Galois Theory and the Algebraic Closedness of $\mathbb{C}$

Ahaan

Outline

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

Some properties of $\mathbb{R}$

Lemma

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

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

Remark

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

p-groups

Remark

Recall:

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

(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 $n \in \{1, 2 \dots\}$ 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 $i \in \{1, \dots, n\} \implies |G_i/\langle z \rangle| = p^i$ 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 $\mathbb{R}$

Lemma

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

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

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

Proof.

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

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

$\mathbb{C}$ is algebraically closed

Theorem

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

Proof.

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

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

so $N = \mathbb{R}(\mathrm{i})$, contradiction. $\square$

Corollary (Fundamental Theorem of Algebra)

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