Universidad de Alcalá

Apellidos: | Pág.:
Nombre: | Fecha:
Titulación:
Asignatura: | Curso / grupo:

2.1. Algebraic numbers

Def: $\alpha \in \mathbb{C}$ is algebraic $/\mathbb{Q}$ if $\exists\, p(x) \in \mathbb{Q}[x]$ ($\Leftrightarrow \in \mathbb{Z}[x]$) s.t. $p(\alpha)=0$.

$\mathbb{A} :=$ algebraics $/\mathbb{Q}$.

Thm 2.1 $\mathbb{A} \subseteq \mathbb{C}$ is a field.

Proof: $\alpha \in \mathbb{A} \Leftrightarrow [\mathbb{Q}(\alpha):\mathbb{Q}] < \infty$

Now, $\alpha, \beta \in \mathbb{A} \Rightarrow [\mathbb{Q}(\alpha):\mathbb{Q}], [\mathbb{Q}(\beta):\mathbb{Q}] < \infty \Rightarrow \exists\, p(x) \in \mathbb{Q}[x] \subseteq \mathbb{Q}(\alpha)[x]$ s.t.

$p(\beta)=0 \Rightarrow [\mathbb{Q}(\alpha,\beta):\mathbb{Q}(\alpha)] < \infty \Rightarrow [\mathbb{Q}(\alpha,\beta):\mathbb{Q}] = [\mathbb{Q}(\alpha,\beta):\mathbb{Q}(\alpha)][\mathbb{Q}(\alpha):\mathbb{Q}] < \infty$

$\Rightarrow \alpha+\beta, \alpha\beta$ algebraic since $[\mathbb{Q}(\alpha,\beta):\mathbb{Q}] = [\mathbb{Q}(\alpha,\beta):\mathbb{Q}(\alpha+\beta)][\mathbb{Q}(\alpha+\beta):\mathbb{Q}]$. #

Obs: $\mathbb{A}/\mathbb{Q}$ not finite $\because$ $[\mathbb{Q}(\zeta_p):\mathbb{Q}] = p-1$.

Def: A number field is $K|\mathbb{Q}$ finite $\Rightarrow K = \mathbb{Q}(\alpha_1, \dots, \alpha_n)$

Thm 2.2 (primitive element)

$K|\mathbb{Q}$ number field $\Rightarrow K = \mathbb{Q}(\theta)$.

Proof

If $K = \mathbb{Q}(\alpha_1)$ ok.

Assume that if $K = \mathbb{Q}(\alpha_1, \dots, \alpha_n) \Rightarrow K = \mathbb{Q}(\theta)$. Must prove that if $K = \mathbb{Q}(\alpha_1, \dots, \alpha_{n+1})$

$\Rightarrow K = \mathbb{Q}(\theta)$.

For that, we will prove that if $K = K_1(\alpha,\beta)$, $K_1 \subseteq K \Rightarrow K = K_1(\theta)$

since in this case, if $K = \mathbb{Q}(\alpha_1, \dots, \alpha_{n+1}) = \mathbb{Q}(\alpha_1, \dots, \alpha_n)(\alpha_{n+1}) = \mathbb{Q}(\theta)(\alpha_{n+1}) =$

$= \mathbb{Q}(\theta, \alpha_{n+1}) \underset{\substack{\uparrow \\ K_1 = \mathbb{Q}}}{=} \mathbb{Q}(\psi)$.

$p(t) = \mathrm{Irr}(K_1,\alpha) = \prod_{i=1}^{n}(t-\alpha_i)$ $\{\alpha_i\}$ distinct $\alpha_1 = \alpha$.

$q(t) = \mathrm{Irr}(K_1,\beta) = \prod_{i=1}^{m}(t-\beta_i)$ $\{\beta_j\}$ distinct. $\beta_1 = \beta$. $\alpha_i \neq \beta_1$

$\forall i \in \{1,\dots,n\}$, $\forall k \in \{2,\dots,m\}$ there is at most $x \in K$ s.t $\alpha_i + x\beta_k =$
$= \alpha_1 + x\beta_1$

if there were 2 : $\alpha_1 + x\beta_1 = \alpha_1 + y\beta_1 \Rightarrow x = y$.

$\Rightarrow \boxed{\exists c \neq 0 \text{ s.t. } \alpha_i + c\beta_k \neq \alpha_1 + c\beta_1 \quad \forall i,k, \quad \theta := \alpha + c\beta}$

$K_1(\theta) \subseteq K_1(\alpha,\beta)$.

now let's see $\beta \in K_1(\theta = \alpha + c\beta) \Rightarrow \alpha = \theta - c\beta \in K_1(\theta)$:

$p(\theta - c\beta) = p(\alpha) = 0$

$r(t) := p(\theta - ct) \in K_1(\theta)(t) \Rightarrow r(\beta) = 0$ $\Rightarrow$ they have only this common
$q(\beta) = 0$ zero

if $q(\xi) = r(\xi) = 0 \Rightarrow \xi = \beta_i$
$\theta - c\xi = \alpha_k$ $\Rightarrow \alpha_k + c\beta_k = \theta = \alpha + c\beta$!

$h(t) = \mathrm{Irr}(K_1(\theta),\beta) \Rightarrow h(t) | q(t)$
$h(t) | r(t)$ $\Rightarrow \partial h = 1$, $h(t) = t + \mu$, $h(\beta) = \beta + \mu = 0$

$\Rightarrow \beta \in K_1(\theta)$ #

2.2. Conjugates and discriminants

$K = \mathbb{Q}(\theta)$ number field. $\exists$ several monomorphisms (of fields) $K \xhookrightarrow{\sigma} \mathbb{C}$,

e.g. $K = \mathbb{Q}(i)$ $\sigma(x+iy) = x \pm iy$.

obs: $\sigma(1) = 1 \Rightarrow \sigma(n) = n$, $\sigma\left(\frac{n}{m}\right) = \frac{\sigma(n)}{\sigma(m)} = \frac{n}{m} \Rightarrow \sigma|_{\mathbb{Q}} = \mathrm{Id}$.

Thm $K = \mathbb{Q}(\theta)$ $[K:\mathbb{Q}] = n \Rightarrow \exists n$ distinct monomorphisms $\sigma_i : K \hookrightarrow \mathbb{C}$

all of them are characterised by $\sigma_i(\theta) = \theta_i$ distinct roots of

$\mathrm{Irr}(\mathbb{Q},\theta)$.

Universidad de Alcalá

Apellidos: | Pág.:
Nombre: | Fecha:
Titulación:
Asignatura: | Curso / grupo:

Proof: $\{\theta_1,\dots,\theta_n\}$ distinct roots of $p(t) = Irr(\mathbb{Q},\theta) = Irr(\mathbb{Q},\theta_i)$.

$\Rightarrow$ the $\{\sigma_1,\dots,\sigma_n\}$ are distinct monomorphisms.

$\Rightarrow \exists!\ \sigma_i : \mathbb{Q}(\theta) \cong \mathbb{Q}(\theta_i) \hookrightarrow \mathbb{C}$ if $\exists\ \sigma : K \hookrightarrow \mathbb{C} \Rightarrow$ given $\alpha \in \mathbb{Q}(\theta)$
$\theta \mapsto \theta_i$

$\alpha = r(\theta) \Rightarrow \sigma(\alpha) = \sigma(r(\theta)) = r(\sigma(\theta)) = \underset{''}{r(\theta_i)} = \sigma(r(\theta)) = \sigma(\alpha)$ #.

Def: $\alpha \in K = \mathbb{Q}(\theta)$. The field polynomial of α/K is $f_\alpha(t) = \prod_{i=1}^{n}(t - \sigma_i(\alpha))$.

$\Rightarrow f_\alpha(t) \in K[t]$

Lemma (Cor. 1.14) K/L, $p(t) \in K[t]$, $\partial p = n$
Let $\theta_1,\dots,\theta_n \in L$ be the zeros of $p(t)$. Then, if $h(t_1,\dots,t_n) \in K[t_1\dots t_n]$ symmetric $\Rightarrow h(\theta_1,\dots,\theta_n) \in K$.

Thm: $f_\alpha(t) \in \mathbb{Q}[t]$.

Proof: $\alpha = r(\theta)$, $r(t) \in \mathbb{Q}[t]$, $\partial r < n \Rightarrow f_\alpha(t) = \prod_{i=1}^{n}(t - \underset{\sigma_i(\alpha)}{\underbrace{r(\theta_i)}}) \Rightarrow$

the coeffs of $f_\alpha(t)$ are $h(\theta_1,\dots,\theta_n)$, h symmetric and $\{\theta_1,\dots,\theta_n\}$ roots of $Irr(\mathbb{Q},\theta) \Rightarrow h(\theta_1,\dots,\theta_n) \in \mathbb{Q}$.

Def: $\{\sigma_i(\alpha),\ 1 \le i \le n\}$ are called the K-conjugates of α

Notice: Although the θ_i are distinct, the K-conjugates of α might not be

so: $\sigma_i(1) = 1\ \forall i$.

$\boxed{\text{Thm (2.6)} \leftarrow \text{Tuesday 27}}$