Lecture 5.2

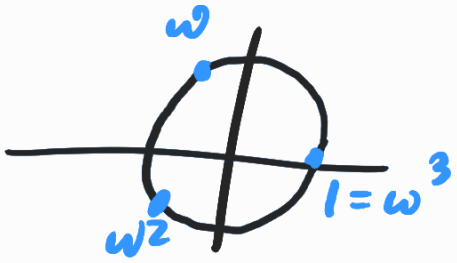
Last time:

- For a quadratic polynomial $f(x) \in \mathbb{C}[x]$, written $f(x) = x^2 + bx + c$, the roots of f are

$$x = \frac{-b \pm \sqrt{b^2 - 4c}}{2}.$$

- If $f(x) = x^3 + bx^2 + cx + d$, the roots of f are

$$x = -\left(b + \omega^k R + \frac{b^2 - 3c}{\omega^k R}\right)$$



where $\omega = e^{2\pi i/3}$ is a primitive 3rd root of unity

$0 \le k \le 2$ (so $\omega^k = 1, \omega, \omega^2$ are the 3rd roots of unity)

and

$$R = \sqrt[3]{\frac{(2b^3 - 9bc + 27d) \pm \sqrt{(2b^3 - 9bc + 27d)^2 - 4(b^2 - 3c)^3}}{2}}$$

- The roots of a quartic (degree 4) polynomial have a similar, but more complicated formula.

Perhaps more surprisingly,

Theorem There is no algebraic formula

(i.e. using $+, -, \times, \div, (\,)^n$ and $\sqrt[n]{\ }$)

for the roots of a general polynomial

$f(x)$ of degree ≥ 5.

Idea behind all the proofs: finding solutions to $f(x) = 0$ is equivalent to studying homomorphisms

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

where $f \in \ker(\varphi)$ and K is a field.

Think: φ = evaluation at $a \in K$ and

$$f(a) = 0 \Rightarrow (x-a) \mid f.$$

For such a K, there is a map

$$\mathbb{F} \hookrightarrow K$$

and a group $G = \mathrm{Aut}(K/\mathbb{F})$

that acts on the roots of polynomials in a way that makes it easier to study the roots algebraically.

When $\deg f = 2, 3, 4$, G is a

subgroup of S_2, S_3 or S_4 and the group theory of S_n allows one to find algebraic formulas for the roots of f.

When $\deg f \geq 5$, $G \leq S_n$ for $n \geq 5$ and no such formulas exist!

Évariste Galois (1811–1832) was a French mathematician who devised some of these algebraic techniques for the purposes of studying roots

of polynomials and some related questions.

Galois Theory, named in his honor, reaches much further and allows mathematicians to study field extensions like K/F using group theory.

Field Extensions

Recall that if F and K are fields, then any ring homomorphism $\varphi: F \to K$

is automatically injective.

Therefore F can be viewed as a subfield of K.

Def Let $F \subseteq K$ be a subfield. Then we say K is a **field extension** of F, written K/F.

not to be confused with G/H or A/I

Recall from linear algebra that a **vector space** over F is an abelian group V equipped with "scalar

group V equipped with

multiplication by F", i.e. a map

$$F \times V \longrightarrow V$$

$$(a, v) \longmapsto av$$

satisfying:

- $(ab)v = a(bv)$ for all $v \in V$, $a, b \in F$
- $1v = v$ for all $v \in V$
- $(a+b)v = av + bv$ for all $a, b \in F$, $v \in V$
- $a(v+w) = av + aw$ for all $a \in F$, $v, w \in V$.

Lemma If K/F is a field extension then K is an F-vector space.

Pf: Define scalar multiplication using the ring operation on K:

$$F \times K \longrightarrow K$$
$$(a, b) \longmapsto ab.$$

Then the vector space axioms follow from the field axioms for F, K. □

Def The degree of a field extension

Def

K/F is the dimension of K as an F-vector space, written $[K:F]$.

If $[K:F] < \infty$, we say K/F is a finite extension.

not $[G:H]$

Ex ① $\mathbb{C}/\mathbb{R}$ is a field extension.

Explicitly, $\mathbb{C} = \{x+iy \mid x, y \in \mathbb{R}\}$ so we see that $[\mathbb{C}:\mathbb{R}] = \dim_{\mathbb{R}} \mathbb{C} = 2$.

② $\mathbb{R}/\mathbb{Q}$ and $\mathbb{C}/\mathbb{Q}$ are field

extensions, and both have infinite degree.

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

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

"F adjoin $\sqrt{2}$"

Formally,

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

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

Multiplication is given by FOIL:

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

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

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

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

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

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

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

Notice that we have a homomorphism

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

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

So $F(\sqrt{2})/F$ is a field extension and we see that $[F(\sqrt{2}) : F] = 2$.

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

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

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

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

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

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

Think: $F(\sqrt{\alpha})$ is the smallest field

containing F and a square root of α.

By construction, $[F(\sqrt{\alpha}) : F] = 2$, as long as $\alpha \neq \beta^2$ for any $\beta \in F$.

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

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

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

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

If $b^2 - 4ac$ has a square root, say $b^2 - 4ac = \beta^2$ for $\beta \in F$, then $f(x)$ is reducible:

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

(the quadratic formula!)

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

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

$= \{s+t\beta \mid s,t \in F\}$

$$F(\beta) = F(\sqrt{b^2-4ac}) = F[x]/(f)$$

is a field extension of F with

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

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

Next time: more on field extensions, and are there quadratic field extensions in characteristic 2?