2+1,\ \cancel{x^4+x^2+x},\ \cancel{x^4+x^2+x+1},\ \cancel{x^4+x^3},$$

$$x^4+x^3+1,\ \cancel{x^4+x^3+x},\ \cancel{x^4+x^3+x+1},\ \cancel{x^4+x^3+x^2},\ \cancel{x^4+x^3+x^2+1},$$

$$\cancel{x^4+x^3+x^2+x},\ x^4+x^3+x^2+x+1$$

$$(x^2+x+1)^2 = (x^2+x+1)(x^2+x+1) = x^4 + \cancel{x^3} + \cancel{x^2} + \cancel{x^3} + \cancel{x^2} + \cancel{x} + x^2 + \cancel{x} + 1$$

$$= x^4 + x^2 + 1 \longleftarrow \text{Reducible !!!}$$

$\Rightarrow$ All primes = irreducibles in $\mathbb{F}_2[x]$ of degree at most 4 are

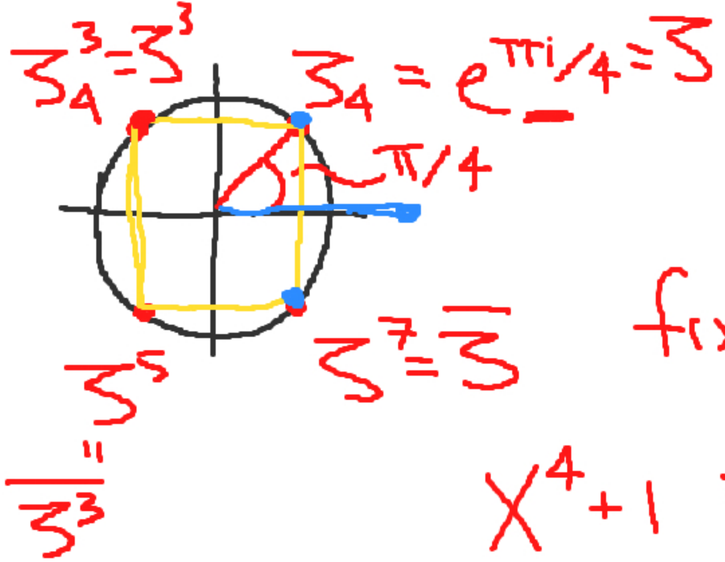
$$\{\overbrace{1}^{1}, \overbrace{x, x+1}^{2}, \overbrace{x^2+x+1}^{1}, \overbrace{x^3+x^2+1, x^3+x+1}^{2}, \overbrace{x^4+x+1,}^{3}$$
$$x^4+x^3+x^2+x+1, \ x^4+x^3+1\}$$

Example of poly $f(x)$ which is irreducible over $\mathbb{Q}[x]$ but reducible in $\mathbb{F}_p[x]$ for every prime.

Consider $f(x) = x^4 + 1 \in \mathbb{Z}[x]$.

<u>Claim 1</u>: x^4+1 is irreducible over $\mathbb{Q}$.

<u>pf</u>: <u>First approach</u>: "complex analytic". Since $\mathbb{Q} \subseteq \mathbb{C}$, $\mathbb{Q}[x] \subseteq \mathbb{C}[x]$ so if f reduces in $\mathbb{Q}$, it better match up with the reduction over $\mathbb{C}$.



$X^4+1=0 \iff X^4=-1 \quad (\zeta_4^4 = e^{\pi i} = -1 \checkmark)$

$f(x)=x^4+1$ has 4 roots $\zeta, \zeta^3, \zeta^5, \zeta^7$.

$$
\begin{aligned}
X^4+1 &= (X-\zeta)(X-\zeta^3)(X-\zeta^5)(X-\zeta^7) \\
&= (X-\zeta)(X-\zeta^3)(X-\overline{\zeta^3})(X-\overline{\zeta}) \\
&= (X-\zeta)(X-\overline{\zeta})(X-\zeta^3)(X-\overline{\zeta^3}) \\
&= (X^2-(\zeta+\overline{\zeta})X+\zeta\overline{\zeta})(X^2-(\zeta^3+\overline{\zeta^3})+\zeta^3\overline{\zeta^3}) \\
&= (X^2-2\mathrm{Re}(\zeta)+1)(X^2-2\mathrm{Re}(\zeta^3)+1) \\
&= (X^2-\sqrt{2}+1)(X^2+\sqrt{2}+1) \notin \mathbb{Q}[X]
\end{aligned}
$$

f is irreducible over $\mathbb{Q}$.

$\Uparrow$

$\mathbb{Q}[X] \not\ni$

Second approach: Eisenstein criteria.

(*) If $f(x)$ has rational root, then so does $f(x+1)$ (same holds for irreducibility over $\mathbb{Q}$). So let's look @

$$f(x+1) = (x+1)^4+1 = (x^4+4x^3+6x^2+4x+1)+1$$
$$= x^4+4x^3+6x^2+4x+\underline{2}.$$

Take $p=2$ in Eisenstein: ① $p=2 \mid a_0, a_1, a_2, a_3 = 2,4,6,4$ ✓

② $p=2 \nmid a_n = a_4 = 1$ ✓ $\Rightarrow$ By Eisenstein, x^4+1 is irreducible $\square$

③ $p^2=4 \nmid a_0 = 2$ ✓

4/23 Discussion 4

<u>Q:</u> → Finish showing x^4+1 is reducible mod every prime (but irreducible over $\mathbb{Q}$ [by Eisenstein])

→ Group actions & Cauchy's Thm (for $p \mid |G|$, $\exists g \in G$ s.t. $\mathrm{ord}(g) = p$)

<u>Claim</u>: X^4+1 is reducible mod every prime.

<u>sol</u>: We do this by investigating certain elements in $\mathbb{F}_p$ & checking whether they are squares.

<u>Case 1</u>: If -1 is a square (mod p). (works for $p=2$)

$\Rightarrow \exists r \in \mathbb{F}_p$ s.t. $r^2 \equiv -1 \pmod{p}$. Then

$$X^4+1 = X^4-(-1) \equiv X^4 - r^2 \equiv \underbrace{(X^2-r)}\,\underbrace{(X^2+r)} \pmod{p}$$

$\Rightarrow$ reducible.

Case 2: If 2 is a square mod p

$\Rightarrow \exists\, s \in \mathbb{F}_p$ s.t. $s^2 \equiv 2 \pmod p$. Then

add 0

$$x^4+1 = x^4+2x^2+1-2x^2 = (x^2+1)^2 - \underbrace{2x^2}_{s^2x^2 \equiv (sx)^2}$$

$$\equiv (x^2+1)^2 - (sx)^2 \equiv ((x^2+1)-sx)((x^2+1)+sx) \pmod p$$

$\Rightarrow$ reducible.

Case 3: If neither -1 or 2 is a square mod p

$\Rightarrow -2$ is a square so $\exists\, t \in \mathbb{F}_p$ s.t. $t^2 \equiv -2 \pmod p$.

non-zero elements of $\mathbb{F}_p$

We have that $\mathbb{F}_p^*$ is a cyclic group. Fact we'll use.

So $\exists a \in \mathbb{F}_p$ s.t. $\langle a \rangle = \mathbb{F}_p^*$, i.e. every non-zero element is a power of a.

Since -1 & 2 were not squares, $\exists n, m \in \mathbb{Z}_{\geq 0}$ s.t.

$-1 \equiv a^{2n+1} \pmod p$ & $2 \equiv a^{2m+1} \pmod p$. Well,

$$-2 \equiv (-1)(2) \equiv a^{2n+1} a^{2m+1} \equiv a^{2(n+m+1)} \pmod p$$

& -2 is a square (of a^{n+m+1}) mod p.

So $\exists\, t \in \mathbb{F}_p$ s.t. $t^2 \equiv -2 \pmod{p}$. Then

$$x^4+1 = x^4 - 2x^2 + 1 + 2x^2 = (x^2-1)^2 + \overset{-(-2x^2) = -(tx)^2}{2x^2}$$

$$\equiv (x^2-1)^2 - (tx)^2 \equiv ((x^2-1) - tx)((x^2-1) + tx) \pmod{p}.$$

$\Rightarrow$ <u>reducible</u>.

This covers all primes, we have x^4+1 is reducible mod every prime, but irreducible over $\mathbb{Q}$. $\square$

<u>Note</u>: X^2+1 is reducible mod every prime p

s.t. $p \equiv 1 \pmod 4$ (Quadratic reciprocity = squares mod p)

In this case,

-1 is a square mod p.

Group Actions $G \circlearrowright X$

"G acting on X"

Let G be a group, X be a set. A group action of G on X is a map $\bullet : G \times X \to X$ s.t.

$\to$ $1_G \cdot x = x \quad \forall x \in X$

$\to$ $g \cdot (h \cdot x) = (gh) \cdot x \quad \forall g, h \in G, \ \forall x \in X$

Ex: Any groups acts on itself by left-multiplication: $g \cdot h := gh$

$X = G$ $\qquad$ $G \ni$

Given $x \in X$, define the <u>orbit of x</u>, $\mathrm{orb}(x)$ or $\mathcal{O}_x$, is

$$X \supseteq \mathcal{O}_x = \{g \cdot x : g \in G\} = \{y \in X : \exists g \in G \text{ s.t. } y = g \cdot x\}$$

the <u>stabilizer of x</u> is $\mathrm{Stab}(x) := \{g \in G : g \cdot x = x\} \leq G$

* In general, $\mathrm{Stab}(x)$ is not normal

<u>Thm</u>: (Orbit-Stabilizer) For a group G s.t. $|G| < \infty$, $\forall x \in X$

$$|G| = |\mathcal{O}_x| \cdot |\mathrm{Stab}(x)|. \qquad G/\mathrm{Stab}(x) \cong \mathcal{O}_x$$

as sets, not groups

Thm: (Cauchy) Let $|G| = p^n m < \infty$, w/ $(p,m)=1$, p prime.

Then $\exists\, g \in G$ s.t. $\mathrm{ord}(g) = p$. ($\Updownarrow$ $p \mid |G|$)

Pf: Let $X = \{(g_1, \dots, g_p) \in G^p : g_1 \cdot g_2 \cdots g_p = 1\}$

① $|X| = |G|^{p-1}$.

why? Once $g_1, \dots, g_{p-1}$ are chosen, this uniquely defines g_p, i.e. $g_p = (g_1 \cdots g_{p-1})^{-1} \in G$. Since there are $|G|^{p-1}$ choices for $g_1, \dots, g_{p-1}$ it follows that $|X| = |G|^{p-1}$.

② $\mathbb{Z}/p\mathbb{Z}$ acts on X by cyclically permuting entries.

Since $p \mid |G|$ & $|X| = |G|^{p-1}$, we have $p \mid |X|$. Hence, we get an action of $\mathbb{Z}/p\mathbb{Z}$ on X by cyclic permutation, i.e.

$k \in \mathbb{Z}/p\mathbb{Z}$ acts on X by

$$k \cdot (g_1, \dots, g_p) := (g_{p-k+1}, \dots, g_p, \overset{k^{th}\text{ spot}}{\overset{\downarrow}{g_1}}, \dots, g_{p-k})$$

Shift every thing right k places.

$$\left(\begin{array}{l} 0 \cdot (g_1, \dots, g_p) = (g_1, \dots, g_p) \\ k \cdot l(\dots) = (k+l) \cdot (\dots) \end{array} \right) \Rightarrow \text{Group action!}$$

③ Use Orbit-Stabilizer & fact that orbits partition X.

$\exists\, \mathcal{O}_1, \dots, \mathcal{O}_r$ s.t. $\mathcal{O}_i \overset{\perp}{=} \mathcal{O}_{x_i}$ for some $x_i \in X$, $\mathcal{O}_i \cap \mathcal{O}_j = \emptyset$ for $i \neq j$, & $\bigcup_{i=1}^{r} \mathcal{O}_i = X$. Take cardinalities, we get $|X| = \sum_{i=1}^{r} |\mathcal{O}_i|$. By orbit-stabilizer, since $\mathbb{Z}/p\mathbb{Z}$ acts on X, $p = |\mathbb{Z}/p\mathbb{Z}| = |\mathcal{O}_{x_i}||\mathrm{Stab}(x_i)| \Rightarrow |\mathcal{O}_i| = 1, p$. So suppose $\mathcal{O}_1, \dots, \mathcal{O}_n$ are of size p & $\underbrace{\mathcal{O}_{n+1}, \dots, \mathcal{O}_r}$ are of size 1.

$$\Rightarrow \underset{\substack{\uparrow \\ \text{divisible by } p}}{|X|} = \sum_{i=1}^{r} |\mathcal{O}_i| = \sum_{i=1}^{n} \overset{p}{|\mathcal{O}_i|} + \sum_{i=n+1}^{r} |\mathcal{O}_i|$$

$$= \sum_{i=1}^{n} p + \sum_{i=n+1}^{r} |\mathcal{O}_i|$$

there must be at least one orbit of size 1, i.e. $\mathcal{O}_{(1,\dots,1)}$

$$\Downarrow$$

$$0 \equiv \sum_{i=1}^{n} 0 + \underbrace{\sum_{i=n+1}^{r} |\mathcal{O}_i|}_{\neq 0} \pmod{p}$$

$\Rightarrow \exists$ another orbit $\mathcal{O}_x$ of size 1.

$\Rightarrow x = (g, \dots, g)$ for some $g \in G$ but $x \in X$ so $g^p = 1$, i.e. g has order p. $\square$

Discussion 5 4/30

Q: → If $K \subseteq I \subseteq R$, then

additive subgp ideal

$$R/K \twoheadrightarrow R/I \quad (\twoheadrightarrow = \text{surjection})$$

→ Examples of $|\mathcal{O}_{\sqrt{-d}}/I|$

algebraic number theory

① Suppose R is a (comm) ring, $I \subseteq R$ is an ideal, & $K \subseteq I$ is an additive subgroup. Prove that R/K surjects onto R/I.

(In particular, this shows that to show $\mathcal{O}_{\sqrt{d}}/I$ is finite for non-zero ideal I, it suffices to find K (additive subgroup of I) & show that $\mathcal{O}_{\sqrt{d}}/K$ is finite. Here, we take $K = I\bar{I}$)

pf: We check 2 things: ① $\exists$ map $R/K \to R/I$ (well-defined)
② the map is surjective

To show the 1st thing, we'll show something more general: Let $\varphi: R \to S$ (R, S - rings) be a homomorphism of rings & suppose $K \subseteq \ker(\varphi)$ is an additive subgroup. Then $\exists\, \tilde{\varphi}: R/K \to S$.

<u>Claim</u>: $\exists\, \tilde{\varphi}: R/K \to S$.

<u>Pf of claim</u>: For $r+K \in R/K$, define $\tilde{\varphi}: R/K \to S$ by $\tilde{\varphi}(r+K) := \varphi(r)$.

We have to show its well-defined: i.e. if $r_1 + K = r_2 + K$

1

Need to show $\tilde{\varphi}$ is <u>well-defined</u>: if $r_1 + K = r_2 + K$, then $\tilde{\varphi}(r_1 + K) = \tilde{\varphi}(r_2 + K)$.

So $r_1 + K = r_2 + K \Rightarrow \exists k_2 \in K$ s.t.

$r_1 = r_2 + k_2$ as elements of R.

$$\Rightarrow \tilde{\varphi}(r_1 + K) = \tilde{\varphi}((r_2 + k_2) + K) = \varphi(r_2 + k_2)$$

$$= \varphi(r_2) + \cancel{\varphi(k_2)}^{\,0} = \varphi(r_2) = \tilde{\varphi}(r_2 + K).$$

(since $k_2 \in K \subseteq \ker(\varphi)$)

Let $S = R/I$ & $\varphi = \pi : R \to R/I$ be the canonical projection. So $\ker(\pi) = I$ & $K \subseteq I \Rightarrow \exists\, \tilde{\pi} : R/K \to R/I$ ✓

② Showing $\tilde{\pi} : R/K \to R/I$ is surjective.

This is true because for $r + I \in R/I$, $\hookrightarrow r + i \in R$

Consider $r + K \in R/K$. Well

$$\tilde{\pi}(r+K) = \underset{\pi(r+i)}{\underset{\shortparallel}{\pi(r)}} = r + I \Rightarrow \tilde{\pi} \text{ is surjective.}$$

Ex: If R/I is finite, then the number of ideals in R containing I is finite.

Pf: This is a direct consequence of the correspondence theorem: $\exists$ bijection between

$$\left\{\begin{array}{l}\text{Ideals } J \subseteq R \text{ s.t.} \\ I \subseteq J \subseteq R\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{Ideals in} \\ R/I\end{array}\right\}$$

$$J \longmapsto \pi(J) = \{\pi(j) : j \in J\}$$
$$= \{r+I \in R/I : \exists j \in J \text{ w/ } r+I = \pi(J)\}$$

$$\pi^{-1}(L) = \{r \in R : \pi(r) \in L\} \longleftarrow\!\shortmid\; L \subseteq R/I$$

Since R/I is finite, it contains finitely many ideals, hence $\exists$ only finitely many ideals in R containing I.

This idea of using the correspondence theorem is instrumental in all parts of algebra. It holds for groups w.r.t. subgroups, rings w.r.t. ideals, & in general to modules w.r.t. submodules.

Example of computing $|\mathcal{O}_{\sqrt{-5}}/I|$

Consider $\mathcal{O}_{\sqrt{-5}}$ & $I = (2\sqrt{-5})$.

Since $-5 \equiv 3 \pmod 4$, we have

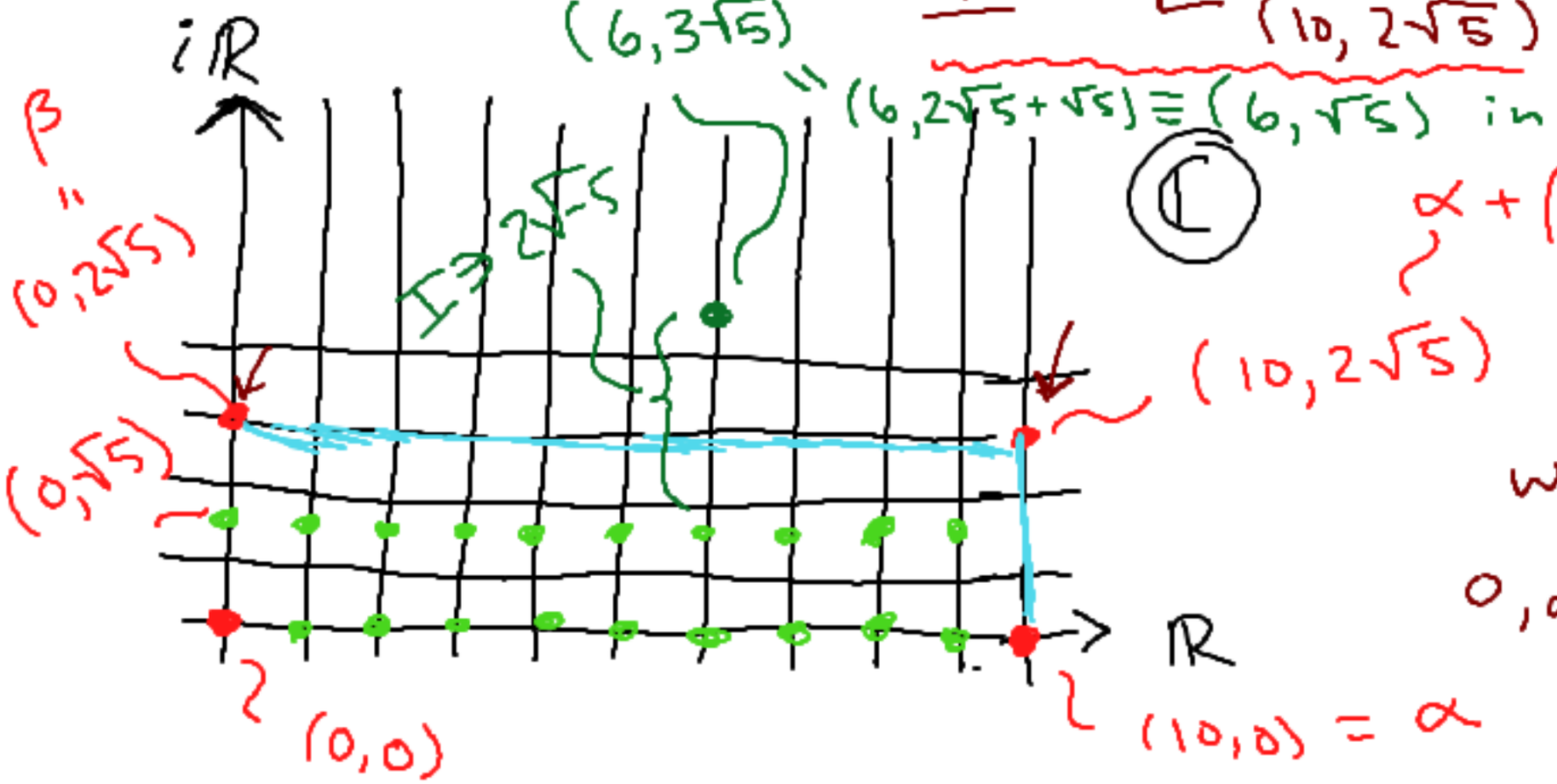
$$\mathcal{O}_{\sqrt{-5}} = L_{(1,\sqrt{5})} = \{a + b\sqrt{-5} : a,b \in \mathbb{Z}\}$$
$$= \{a + b\sqrt{5}\,i : a,b \in \mathbb{Z}\}$$

& $I = L_{(\alpha,\beta)}$ for some $\alpha,\beta \in \mathbb{R}$.

Well, $2\sqrt{-5} \in I \Rightarrow (2\sqrt{-5})(\sqrt{-5}) = -10 \in I$

$\Rightarrow 10 \in I$, & 10 is the smallest integer st. $10 \in I$. $\Rightarrow I = L_{(10,\, 2\sqrt{5})}$

$(6, 3\sqrt{5}) = (6, 2\sqrt{5} + \sqrt{5}) \equiv (6, \sqrt{5})$ in $\mathcal{O}_{\sqrt{-5}}/I$



Parallelogram w/ vertices $0, \alpha, \beta, \alpha + \beta$

What this shows is

$|\mathcal{O}_{\sqrt{-5}}/I| =$ # of lattice points in the parallelogram w/ vertices $0, \alpha, \beta, \alpha+\beta$ & not including the top & right edge.

$= \underline{20}$.

In class, it was shown $\mathcal{O}_{\sqrt{-5}}/I$ is finite by showing $\mathcal{O}_{\sqrt{-5}}/I\bar{I}$ is finite & this surjects onto $\mathcal{O}_{\sqrt{-5}}/I$. What is $|\mathcal{O}_{\sqrt{-5}}/I\bar{I}|$?

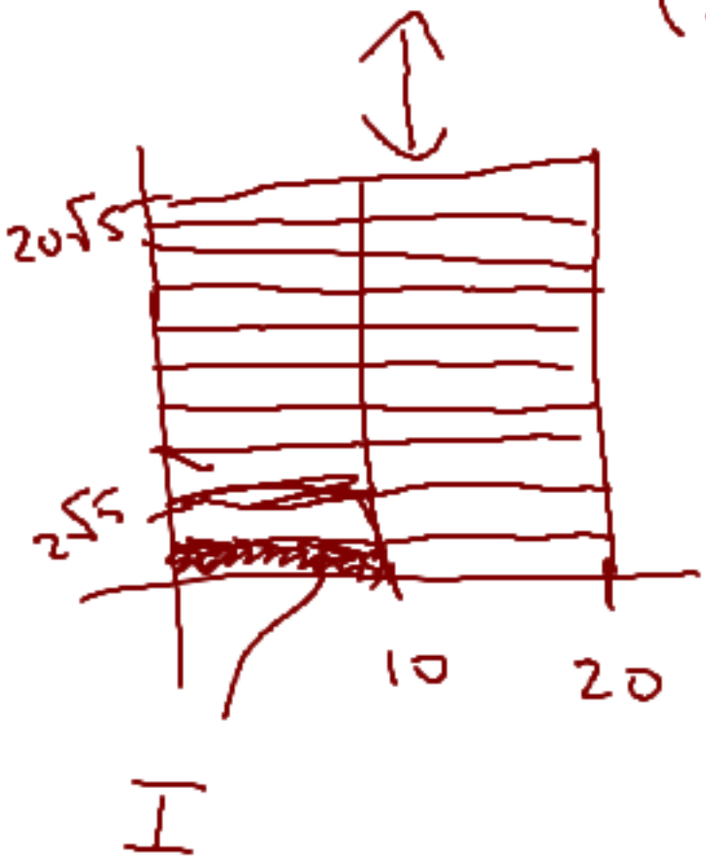
$$I = (\overset{\alpha}{\overset{\shortparallel}{10}}, \overset{\beta}{\overset{\shortparallel}{2\sqrt{-5}}}), \quad \bar{I} = (\overset{\bar{\alpha}}{\overset{\shortparallel}{10}}, \overset{\bar{\beta}}{\overset{\shortparallel}{-2\sqrt{-5}}})$$

$$\therefore I\bar{I} = (\underset{\alpha\bar{\alpha}}{100}, \underset{\bar{\alpha}\beta}{20\sqrt{-5}}, \underset{\alpha\bar{\beta}}{-20\sqrt{-5}}, \underset{\beta\bar{\beta}}{20}) = (n) = (20)$$

$$= (100, 20, 0) = 20$$

$$n = \gcd(\alpha\bar{\alpha}, \beta\bar{\beta}, \alpha\bar{\beta} + \bar{\alpha}\beta)$$

$$\Rightarrow \mathcal{O}_{\sqrt{-5}} / \underset{\substack{\shortparallel \\ (20)}}{II} = \{ a + b\sqrt{-5} : a, b \in \mathbb{Z}/20\mathbb{Z} \}$$



$$\Downarrow$$

$$|\mathcal{O}_{\sqrt{-5}}/II| = |\mathbb{Z}/20\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}|$$

$$= 20 \cdot 20 = 400.$$

$$|\mathcal{O}_{\sqrt{-5}}/I| = 20$$

Discussion 6 5/7

Q: → Examples of calculations for minimal polys

→ Field theory

In class yesterday, it was shown that if α & β are algebraic over $\mathbb{F}$, then

$$\alpha+\beta, \quad \alpha\cdot\beta, \quad \alpha/\beta \quad (\beta\neq 0)$$

are also algebraic over $\mathbb{F}$. In general, finding minimal poly of $\alpha+\beta, \alpha\beta, \alpha/\beta$ is quite difficult. (α algebraic iff $|\mathbb{F}(\alpha):\mathbb{F}|<\infty$)

Ex: Let $\alpha = \sqrt{2}$, $\beta = \sqrt{3}$. Then α & β are algebraic over $\mathbb{Q}$ ($P_{\sqrt{2}}(x) = x^2 - 2$, $P_{\sqrt{3}}(x) = x^2 - 3$)

What is ① $P_{\alpha+\beta}(x) = P_{\sqrt{2}+\sqrt{3}}(x)$ over $\mathbb{Q}$?

② $P_{\alpha\beta}(x) = P_{\sqrt{2}\sqrt{3}}(x) = P_{\sqrt{6}}(x)$ over $\mathbb{Q}$?

Sol: ② is easier, so lets look at it first.

We have $P_{\sqrt{6}}(x) = x^2 - 6 = (x - \sqrt{6})(x + \sqrt{6})$ is irreducible over $\mathbb{Q}$ (HW5: ax^2+bx+c irr $\Leftrightarrow b^2 < 4ac$)

Therefore, $P_{\sqrt{6}}(x) = x^2 - 6$ is the minimal poly for $\alpha \cdot \beta = \sqrt{6}$.

$\underline{①}$: We've seen that $\gamma \in \mathbb{C}$, then $\overset{N(\gamma)}{\overset{\shortparallel}{\gamma\bar{\gamma}}} \in \mathbb{R}$.

In general, if α is of degree 2 over $\mathbb{Q}$, then $\alpha\bar{\alpha} \in \mathbb{Q}$. To study the minimal poly of $\alpha+\beta$, we need to know about α & β's conjugates, i.e. other roots of their minimal polys

Namely, we have for $\alpha = \sqrt{2}$, let

$\overline{\alpha} = -\sqrt{2}$ (this is b/c the other root

of $P_{\sqrt{2}}(x) = x^2 - 2$ is $-\sqrt{2}$.) Similarly,
$= (x-\sqrt{2})(x+\sqrt{2})$

define $\overline{\beta} = -\sqrt{3}$ (for same reason). Now

lets consider the following numbers,

$\alpha+\beta$, $\overline{\alpha}+\beta$, $\alpha+\overline{\beta}$, $\overline{\alpha}+\overline{\beta}$ ← All possible numbers obtained by conjugating α or β.

Consider $f(x) = (x-(\alpha+\beta))(x-(\bar{\alpha}+\beta))(x-(\alpha+\bar{\beta}))(x-(\bar{\alpha}+\bar{\beta}))$

& note $\bar{\alpha} = -\alpha$, $\bar{\beta} = -\beta$. $\quad ((x-y)(x+y) = x^2-y^2)$

$$= (x-(\alpha+\beta))(x-(-\alpha+\beta))(x-(\alpha-\beta))(x-(-\alpha-\beta))$$

$$= (x-(\alpha+\beta))(x+(\alpha+\beta))(x-(\alpha-\beta))(x+(\alpha-\beta))$$

$$= (x^2-(\overset{\alpha^2+2\alpha\beta+\beta^2}{\overset{\shortparallel}{\alpha+\beta}})^2)(x^2-(\alpha-\beta)^2)$$

$$= x^4 - ((\alpha+\beta)^2+(\alpha-\beta)^2)x^2 + (\alpha+\beta)^2(\alpha-\beta)^2 \in \mathbb{Q}[x]$$

$$= x^4 - \left((\alpha+\beta)^2 + (\alpha-\beta)^2 \right) x^2 + (\alpha+\beta)^2 (\alpha-\beta)^2$$

$$= x^4 - \left(\alpha^2 + \cancel{2\alpha\beta} + \beta^2 + \alpha^2 - \cancel{2\alpha\beta} + \beta^2 \right) x^2 + (\alpha^2 - \beta^2)^2$$

$$= x^4 - (2\alpha^2 + 2\beta^2) x^2 + (\alpha^2 - \beta^2)^2 \quad \Big| \quad \begin{array}{l} \alpha = \sqrt{2} \\ \beta = \sqrt{3} \end{array}$$

$$= x^4 - 2(2+3)x^2 + (2-3)^2$$

$$= x^4 - 10x^2 + 1 = f(x) \in \mathbb{Q}[x].$$

$\Rightarrow$ $f(x) = P_{\sqrt{2}+\sqrt{3}}(x) = \underline{x^4 - 10x^2 + 1}$ is minimal poly for $\sqrt{2} + \sqrt{3}$.

We see here

$$\deg(P_{\alpha+\beta}(x)) > \deg(P_\alpha(x)), \deg(P_\beta(x))$$

However $\deg(P_{\alpha\beta}(x)) = \deg(P_\alpha(x)), \deg(P_\beta(x))$

but in general, we need not have equality here. Arithmetic surrounding minimal polynomials is complicated but <u>doable</u>.

Ex: You are given that π & e are transcendental over $\mathbb{Q}$ (i.e. NOT algebraic, so not a root of a finite degree poly w/ coefficients in $\mathbb{Q}$). Assuming this transcendance, prove that at most one of

$$e+\pi \quad \text{or} \quad e\pi$$

is rational.

$\left(\text{Rough: Maybe } \frac{\pi}{4} = \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n+1)!}\right)$

Pf: Assume $e+\pi$ & $e\pi$ are rational. Consider

$$f(x) = (x-e)(x-\pi) = x^2 - (e+\pi) + e\pi \in \mathbb{Q}[x]$$

However, $f(e) = f(\pi) = 0$ & $\deg(f) = 2 < \infty$.

This means that e & π are algebraic, but this contradicts the transcendance of both e & π. Hence, not both $e\pi$ & $e+\pi$ are rational (i.e. at least one is irrational).

$\square$

Ex: We want to show

$$\longrightarrow \mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3}) \leftarrow .$$

$$\parallel$$

$$\{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} : a,b,c,d \in \mathbb{Q}\}$$

has basis $\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$.

Sol: To show these fields are the same, we'll show "$\subseteq$" & "$\supseteq$". $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3})$.

"$\supseteq$": Since $\sqrt{2},\sqrt{3} \in \mathbb{Q}(\sqrt{2},\sqrt{3})$, $\Rightarrow \sqrt{2}+\sqrt{3} \in \mathbb{Q}(\sqrt{2},\sqrt{3})$ $\square$

"$\underline{\subseteq}$" We want to show $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$.

Since $(\sqrt{2}+\sqrt{3}) \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$, so is $(\sqrt{2}+\sqrt{3})^2 = 2+\sqrt{6}+3$
$= 5+\sqrt{6}$

$\Rightarrow \sqrt{6} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$

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

$-2(\sqrt{2}+\sqrt{3}) = -2(\sqrt{2}+\sqrt{3})$

everything in orange took place in our field, so its closed

i.e. $\sqrt{2} = \sqrt{6}(\sqrt{2}+\sqrt{3}) - 2(\sqrt{2}+\sqrt{3}) \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$

$\sqrt{3} = 3(\sqrt{2}+\sqrt{3}) - \sqrt{6}(\sqrt{2}+\sqrt{3}) \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$
$= 3\sqrt{2}+3\sqrt{3} - 3\sqrt{2} - 2\sqrt{3}$

$\Rightarrow \mathbb{Q}(\sqrt{2},\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}+\sqrt{3}) \Rightarrow$ Equality!

Discussion 7 5/14

Q: → Simplified version of primitive element thm:

α, β algebraic / $\mathbb{Q}$ & $[\mathbb{Q}(\beta):\mathbb{Q}] = 2$

$\Rightarrow \mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha + c\beta)$ for some $c \in \mathbb{Q}$

→ Examples w/ constructibility

In class yesterday, it was mentioned that for the poly $f(x) = x^3 - 2$, adjoining $\sqrt[3]{2}$ to $\mathbb{Q}$ is not enough to get the splitting field for f (namely, you also need one more root, just take $i\sqrt{3}$ (this is b/c other roots are $\sqrt[3]{2}\,\zeta_3$, $\sqrt[3]{2}\,\zeta_3^2$ where $\zeta_3 = e^{2\pi i/3}$ ζ_3 $\zeta_3 = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$).

Last section, we showed

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

which shows $\mathbb{Q}(\sqrt{2},\sqrt{3})$ is a <u>simple</u> extension (generated by a single element).

We'll show we can do the same w/ $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$ (i.e. its generated by a single element)

<u>Prop</u>: Let α, β be algebraic over $\mathbb{Q}$ & assume $[\mathbb{Q}(\beta):\mathbb{Q}] = 2$. Then $\exists\, c \in \mathbb{Q}$ s.t. $\mathbb{Q}(\alpha,\beta) = \mathbb{Q}(\alpha + c\beta)$.

[In comparison to $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$, $c=1$]

<u>Pf</u>: We have $\mathbb{Q}(\alpha+c\beta) \subseteq \mathbb{Q}(\alpha,\beta)$ from definition. We want to show other inclusion. Let $f(x)$ & $g(x)$ be the minimal polynomials of α & β respectively over $\mathbb{Q}$.

Then we have

$$\overset{\alpha}{\overset{\shortparallel}{\alpha_1}}, \ldots, \alpha_n \quad \text{are roots of } f(x)$$

$$\underset{\beta}{\underset{\shortparallel}{\beta_1}}, \beta_2 \quad \text{are roots of } g(x)$$

Since $[\mathbb{Q}(\beta) : \mathbb{Q}] = 2$, this implies $\beta_1 \neq \beta_2$.

Now pick $c \in \mathbb{Q} \setminus \{0\}$ that is <u>different</u> from

$$(\alpha - \alpha_i)(\beta - \beta_2) \qquad i = 2, \ldots, n$$

Consider the polynomial

$$h(x) = f(\alpha + c\beta - cx) \in \overbrace{\mathbb{Q}(\alpha + c\beta)}^{\text{want to show } \beta \text{ is in here}}[x].$$

From this definition, we see

Want these properties
$$\begin{cases} ① \ h(\beta) = 0 & \left(h(\beta) = f(\alpha + c\beta - c\beta) = f(\alpha) = 0\right) \\ ② \ h(\beta_2) \neq 0 & (\text{how we chose our } c) \end{cases}$$

$$f(\alpha + c\beta - c\beta_2) = f(\overbrace{\alpha + c(\beta - \beta_2)}^{\neq \alpha_i \ \forall i}) \neq 0$$

Since both $h(x)$ & $g(x)$ satisfy

$$h(\beta) = g(\beta) = 0,$$

the minimal poly of β over $\mathbb{Q}(\alpha + c\beta)$ divides $h(x)$ & $g(x)$. But not every root of $g(x)$ is a root of $h(x)$, hence the minimal poly of β over $\mathbb{Q}(\alpha + c\beta)$ has degree 1, & so $\beta \in \mathbb{Q}(\alpha + c\beta)$. Thus $\alpha = \alpha + c\beta - c \cdot \beta \in \mathbb{Q}(\alpha + c\beta)$. The fields are equal $\square$

Remark: The proof is good to show us why the field extensions are equal but doesn't necessarily provide good means for calculating a good c which makes this work easier.

In fact $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha + c\beta)$

for any $c \in \mathbb{Q} \setminus \{0, (\alpha - \alpha_i)(\beta - \beta_2) \text{ for } i = 2, \ldots, n\}$

Ex: If $\alpha = \sqrt[3]{2}$, $\beta = i\sqrt{3}$ $\left(P_{i\sqrt{3}}(x) = x^2+3\right)$,

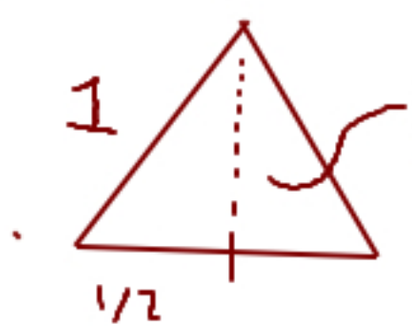
the number $c=1$ should work, i.e.,

$$\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) = \mathbb{Q}(\sqrt[3]{2} + i\sqrt{3})$$

However, showing directly is a lot of work by hand.

Ex: Is it possible to construct a square whose area is equal to that of a given triangle? (ie. if I give you an equilateral triangle, can you give me a square that has the same area?)

Sol: Suppose that the side length is equal to 1.



$h = \frac{\sqrt{3}}{2} \Rightarrow$ area $= 2 \cdot \frac{1}{2} \cdot \frac{\sqrt{3}}{2} \cdot \frac{1}{2}$

$= \sqrt{3}/4$

The area is $\frac{\sqrt{3}}{4}$, so for a square to have area $\frac{\sqrt{3}}{4}$ it must have side length $\sqrt{\frac{\sqrt{3}}{4}}$. Since $\sqrt{\frac{\sqrt{3}}{4}}$ is obtained by a sequence of square roots & field operations, it is constructible.

$\square$

Ex: The measure of a given angle is $\frac{180°}{n}$, where n is not divisible by 3. Prove that the angle can be trisected by straightedge & compass.

Pf: We want to show $\frac{60}{n}$ is constructible.

Saying $3 \nmid n$ is the same as saying $\gcd(n,3)=1$.

So $\exists s, t \in \mathbb{Z}$ s.t. $s \cdot n + t \cdot 3 = 1$.

So we have integers s & t w/

$$s \cdot n + t \cdot 3 = 1.$$

Multiply both sides by $\frac{60}{n}$

$$\Rightarrow \underset{\mathbb{Z}}{s} \cdot \underbrace{60} + \underset{\mathbb{Z}}{t} \cdot \underbrace{\frac{180}{n}} = \frac{60}{n}$$

$\mathbb{Z}$ constructible $\mathbb{Z}$ given

$\Rightarrow \frac{60}{n}$ is constructible as it is sum of multiples of constructible angles. $\square$

Ex: We've shown $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$.

We can also show $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}-\sqrt{3})$

$\Big((\sqrt{2}-\sqrt{3})^2 = 2 - 2\sqrt{6} + 3 \Rightarrow \sqrt{6} \in \mathbb{Q}(\sqrt{2}-\sqrt{3})$

$\sqrt{6}(\sqrt{2}-\sqrt{3}) = 3\sqrt{2} - 2\sqrt{3} = \sqrt{2} \in \mathbb{Q}(\sqrt{2}-\sqrt{3})\Big)$

$-2(\sqrt{2}-\sqrt{3}) \quad -2(\sqrt{2}-\sqrt{3})$

① Is it is obvious $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2}-\sqrt{3})$? Y

② Is it is obvious $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\frac{1}{2}\sqrt{3})$? N

① The reason $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2}-\sqrt{3})$

is $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}[\sqrt{2}+\sqrt{3}] = \mathbb{Q}[x] / P_{\sqrt{2}+\sqrt{3}}(x) = (\star)$

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

as another root, $P_{\sqrt{2}+\sqrt{3}}(x) = P_{\sqrt{2}-\sqrt{3}}(x)$ &

$(\star) = \mathbb{Q}[x] / P_{\sqrt{2}-\sqrt{3}}(x) = \mathbb{Q}(\sqrt{2}-\sqrt{3})$.

Discussion 8

5/21

Q: $\rightarrow$ Go over $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$

$$\cong \mathbb{F}_p^{\times} \qquad \overset{\shortparallel}{G(\mathbb{Q}(\zeta_p)/\mathbb{Q})} \ (p \text{ prime})$$

$\rightarrow$ Results on extensions

$\rightarrow$ irreducibility of $x^p - x + \alpha$ for $\alpha \neq 0$ in $\mathbb{F}_p$

① Let ζ_p be a primitive p^{th} root of unity, p prime ($\zeta_p = e^{2\pi i/p}$). Show

$$G(\mathbb{Q}(\zeta_p)/\mathbb{Q}) = \mathbb{F}_p^{\times}. \leftarrow$$

Sol: We have the following lemma:

Lem: If α & α' are roots of the same irred. poly $f \in \mathbb{F}[x]$, then $\exists$ unique isomorphism $\varphi : \mathbb{F}[\alpha] \to \mathbb{F}[\alpha']$ s.t.

① $\varphi(r) = r \quad \forall r \in \mathbb{F}$

② $\varphi(\alpha) = \alpha'$

For ζ_p = primitive p^{th} root of unity, it and all its powers are roots of $x^p - 1$.

Roots of $x^p - 1$ are $1, \zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}$.

However, this is not irreducible. But

$$\Phi_p(x) = p^{th} \text{ cyclotomic} = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1$$

is irreducible w/ roots $\zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}$.

from HW

Since p is prime, $\mathbb{Q}(\zeta_p) = \mathbb{Q}(\zeta_p^j)$ for any $j = 1, 2, \ldots, p-1$. (Reason: look at bases as vector spaces over $\mathbb{Q}$, i.e. $\{1, \zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}\}$ is a basis for both). The lemma says that $\forall j \in \{1, \ldots, p-1\}$ $\exists!\ \varphi_j : \mathbb{Q}(\zeta_p) \to \mathbb{Q}(\zeta_p^j)$ s.t. $\varphi_j(\zeta_p) = \zeta_p^j$.

Want to know how to multiply φ_j's.

Concatenation

For $j, j' \in \{1, \dots, p-1\}$, we have

$$\varphi_j \circ \varphi_{j'}(\zeta_p) = \varphi_j(\zeta_p^{j'}) = \varphi_j(\zeta_p)^{j'}$$

$$\zeta_p^{j'} = \underbrace{\zeta_p \cdot \zeta_p \cdots \zeta_p}_{j' \text{ times}} = (\zeta_p^{j})^{j'}$$

$$= \zeta_p^{jj'}$$

$$= \varphi_{jj'}(\zeta_p)$$

$\Rightarrow \varphi_j \circ \varphi_{j'} = \varphi_{jj'}$ ← Multiplication of maps (φ_j's) is same as multiplying the indices

$\Rightarrow$ Multiplication in $G(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ is same as in $\mathbb{F}_p^\times$. Also, they both are of size $p-1$. Hence

$$G(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong \mathbb{F}_p^\times \leftarrow \text{under multiplication}$$

Details of isomorphism

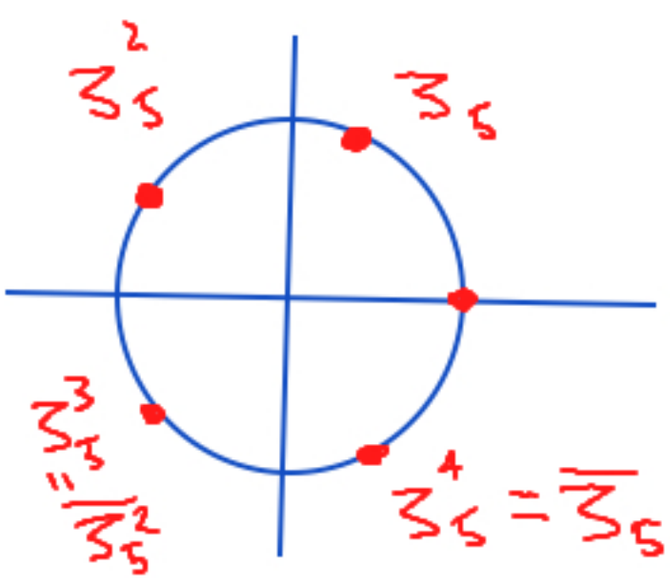
$$\begin{cases} \varphi_j \longleftarrow j \\ \varphi_j \longmapsto j \end{cases}$$

Ex: Let $p=5$. $\zeta_5 = 5^{th}$ root of unity.

Its minimal poly is $x^4+x^3+x^2+x+1$, which has roots $\zeta_5, \zeta_5^2, \zeta_5^3, \zeta_5^4$. Define

$\varphi_j \in G(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ by $\varphi_j(\zeta_5) = \zeta_5^j$, $j=1,2,3,4$

$\varphi_j(r) = r$ for $r \in \mathbb{Q}$.



$\Rightarrow$ $\varphi_1(\zeta_5) = \zeta_5$ $\quad \varphi_3(\zeta_5) = \zeta_5^3 = \overline{\zeta_5^2} = \varphi_4 \circ \varphi_2(\zeta_5)$

$\varphi_2(\zeta_5) = \zeta_5^2$ $\quad \varphi_4(\zeta_5) = \zeta_5^4 = \overline{\zeta_5}$

Note: $4 \cdot 2 \equiv 3 \pmod 5$

Consider $\varphi_4 \circ \varphi_3(\zeta_5) = \varphi_4(\zeta_5^3) = \overline{\zeta_5^3} = \zeta_5^2$

$$= \varphi_2(\zeta_5)$$

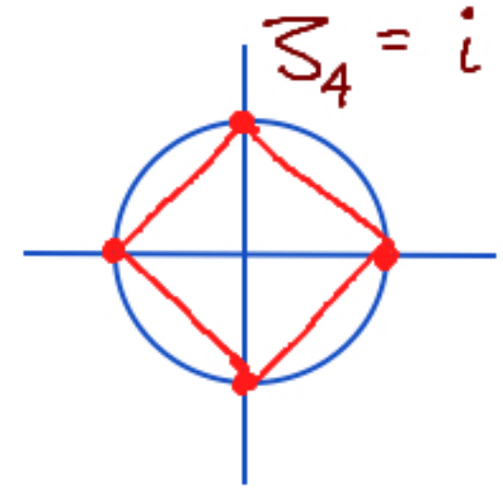
$\because$ $4 \cdot 3 = 12 \equiv 2 \pmod 5$

Takeaway: $G(\mathbb{Q}(\zeta_5)/\mathbb{Q}) \cong \mathbb{F}_5^\times$ ← cyclic of order $5-1=4$

$$\cong \mathbb{Z}/4\mathbb{Z}.$$

Ex: What if p isn't prime?

Let $p=4$, $\zeta_4 = 4^{th}$ root of unity
$= i$



$\left(\sum_{j=1}^{p} \zeta_p^j = 0\right)$
except $p=1$

Note though that minimal poly of i over $\mathbb{Q}$ is x^2+1, so $\exists!\ \varphi: \mathbb{Q}(i) \to \mathbb{Q}(-i)$ & this is the only non-trivial map in $G(\mathbb{Q}(i)/\mathbb{Q})$, namely, $\varphi(a+bi) = a-bi = \overline{a+bi}$

So $|G(\mathbb{Q}(i)/\mathbb{Q})| = 2 \neq 3 = |\mathbb{F}_4^\times|$.

$\Rightarrow G(\mathbb{Q}(\zeta_4)/\mathbb{Q}) \not\cong \mathbb{F}_4^\times$.

Very Geometric

(look at last slide)

<u>Takeaway</u>: For non-primes n, we have

$$G(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \not\cong \mathbb{F}_n^\times \leftarrow$$

this doesn't even make sense for n not a prime power

Goal is to prove the following:

<u>Lem</u>: Let $H \leq \mathrm{Aut}(\mathbb{K})$ be finite & $\mathbb{F} = \mathbb{K}^H$ $= \mathrm{Fix}(H) = \{\alpha \in \mathbb{K} : \varphi(\alpha) = \alpha \ \forall \varphi \in H\}$. Then

$$[\mathbb{K} : \mathbb{F}] = [\mathbb{K} : \mathbb{K}^H] < \infty.$$

(In fact, $[\mathbb{K} : \mathbb{K}^H] = |H|$ ← to be shown tomorrow)

We'll break this into 2 parts.

<u>Lem 1</u>: If $\mathbb{K}$ is an algebraic extension of $\mathbb{F}$ & $[\mathbb{K}:\mathbb{F}]=\infty$, for every $n>0$ $\exists \alpha \in \mathbb{K}$ s.t. $[\mathbb{F}(\alpha):\mathbb{F}]>n$. (Has elements of unbounded order)

<u>pf</u>: Let $n \in \mathbb{Z}_{>0}$ be fixed. Since $[\mathbb{K}:\mathbb{F}]=\infty$, $\exists \alpha_1 \in \mathbb{K} \setminus \mathbb{F}$. If $[\mathbb{F}(\alpha_1):\mathbb{F}]>n$, we're done. Otherwise, since $[\mathbb{F}(\alpha_1):\mathbb{F}]<\infty$ $\exists \alpha_2 \in \mathbb{K} \setminus \mathbb{F}(\alpha_1)$. So $\infty > [\mathbb{F}(\alpha_1,\alpha_2):\mathbb{F}(\alpha_1)]>1 \Rightarrow [\mathbb{F}(\alpha_1,\alpha_2):\mathbb{F}]<\infty$. By the primitive element thm, since $[\mathbb{F}(\alpha_1,\alpha_2):\mathbb{F}]<\infty$

$\exists\, \alpha_3 \in \mathbb{F}(\alpha_1, \alpha_2)$ s.t. $\mathbb{F}(\alpha_1, \alpha_2) = \mathbb{F}(\alpha_3)$.

If $[\mathbb{F}(\alpha_3) : \mathbb{F}] > n$, we're done. Otherwise, continue this procedure. Idea is that w/ each α_i adjoined, the degree of the extension <u>strictly</u> increases. So eventually (after finitely many steps) we have α_k s.t.

$$[\mathbb{F}(\alpha_k) : \mathbb{F}] > n.$$

$\square$

<u>Lem 2</u>: If $\mathbb{K}$ is an algebraic extension of $\mathbb{K}^H$, then $[\mathbb{K}^H(\alpha):\mathbb{K}^H]$ divides $|H|$ $\forall \alpha \in \mathbb{K}$.

(w/o proof / look in lec. notes 5/20)

<u>proof of Lemma</u>: Suppose for sake of contradiction that $[\mathbb{K}:\mathbb{K}^H]=\infty$. Then $\forall n \in \mathbb{Z}_{>0}$, $\exists \alpha$ s.t. $[\mathbb{K}^H(\alpha):\mathbb{K}^H]>n$ (from Lem ①). However, by Lem ② we have that $\forall \alpha \in K$, $[\mathbb{K}^H(\alpha):\mathbb{K}] \mid |H|$. If we take $n>|H|$, $\exists \alpha_n \in K$ s.t. $[\mathbb{K}^H(\alpha):\mathbb{K}^H] > n > |H|$ ↯ to $[\mathbb{K}^H(\alpha):\mathbb{K}^H] \mid |H|$. ↳

Discussion 9 5/28

Q: → Fundamental Theorem of Galois Theory (FTGT)

→ Example of FTGT at play

Thm (Fundamental Theorem of Galois Theory, FTGT)
(also called the Galois correspondence)

Let $\mathbb{K}/\mathbb{F}$ be a Galois extension, i.e. $G = G(\mathbb{K}/\mathbb{F})$.

Then there is a bijection

$$\left\{\begin{array}{c}\text{subfields}\\ \mathbb{E} \text{ of } \mathbb{K}\\ \text{containing}\\ \mathbb{F}\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{subgroups}\\ H \text{ of } G\end{array}\right\}$$

$$\begin{array}{ccc} \mathbb{K} & & 1 \\ | & & | \\ \mathbb{E} & & H \\ | & & | \\ \mathbb{F} & & G \end{array}$$

$$\mathbb{K}^H \longleftarrow\!\shortmid H$$

$$\mathbb{E} \longmapsto \{a \in \underbrace{G}_{G(\mathbb{K}/\mathbb{E})} : \underbrace{a(\mathbb{E}) = \mathbb{E}}_{=}\}$$

Under this correspondence,

H	g_2H	g_4H
g_1H	g_3H	g_5H

$[G:H] = 6$

① (inclusion reversing) If $\mathbb{E}_1, \mathbb{E}_2$ correspond to H_1, H_2 respectively, then $\mathbb{E}_1 \subseteq \mathbb{E}_2$ iff $H_1 \supseteq H_2$.

② $|\mathbb{K}:\mathbb{E}| = |H|$ & $|\mathbb{E}:\mathbb{F}| = [G:H]$ ← index of H in G:

$[G:H]$ is the size of G/H, or its the # of right (or left) cosets of H in G

$$\begin{array}{c} \mathbb{K} \\ | \ |H| \\ \mathbb{E} \\ | \ [G:H] \\ \mathbb{F} \end{array}$$

← degree of $\mathbb{K}$ over $\mathbb{E}$ is $|H|$

$|H|[G:H] = |G|$

$$\begin{array}{c} \mathbb{K} \\ | \ |H| \\ \mathbb{E} \end{array}$$

③ $\mathbb{K}/\mathbb{E}$ is always Galois w/ $G(\mathbb{K}/\mathbb{E}) \cong H$

④ $\mathbb{E}/\mathbb{F}$ is Galois iff H is normal in G.

If this is the case, then

$$G(\mathbb{E}/\mathbb{F}) \cong G/H$$

$$\begin{array}{c} \mathbb{E} \\ | \\ \mathbb{F} \end{array} \quad [G:H] = |G/H|.$$

<u>Moral of the story:</u>

The problem of studying intermediate fields of a Galois extension is the same as studying subgroups of the Galois group

* This correspondence gives uniqueness properties: if H fixes $\mathbb{E}$, then $\mathbb{E} = \mathbb{K}^H$

Ex: Let $\mathbb{K}$ = splitting field of x^4-2 over $\mathbb{Q}$, so $\mathbb{F} = \mathbb{Q}$. Find all intermediate fields & draw lattice diagram (field inclusions).

First, x^4-2 is irreducible / $\mathbb{Q}$ by Eisenstein w/ $p=2$. Let $\alpha = \sqrt[4]{2}$ be the positive real root of x^4-2. Then all roots are $\alpha, \alpha\zeta_4, \alpha\zeta_4^2, \alpha\zeta_4^3$.

But ζ_4 = primitive 4th root of unity $= i$ $(i^2=-1 \Rightarrow i^4=1)$.

$\Rightarrow$ All roots are $\alpha, i\alpha, -\alpha, -i\alpha$. $\leftarrow$ some are in $\mathbb{C}$

$\mathbb{K}$ must contain i as $i = \frac{\alpha i \in \mathbb{K}}{\alpha \in \mathbb{K}}$, hence $\mathbb{K}$ is not real. Since $\alpha \in \mathbb{R}$, $\mathbb{Q}(\alpha) \subsetneq \mathbb{K}$ (want $\mathbb{Q}(\alpha) \neq \mathbb{K}$). Let $\mathbb{E} = \mathbb{Q}(\alpha)$, which has basis $B = \{1, \alpha, \alpha^2, \alpha^3\}$ over $\mathbb{Q}$ & since X^2+1 is irred over $\mathbb{Q}(\alpha)$ & has i as a root, it is its minimal poly. Namely, $\mathbb{Q}(\alpha, i)$ is degree 2 over $\mathbb{E}$ w/ basis $\{1, i\}$. So $\mathbb{K} = \mathbb{Q}(\alpha, i)$, w/ basis $\{\overbrace{1, \alpha, \alpha^2, \alpha^3}^{B}, \overbrace{i, i\alpha, i\alpha^2, i\alpha^3}^{iB}\}$ over $\mathbb{Q}$.

$\Rightarrow [\mathbb{K} : \mathbb{Q}] = 8$. Since $\mathbb{K}/\mathbb{Q}$ is Galois ($\mathbb{K}$ is a splitting field), we know $|G(\mathbb{K}/\mathbb{Q})| = 8$.

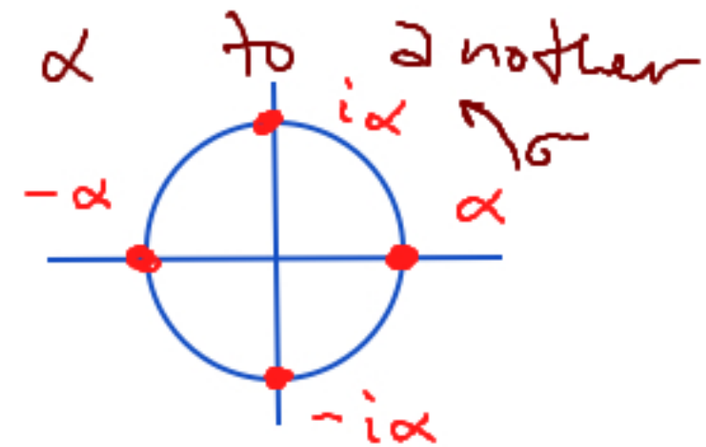
So we have to find 8 automorphisms of $\mathbb{K} = \mathbb{Q}(\alpha, i)$ which fix $\mathbb{Q}$.

$$[\mathbb{K} : \mathbb{Q}] = [\mathbb{Q}(\alpha, i) : \mathbb{Q}] = \underbrace{[\mathbb{Q}(\alpha, i) : \mathbb{Q}(\alpha)]}_{=2} \cdot \overbrace{\underbrace{[\mathbb{Q}(\alpha) : \mathbb{Q}]}_{=4}}^{=8}$$

Since $\{1, \alpha, \alpha^2, \alpha^3, i, i\alpha, i\alpha^2, i\alpha^3\}$ are a basis for $\mathbb{K}/\mathbb{Q}$, any $\sigma \in G(\mathbb{K}/\mathbb{Q})$ is defined by its action on α & i. (Since automs break up over sums & products

So $\sigma \in G(\mathbb{K}/\mathbb{Q})$ is defined by $\sigma(\alpha), \sigma(i)$.

Any automorphism must send α to another root of its minimal poly.



Define $\sigma, \tau \in G(\mathbb{K}/\mathbb{F})$ by

$\mathbb{K} = \mathbb{Q}(\alpha, i)$

$$\sigma : \begin{cases} \alpha \mapsto i\alpha \\ i \mapsto i \end{cases} \qquad \tau : \begin{cases} \alpha \mapsto \alpha \\ i \mapsto -i \end{cases}$$

$\mathrm{ord}(\tau) = 2$

$\mathrm{ord}(\sigma) = 4$

$\Uparrow$

$\sigma^4(\alpha) = \sigma(\sigma^3(\alpha)) = \sigma(-i\alpha) = \alpha$

<u>Note:</u> $\sigma^2(\alpha) = \sigma(i\alpha) = \sigma(i)\sigma(\alpha) = i(i\alpha) = -\alpha$

$\sigma^3(\alpha) = \sigma(\sigma^2(\alpha)) = \sigma(-\alpha) = -i\alpha$

So $|\langle\sigma,\tau\rangle| = \dfrac{|\langle\sigma\rangle|\,|\langle\tau\rangle|}{|\langle\sigma\rangle\cap\langle\tau\rangle|} = \dfrac{4\cdot 2}{1} = 8.$

& $|G(\mathbb{K}/\mathbb{Q})| = 8 \Rightarrow G(\mathbb{K}/\mathbb{F}) = \langle\sigma,\tau \mid \sigma^4=\tau^2=1,$ other relations)

Other relations = commutation relation b/w σ & τ.

Lets look at $\tau\sigma\tau^{-1}$ (conjugate σ by τ). $\tau^{-1}=\tau$.

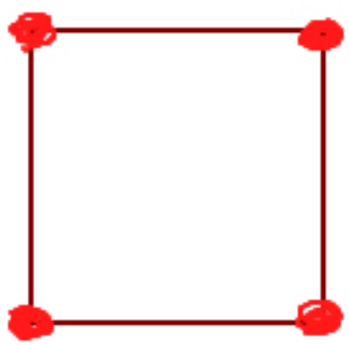
$\tau\sigma\tau(\alpha) = \tau\sigma(\alpha) = \tau(i\alpha) = \tau(i)\tau(\alpha) = -i\alpha$
$= \sigma^3(\alpha) = \sigma^{-1}(\alpha)$

$\uparrow$

$\tau\sigma\tau(i) = \tau\sigma(-i) = \tau(-i) = i = \sigma^{-1}(i) \Rightarrow \tau\sigma\tau^{-1} = \sigma^{-1}$

$$\Rightarrow G(\mathbb{K}/\mathbb{F}) = \langle \sigma, \tau \mid \sigma^4 = \tau^2 = 1, \underbrace{\tau\sigma\tau^{-1} = \sigma^{-1}}_{\text{Dihedral condition}} \rangle$$

$$\cong D_4$$



dihedral group on square

$\shortparallel$

symmetries of $\square$

In the book, we have lattice of subgroups of D_4:

$$D_4 = \langle \sigma, \tau \mid R \rangle$$

$H_1 = \{1, \sigma^2, \tau, \sigma^2\tau\}$ $\quad$ $H_2 = \{1, \sigma, \sigma^2, \sigma^3\}$ $\quad$ $H_3 = \{1, \sigma^2, \sigma\tau, \sigma^3\tau\}$

$H_4 = \{1, \tau\}$ $\quad$ $H_5 = \{1, \sigma^2\tau\}$ $\quad$ $H_6 = \{1, \sigma^2\}$ $\quad$ $H_7 = \{1, \sigma\tau\}$ $\quad$ $H_8 = \{1, \sigma^3\tau\}$

$\{1\}$

This gives lattice of intermediate fields

$$
\begin{tikzcd}
 & \mathbb{K}^{D_4} = \mathbb{Q} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{K}^{H_1} = \mathbb{Q}(\alpha^2) \arrow[d, dash] \arrow[dr, dash] & \mathbb{K}^{H_2} = \mathbb{Q}(i) \arrow[d, dash] & \mathbb{K}^{H_3} = \mathbb{Q}(i\alpha^2) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] \\
\mathbb{K}^{H_4} = \mathbb{Q}(\alpha) \arrow[dr, dash] & \mathbb{K}^{H_5} = \mathbb{Q}(i\alpha) \arrow[d, dash] & \mathbb{K}^{H_6} = \mathbb{Q}(\alpha i) \arrow[d, dash] & \mathbb{K}^{H_7} \arrow[dl, dash] \arrow[dr, dash] & \mathbb{K}^{H_8} = \mathbb{Q}(i-i\alpha) \arrow[dl, dash] \\
 & \mathbb{K}^{1} = \mathbb{Q}(\alpha, i) = \mathbb{K} & & \mathbb{Q}(i+i\alpha) &
\end{tikzcd}
$$

Discussion 10 6/4

Q: → Find fixed fields corresponding to subgroups of $G(\mathbb{K}/\mathbb{F})$

→ Class Equation

Ex: Consider $\mathbb{K}$ = splitting field of $x^4 - 2$ over $\mathbb{Q}$ $= \mathbb{Q}(\alpha, i)$ for $\alpha = \sqrt[4]{2}$. We showed last time

$$G(\mathbb{Q}(\alpha, i)/\mathbb{Q}) \cong D_4$$
$$= \langle \sigma, \tau \mid \sigma^4 = \tau^2 = 1, \tau\sigma\tau^{-1} = \sigma^{-1} \rangle$$

$$\sigma : \begin{cases} \alpha \mapsto i\alpha \\ i \mapsto i \end{cases}$$

$$\tau : \begin{cases} \alpha \mapsto \alpha \\ i \mapsto -i \end{cases}$$

D_4 has the following lattice of subgroups

$\mathbb{Q}$

$D_4 = \langle \sigma, \tau \mid R \rangle$

$[D_4 : H_1] = 2$

$\mathbb{Q}(\alpha^2)$ $\quad$ $\mathbb{Q}(i)$ $\quad$ $\mathbb{Q}(\alpha^2 i)$

$H_1 = \{1, \sigma^2, \tau, \sigma^2\tau\}$ $\quad$ $H_2 = \{1, \sigma, \sigma^2, \sigma^3\}$ $\quad$ $H_3 = \{1, \sigma^2, \sigma\tau, \sigma^3\tau\}$

$\mathbb{Q}(\alpha)$ $\quad$ $\mathbb{Q}(i, \alpha^2)$ $\quad$ $\mathbb{Q}(\alpha + i\alpha)$

$H_4 = \{1, \tau\}$ $\quad$ $H_5 = \{1, \sigma^2\tau\}$ $\quad$ $H_6 = \{1, \sigma^2\}$ $\quad$ $H_7 = \{1, \sigma\tau\}$ $\quad$ $H_8 = \{1, \sigma^3\tau\}$

$\mathbb{Q}(\alpha - i\alpha)$

$\{1\}$

2 $\quad$ 2 $\quad$ 2 $\quad$ 2 $\quad$ 2 $\quad$ 2 $\quad$ 2 $\quad$ 2 $\quad$ 2 $\quad$ 2

$\underline{H_2}$: Since $[D_4 : H_2] = 2$, $\mathbb{K}^{H_2}$ is a degree 2 extension of $\mathbb{Q}$, $\left[[G:H] = [\mathbb{K}^H : \mathbb{F}] \right]$ fixed by $H_2 = \{1, \sigma, \sigma^2, \sigma^3\}$. Since $\sigma(i) = i$ $\Rightarrow \sigma^j(i) = i \quad \forall j \in \{0, \dots, 3\}$. So $i \in \mathbb{K}^{H_2}$. $\Rightarrow$ $\mathbb{Q}(i) \subseteq \mathbb{K}^{H_2}$ but both are degree 2 extensions

$$\Rightarrow \boxed{\mathbb{K}^{H_2} = \mathbb{Q}(i)}$$

$\underline{H_6}$: So $H_6 = \underbrace{\{1, \sigma^2\}}$ & $[H_2 : H_6] = 2$, so

$\mathbb{K}^{H_6}$ is a degree 2 extension over $\mathbb{Q}(i)$

$= \mathbb{K}^{H_2}$. We need to find what is fixed by

σ^2. Well, $\sigma^2(\alpha) = \sigma(i\alpha) = i^2\alpha = -\alpha$

$\Rightarrow \sigma^2(\alpha^2) = \sigma^2(\alpha)\sigma^2(\alpha) = (-\alpha)(-\alpha) = \alpha^2$

$\Rightarrow \sigma^2$ & identity fix α^2. $\Rightarrow \boxed{\mathbb{K}^{H_6} = \mathbb{Q}(i, \alpha^2)}$

$\cong (\mathbb{Q}(i))(\alpha^2)$ $\left(P_{\alpha^2, \mathbb{Q}(i)}(x) = x^2 - 2 \text{ b/c } P(\alpha^2) = \alpha^4 - 2 = 0 \right)$

$\underline{H_4}$: We know $\tau(\alpha) = \underline{\alpha}$ & $H_4 = \{1, \underline{\tau}\}$.

Also, by looking at sizes, we have $[D_4 : H_4] = 4$. Well α is degree 4 over $\mathbb{Q}$ & fixed by H_4 $\Rightarrow$ $\boxed{\mathbb{K}^{H_4} = \mathbb{Q}(\alpha)}$

$\underline{H_1}$: By inclusion & guessing, we'll see that

$\mathbb{Q}(\alpha^2) = \mathbb{K}^{H_1}$ for $H_1 = \{1, \sigma^2, \tau, \sigma^2\tau\}$.

By previous work, we know $\sigma^2(\alpha^2) = \alpha^2$, &

$\tau(\alpha^2) = \alpha^2$. $\Rightarrow \sigma^2\tau(\alpha^2) = = \sigma^2(\alpha^2) = \alpha^2$

$\Rightarrow \alpha^2$ is fixed by H_1 & α^2 is degree

2 over $\mathbb{Q}$ ($P_{\alpha^2, \mathbb{Q}}(x) = x^2 - 2$) $\Rightarrow$ $\boxed{\mathbb{K}^{H_1} = \mathbb{Q}(\alpha^2)}$

Since $H_6 \leq H_1 \Rightarrow \underbrace{\mathbb{K}^{H_6}}_{\mathbb{Q}(i, \alpha^2)} \geq \mathbb{K}^{H_1} = \mathbb{Q}(\alpha^2)$.

$\underline{H_5}$: For $H_5 = \{1, \sigma^2\tau\}$, we have

$\sigma^2(\alpha) = -\alpha$, $\sigma^2(i) = i$ $\leftarrow$ σ^2 gives -1 to α

$\tau(\alpha) = \alpha$, $\tau(i) = -i$ $\leftarrow$ τ gives -1 to i

$$\Rightarrow \sigma^2\tau(\alpha i) = \sigma^2(\tau(\alpha)\tau(i)) = \sigma^2(\alpha(-i))$$

$$= \sigma^2(\alpha)\sigma^2(-i) = (-\alpha)(-i) = \alpha i$$

$\Rightarrow$ H_5 fixes αi & since αi is a root of $x^4 - 2$, its degree over $\mathbb{Q}$ is 4. And also $[D_4 : H_5] = 4$ $\Rightarrow$ $\boxed{\mathbb{K}^{H_5} = \mathbb{Q}(i\alpha)}$

$\underline{H_3}$: We have $H_3 = \{1, \sigma^2, \sigma\tau, \sigma^3\tau\}$.

$\sigma^2(\alpha^2) = \alpha^2$, $\sigma^2(i) = i \Rightarrow \sigma^2(\alpha^2 i) = \alpha^2 i$.

$$\sigma\tau(\alpha^2 i) = \sigma(\tau(\alpha^2)\tau(i)) = \sigma(\alpha^2(-i)) =$$

$$= \sigma(\alpha)\sigma(\alpha)\sigma(-i) = (i\alpha)(i\alpha)(-i)$$

$$= \alpha^2 i$$

$$\sigma^3\tau(\alpha^2 i) = \ldots = \alpha^2 i.$$

Note $P_{\alpha^2 i}(x) = x^2 + 2$ since $(\alpha^2 i)^2 + 2 = -\alpha^4 + 2 = 0$

$\Rightarrow [\mathbb{Q}(\alpha^2 i) : \mathbb{Q}] = 2 = [D_4 : H_3] \Rightarrow \boxed{\mathbb{K}^{H_3} = \mathbb{Q}(\alpha^2 i)}$

$\underline{H_7}$: Our group $H_7 = \{1, \sigma\tau\}$ is of size 2, so it must fix $\alpha + \sigma\tau(\alpha)$, the reason for this is if we apply either id or $\sigma\tau$ to $\alpha + \sigma\tau(\alpha)$, we're left again w/ $\alpha + \sigma\tau(\alpha) = \sum_{\varphi \in H_7} \varphi(\alpha)$. And by direct calculation,

$\alpha + \sigma\tau\alpha = \alpha + \sigma(\alpha) = \alpha + i\alpha$ & this is degree 2 over $\mathbb{Q}(\alpha^2 i)$ $\Rightarrow$ $\boxed{\mathbb{K}^{H_7} = \mathbb{Q}(\alpha + i\alpha)}$

$\underline{H_8}$: We do this similarly to H_7 but w/ $H_8 = \{1, \sigma^3\tau\}$. Note

$\alpha + \sigma^3\tau(\alpha)$ is fixed by H_8 &

$\alpha + \sigma^3\tau\alpha = \alpha + \sigma^3(\alpha) = \alpha - i\alpha$. We don't try this for i since

$i + \sigma^3\tau(i) = i + \sigma^3(-i) = i - i = 0$ which is always fixed. $\Rightarrow$ $\boxed{\mathbb{K}^{H_8} = \mathbb{Q}(\alpha - i\alpha).}$

In conclusion, we usually draw top-to-bottom

$$\begin{tikzcd}[column sep=small]
 & & \mathbb{K}^G = \mathbb{Q} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & & \\
 & \mathbb{K}^{H_1} = \mathbb{Q}(\alpha^2) \arrow[dl, dash] \arrow[dr, dash] \arrow[drr, dash] & \mathbb{K}^{H_2} = \mathbb{Q}(i) \arrow[d, dash] & \mathbb{K}^{H_3} = \mathbb{Q}(\alpha^2 i) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{K}^{H_4} = \mathbb{Q}(\alpha) \arrow[drr, dash] & \mathbb{K}^{H_5} = \mathbb{Q}(\alpha i) \arrow[dr, dash] & \mathbb{K}^{H_6} = \mathbb{Q}(i, \alpha^2) \arrow[d, dash] & \mathbb{K}^{H_7} = \mathbb{Q}(\alpha + i\alpha) \arrow[dl, dash] & \mathbb{K}^{H_8} = \mathbb{Q}(\alpha - i\alpha) \arrow[dll, dash] \\
 & & \mathbb{Q}(\alpha, i) & &
\end{tikzcd}$$

$$
\begin{tikzcd}
 & & \mathbb{Q}(\alpha, i) \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] \arrow[drr, dash] & & \\
\mathbb{Q}(\alpha) \arrow[dr, dash] & \mathbb{Q}(i\alpha) \arrow[d, dash] & \mathbb{Q}(\alpha^2, i) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \mathbb{Q}(\alpha + i\alpha) \arrow[d, dash] & \mathbb{Q}(\alpha - i\alpha) \arrow[dl, dash] \\
 & \mathbb{Q}(\alpha^2) \arrow[dr, dash] & \mathbb{Q}(i) \arrow[d, dash] & \mathbb{Q}(i\alpha^2) \arrow[dl, dash] & \\
 & & \mathbb{Q} & &
\end{tikzcd}
$$