# Galois' Theory and the Algebraic Closedness of $\mathbf{C}$

Ahaan

# Outline

- Properties of $\mathbf{R}$
- Group Theory Necessities
- $\mathbf{C}$ is algebraically closed

# Some properties of $\mathbf{R}$

### Lemma

(i) *If* $y \in (0, \infty)$*, then* $\exists x \in \mathbf{R} : x^2 = y$.

(ii) *If* $f \in \mathbf{R}[t]$ *and* $\deg f \equiv_2 1$*, then* $\exists x \in \mathbf{R} : f(x) = 0$.

### Remark

Separability need not be worried about when applying Galois' fundamental theorem to finite normal extensions of $\mathbf{R}$: since $\mathbf{R} \leq \mathbf{C}$, every algebraic extension is separable. More generally, it suffices to note that $\operatorname{char} \mathbf{R} = 0$.

# $p$-groups

### Remark

Recall:

(i) a finite group $G$ is a $p$-group if $|G| = p^n$, for some $n \in \mathbf{N}$;

(ii) the centre of a finite $p$-group is non-trivial.

### Lemma ($p$-chain)

*If* $|G| = p^n$*, for some* $n \in \{0, 1, \dots\}$*, then* $\exists G_0, \dots, G_n \lhd G$ :

$$\forall i \in \{0, \dots, n\}\ |G_i| = p^i \text{ and } G_0 \subset \cdots \subset G_n.$$

# Proof of the $p$-chain lemma

## Proof (induction).

See that the conclusion holds if $n = 0$. Suppose $n \in \{1, 2 \ldots\}$ and the conclusion holds for $n - 1$. Now $|G| = p^n \implies |Z(G)| = p^s$, for some $1 < s \leq n$. So $\exists z \in Z(G) : |\langle z \rangle| = p$. Since $\langle z \rangle \lhd G$, $|G/\langle z \rangle| = p^{n-1}$, and the inductive hypothesis yields a chain

$$G_1/\langle z \rangle \subset \cdots \subset G_n/\langle z \rangle$$

where $i \in \{1, \ldots, n\} \implies |G_i/\langle z \rangle| = p^i$ and $G_i/\langle z \rangle \lhd G/\langle z \rangle$. But then $|G_i| = p^{i+1}$ and $G_i \lhd G$. Taking $G_0 = 1$ concludes. $\square$

# The degree of a finite extension of $\mathbf{R}$

## Lemma

*Suppose $M$ is a non-trivial finite extension of $\mathbf{R}$. Then:*

(i) $[M : \mathbf{R}] \equiv_2 0$;

(ii) *if $[M : \mathbf{R}]$ is normal, then for any odd prime $p$, $[M : \mathbf{R}] \not\equiv_p 0$.*

## Proof.

(i) Suppose not. Let $\alpha \in M \setminus \mathbf{R}$. Denote by $m$ the minimal polynomial of $\alpha$ over $\mathbf{R}$. Then $\deg m \mid [M : \mathbf{R}]$, so $\deg m \equiv_2 1$. So $\exists x \in \mathbf{R} : m(x) = 0$, contradiction.

(ii) By (i), $[M : \mathbf{R}] \equiv_2 0$ and by the fundamental theorem, $|\Gamma(M : \mathbf{R})| \equiv_2 0$. Let $H \in \mathrm{Syl}_2 \Gamma$. Then $[\Gamma : H] \not\equiv_2 0$ and again by the fundamental theorem, $\left[H^\dagger : \mathbf{R}\right] \not\equiv_2 0$. But by (i) $H^\dagger \neq \mathbf{R} \implies \left[H^\dagger : \mathbf{R}\right] \equiv_2 0$. So it must be that $H^\dagger = \mathbf{R}$ and $\Gamma = H$, whence the result follows. $\square$

# $\mathbf{C}$ is algebraically closed

### Theorem

*There are no non-trivial finite extensions of* $\mathbf{R}(\mathrm{i})$.

### Proof.

Suppose $M$ is a non-trivial finite extension of $\mathbf{R}(\mathrm{i})$. WLOG assume $M : \mathbf{R}$ is normal. By the preceding lemma, $\Gamma(M : \mathbf{R})$ is a $2$-group. By the $p$-chain lemma and the fundamental theorem, there is an extension $N$ of $\mathbf{R}(\mathrm{i})$ such that $[N : \mathbf{R}(\mathrm{i})] = 2$. Then $\exists \alpha \in \mathbf{R}(\mathrm{i}) : N = \mathbf{R}(\mathrm{i})(\sqrt{\alpha})$. Write $\alpha = a + b\mathrm{i}$, for some $a, b \in \mathbf{R}$. Then

$$\sqrt{a + b\mathrm{i}} = \pm \left( \sqrt{\frac{a + \sqrt{a^2 + b^2}}{2}} + \mathrm{i}\sqrt{\frac{-a + \sqrt{a^2 + b^2}}{2}} \right) \in \mathbf{R}(\mathrm{i})$$

so $N = \mathbf{R}(\mathrm{i})$, contradiction. □

### Corollary (Fundamental Theorem of Algebra)

*Let* $f \in \mathbf{C}[t]$. *If* $\deg f \geq 1$, *then* $f$ *splits over* $\mathbf{C}$.