Lecture 10.1

Where we're going: given an algebraic number $\alpha \in \mathbb{C}$, there is a group that acts on the set of roots of its minimal polynomial $p_\alpha(x)$.

Often, questions about the polynomial, e.g.

"what are the irreducible factors over some field extension?"

can be translated and solved using group theory.

Ex 1 Let $f(x) = x^4 - 4x^2 + 5$

Let $f(x) = x^4 - 4x^2 - 5$.

Treating this as a quadratic polynomial in x^2, we see that

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

So the 4 complex roots of $f(x)$ are

$$\alpha_1 = \sqrt{5}, \quad \alpha_2 = -\sqrt{5}, \quad \alpha_3 = i, \quad \alpha_4 = -i.$$

There are lots of groups that act on these 4 elements, e.g. S_4 acts by permuting the subscripts, but the type of group actions we are interested in are those that preserve algebraic relations between the roots, e.g.

$$\alpha_1^2 - 5 = 0, \quad \alpha_4^2 + 1 = 0, \quad \alpha_1 + \alpha_2 = 0$$

$$\alpha_1\alpha_4 - \alpha_2\alpha_3 = 0, \quad \alpha_3 + \alpha_4 = 0, \text{ etc.}$$

Define

$$G(f) = \left\{ \begin{array}{l} \text{permutations} \\ \sigma : \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\} \to \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\} \end{array} \middle| \right.$$

for any polynomial relation satisfied by $\alpha_1, \alpha_2, \alpha_3, \alpha_4$, the permuted elements $\sigma(\alpha_1), \sigma(\alpha_2), \sigma(\alpha_3), \sigma(\alpha_4)$ also satisfy the same relation $\}$.

Exercise 1: Check that $G(f)$ is a group.

Here are some permutations in $G(f)$:

$$\alpha_1 \mapsto \alpha_1$$

$\alpha_1 \longmapsto \alpha_2$

$\mathrm{id}: \quad \alpha_2 \longmapsto \alpha_2$

$\alpha_3 \longmapsto \alpha_3$

$\alpha_4 \longmapsto \alpha_4$

$\sigma: \quad \alpha_1 \longmapsto \alpha_2$

$\alpha_2 \longmapsto \alpha_1$

$\alpha_3 \longmapsto \alpha_3$

$\alpha_4 \longmapsto \alpha_4$

$\alpha_1 \longmapsto \alpha_1$

$\tau: \quad \alpha_2 \longmapsto \alpha_2$

$\alpha_3 \longmapsto \alpha_4$

$\alpha_4 \longmapsto \alpha_3$

$\tau\sigma: \quad \alpha_1 \longmapsto \alpha_2$

$\alpha_2 \longmapsto \alpha_1$

$\alpha_3 \longmapsto \alpha_4$

$\alpha_4 \longmapsto \alpha_3$

Exercise 2 (8.1 in the textbook): Verify that $\sigma, \tau \in G(f)$. Of course $\tau\sigma \in G(f)$ then, once you've done Exercise 1.

On the other hand, some permutations do not preserve all algebraic relations:

γ :
$\alpha_1 \longmapsto \alpha_2$
$\alpha_2 \longmapsto \alpha_3$
$\alpha_3 \longmapsto \alpha_4$
$\alpha_4 \longmapsto \alpha_1$

$\alpha_1 + \alpha_2 = \sqrt{5} - \sqrt{5} = 0$

but $\gamma(\alpha_1) + \gamma(\alpha_2) = -\sqrt{5} + i \neq 0.$

δ :
$\alpha_1 \longmapsto \alpha_1$
$\alpha_2 \longmapsto \alpha_3$
$\alpha_3 \longmapsto \alpha_4$
$\alpha_4 \longmapsto \alpha_2$

$\alpha_1\alpha_4 - \alpha_2\alpha_3 = \sqrt{5}(-i) - (-\sqrt{5})i = 0$

but $\delta(\alpha_1)\delta(\alpha_4) - \delta(\alpha_2)\delta(\alpha_3)$

$= \sqrt{5}(-\sqrt{5}) - i(-i) \neq 0.$

With a bit of work, we can see that

$$G(f) = \{ id, \sigma, \tau, \tau\sigma \}.$$

Can you see what group this is isomorphic to?

Consider the subgroup $\langle \sigma \rangle = \{ id, \sigma \} \subseteq G(f)$.

Claim: the set of elements in the field

$$K = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$$

fixed by all permutations in $\langle \sigma \rangle$ is precisely the subfield $\mathbb{Q}(\alpha_3, \alpha_4)$. Similarly, the set of elements in K fixed by all of $G(f)$ is the subfield $\mathbb{Q}$.

$$\begin{array}{ll} K = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4) & \{id\} \\ \cup & \cap \\ \mathbb{Q}(\alpha_3, \alpha_4) & \langle \sigma \rangle \end{array}$$

$\cup$	$\cap$
$\mathbb{Q}$	$G(f)$

The amazing fact is that the four roots $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ can be recovered from this group structure!

Since $\alpha_1 + \alpha_2$ and $\alpha_1\alpha_2$ are both fixed by $\langle\sigma\rangle$, they must lie in $\mathbb{Q}(\alpha_3, \alpha_4)$, but then

$$(x-\alpha_1)(x-\alpha_2) = x^2 - (\alpha_1+\alpha_2)x + \alpha_1\alpha_2$$

must be the minimal polynomial of α_1 and α_2 over $\mathbb{Q}(\alpha_3, \alpha_4)$

This allows us to express the roots α_1 and α_2 in terms of algebraic functions of α_3 and α_4 — or vice versa, if we use $\langle z \rangle \subseteq G(f)$ instead.

With a little more work, this will produce the quartic formula for any polynomial of degree 4 whose group of permutations $G(f)$ is isomorphic to the one above.

Exercise 3: Find the roots of

$$f(x) = x^4 - 8x^2 + 15$$

using algebraic expressions of the coefficients of f (i.e. solve f by radicals).

Field Homomorphisms

The modern version of Galois theory uses the language of field homomorphisms.

Def Let K/F and L/F be two field

extensions of F. An **F-homomorphism** from K to L is a ring homomorphism

$$\varphi : K \longrightarrow L$$

that preserves the subfield F, i.e. for all $x \in F \subseteq K$, $\varphi(x) = x \in F \subseteq L$.

An **F-automorphism** of K/F is an F-homomorphism that is bijective. The set of all F-automorphisms of K/F is denoted $\mathrm{Aut}(K/F)$.

Lemma For any extension K/F, $\mathrm{Aut}(K/F)$

is a group under composition.

Pf: Composition is associative, the identity on K is the identity and bijections have inverses. □

Ex ② For the extension $\mathbb{C}/\mathbb{R}$, complex conjugation is an $\mathbb{R}$-automorphism:

$$\tau : \mathbb{C} \longrightarrow \mathbb{C}$$

$$z = x + iy \longmapsto \bar{z} = x - iy.$$

In fact, $\mathrm{Aut}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}, \tau\}$ because for any $\mathbb{R}$-automorphism $\varphi : \mathbb{C} \to \mathbb{C}$,

$$\varphi(i)^2 = \varphi(i^2) = \varphi(-1) = -1.$$

③ Let $\zeta = \zeta_3 = e^{2\pi i/3}$ be a 3rd root of unity and $K = \mathbb{Q}(\zeta)$ the 3rd cyclotomic extension of $\mathbb{Q}$. We know

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = 3 - 1 = 2$$

with $\mathbb{Q}$-basis $\{1, \zeta\}$. Define

$$\varphi : \mathbb{Q}(\zeta) \longrightarrow \mathbb{Q}(\zeta)$$

$$a + b\zeta \longmapsto a + b\zeta^2 = a - b - b\zeta$$

since $\zeta^2 = -1 - \zeta$

This is a $\mathbb{Q}$-automorphism of $\mathbb{Q}(\zeta)$:

- φ is clearly $\mathbb{Q}$-linear

- $\varphi(\zeta^2) = \varphi(-1-\zeta) = -1-\zeta^2 = \zeta = \zeta^4 = \varphi(\zeta)^2$

- $\varphi((a+b\zeta)(c+d\zeta)) = \varphi(ac + (ad+bc)\zeta + bd(\zeta^2)$

$$= ac + (ad+bc)\zeta^2 + bd\zeta$$

$$= ac + (ad+bc)\zeta^2 + bd\zeta^4$$

$$= (a+b\zeta^2)(c+d\zeta^2)$$

$$= \varphi(a+b\zeta)\,\varphi(c+d\zeta)$$

- $\varphi(a) = a$ for any $a \in \mathbb{Q}$.

See if you can prove that

$$\mathrm{Aut}(\mathbb{Q}(\zeta)/\mathbb{Q}) = \{\mathrm{id}, \varphi\}.$$

④ The $\mathbb{Q}$-linear map

$$\varphi : \mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{Q}(\sqrt{3})$$

$$a + b\sqrt{2} \longmapsto a + b\sqrt{3}$$

is an isomorphism of $\mathbb{Q}$-vector spaces, but it is NOT a $\mathbb{Q}$-homomorphism:

$$\varphi(\sqrt{2}\sqrt{2}) = \varphi(2) = 2$$

but $\varphi(\sqrt{2})\varphi(\sqrt{2}) = \sqrt{3}\sqrt{3} = 3.$

⑤ Let $\alpha = \sqrt[3]{2}$, so that

$$\mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(x^3 - 2).$$

This is a degree 3 extension of $\mathbb{Q}$

with basis $\{1, \alpha, \alpha^2\} \subseteq \mathbb{R}$.

Suppose $\varphi \in \mathrm{Aut}(\mathbb{Q}(\alpha)/\mathbb{Q})$. Then

$$\varphi(\alpha)^3 = \varphi(\alpha^3) = \varphi(2) = 2.$$

But α is the only real cube root of 2, so $\varphi(\alpha) = \alpha$, forcing $\varphi = \mathrm{id}$.

This means $\mathrm{Aut}(\mathbb{Q}(\alpha)/\mathbb{Q}) = \{\mathrm{id}\}$.

Next time: more on field homomorphisms.