Algebraic conjugates

Lecture 5

Suppose that $\mathbb{F}$ is a field and $f \in \mathbb{F}[t]$ is an irreducible pol. Then one can define the quotient ring $\mathbb{F}[t]/(f)$ (i.e. $g \sim h \Leftrightarrow f \mid (g-h)$)

As above, one can see that $\mathbb{F}[t]/(f)$ is a field. Indeed, if $g \in \mathbb{F}[t]$, $f \nmid g$, then f & g are coprime (recall that f is irreducible) and hence $\exists\, a, b : 1 = af + bg \Rightarrow bg \in 1 + (f)$
$\Rightarrow b + (f)$ is the multiplicative inverse of $g + (f)$ in $K[t]/(f)$.

Cor. $L:K$, $\alpha \in L$ is algebraic over K. Then $K[t]/(\mu_\alpha^K)$ is a field.

Thm 1 Let K be a field, $f \in K[t]$ is irreducible. Then $\exists$ a field extension $\varphi : K \to L$ s.t. L contains a root of $\varphi(f)$.

Pf. Put $L := K[t]/(f)$. Then L is a field and $\varphi : K \to L$, where $\varphi(k) = k + (f)$, $\forall k \in K$ is a homomorphism and hence $L:K$ is a field extension. It remains to prove that L contains a root of $\varphi(f)$. Let

$f = a_0 + \ldots + a_n t^n$ and put $\alpha = t + (f)$

Then $(\varphi(f))(\alpha) = \sum \varphi(a_i)\alpha^i$

$$= \sum (a_j + (f))(t + (f))^j$$
$$= \sum (a_j t^j + (f)) = f + (f) = (f).$$

In other words, $(\varphi(\underbrace{f}_{L}))(\alpha) = 0$ in L ∎

Exm Consider $\underbrace{\mathbb{F}_2[t]/(t^2+t+1)}$ $\Rightarrow$ the coset representetatives are $0, 1, t, t+1$ $(= \{at + b \mid a, b \in \mathbb{F}_2\})$. In $\mathbb{F}_2[t]$ there is no $g \in \mathbb{F}_2[t]$ s.t. $g^2 = t+1$. But in L:

$$\alpha = t + (t^2+t+1) \Rightarrow \alpha^2 = t^2 + (t^2+t+1)$$
$$= t+1 + (t^2+t+1).$$

By consistently applying Thm. 1 we can obtain a tower of field extensions $K_n : \dots : K_2 : K$ s.t. our polynomial $f \in K[t]$ factors as a product of linear polynomials over K_n (but some accuracy is required to create a global field $\overline{K}$ s.t. any polynomial is a product of linear polynomials, we will discuss this later).

Algebraic conjugates Let us start with an

Exm 1) $\mathbb{R} - \mathbb{C}$. Then the complex conjugate of $a+ib$ is $a-ib$

2) $\mathbb{Q} - \mathbb{Q}(\sqrt{2})$. Then $a \pm \sqrt{2}\, b$ are conjugate elements

3) $\mathbb{Q} - \mathbb{Q}(\sqrt[3]{2})$: $\sqrt[3]{2}$, $\varepsilon_3 \sqrt[3]{2}$, $\varepsilon_3^2 \sqrt[3]{2}$

Df. Let μ_α^K be the minimal pol. and suppose that μ_α^K factors as a product of linear polynomials over a field $L \supseteq K$:

$$\mu_\alpha^K(x) = (x-\alpha_1)\ldots(x-\alpha_n), \quad \alpha_1, \ldots, \alpha_n \in L$$

Then $\alpha_1, \ldots, \alpha_n$ are algebraic conjugates of our algebraic element α.

Exm 1) $\alpha = \cos\frac{2\pi}{9} \Rightarrow \alpha_1 = \alpha$, $\alpha_2 = \cos\frac{4\pi}{9}$, $\alpha_3 = \cos\frac{8\pi}{9}$

2) Take $\alpha = i \Rightarrow \mu_\alpha^{\mathbb{R}} = x^2+1 \Rightarrow i, -i$ are algebraic conjugates of i over $\mathbb{R}$. But $\mu_\alpha^{\mathbb{C}}(x) = x - i \Rightarrow$ the only conjugate of i over $\mathbb{C}$ is i.

3) $x^4 - 2 \Rightarrow$ over $\mathbb{Q}$ we have 4 conjugates: $\sqrt[4]{2}$, $-\sqrt[4]{2}$, $i\sqrt[4]{2}$, $-i\sqrt[4]{2}$ but over $\mathbb{Q}(\sqrt{2})$:

$x^4 - 2 = (x^2 - \sqrt{2})(x^2 + \sqrt{2})$ and each $x^2 \pm \sqrt{2}$ is irreducible over $\mathbb{Q}(\sqrt{2}) \Rightarrow \pm\sqrt[4]{2}$ are conjugated and $\pm i\sqrt[4]{2}$ are conjugated over $\mathbb{Q}(\sqrt{2})$

Finally, over $\mathbb{Q}(\sqrt[4]{2})$ we have
$x^4-2 = (x-\sqrt[4]{2})(x+\sqrt[4]{2})(x^2+\sqrt{2}) \Rightarrow \pm i\sqrt[4]{2}$ are conjugated over $\mathbb{Q}(\sqrt[4]{2})$ but $\sqrt[4]{2}$ and $-\sqrt[4]{2}$ are not.

Suppose that we have two algebraic elements over K, say, α and β. Also, let

$\alpha=\alpha_1, \alpha_2, \dots, \alpha_m$
$\beta=\beta_1, \beta_2, \dots, \beta_n$ are conjugates of α & β

Can we find all conjugates of $\alpha+\beta$ or $\alpha\cdot\beta$, say? (we know that $\alpha+\beta$ and $\alpha\cdot\beta$ are algebraic over K).

In the first case consider the pol.

$$\prod_{i=1}^{n}\prod_{j=1}^{m}(x-\alpha_i-\beta_j) =: F_{\alpha+\beta}(x)$$

L. (follows from Vieta's formulae and the fundamental theorem of symmetric polynomials)

Let $(x-\alpha_1)\dots(x-\alpha_n)\in K[x]$ & $f(\bar{y}, x_1, \dots, x_n) \in K[\bar{y}, x_1, \dots, x_n]$ is symm. pol. in $x_1, \dots, x_n$. Then $f(\bar{y}, \alpha_1, \dots, \alpha_n) \in K[\bar{y}]$.

Thus by the lemma $F_{\alpha+\beta} \in K[x]$

(in particular we have proved that $\alpha+\beta$ is algebraic over K)

Exm $\alpha=\sqrt{2}$, $\beta=-\sqrt{2}$ $\Rightarrow$ $\alpha+\beta=0$ $\Rightarrow$ $F_{\alpha+\beta}$ is not minimal polynomial for $\alpha+\beta$.

Similarly, for $* \in \{+,-,\cdot,/\}$ conjugates of $\alpha * \beta$ are contained in $\alpha_i * \beta_j$.

Thm 2 Let α is algebraic over K and $\alpha=\alpha_1, \alpha_2, \dots, \alpha_n$ are algebraic conjugates of α over K. Then for any $f \in K[x]$ the algebraic conjugates of $f(\alpha)$ are exactly $f(\alpha_1), \dots, f(\alpha_n)$.

Pf. $f(\alpha) \in K[\alpha]$ and α is algebraic $\Rightarrow$ $f(\alpha)$ is algebraic over K (see the previous lecture).

Consider $\mu^K_{f(\alpha)}(f(x)) =: g(x)$ $\Rightarrow$ $g(\alpha)=0$ & $g \in K[x]$. Therefore, $\mu^K_\alpha \mid g$. In particular, all roots $\alpha_1, \dots, \alpha_n$ of μ^K_α are roots of g. Thus $f(\alpha_i)$ are algebraic conjugates of $f(\alpha)$. It remains to show that all conjugates of $f(\alpha)$ $\subseteq \{f(\alpha_1), \dots, f(\alpha_n)\}$ (this is a multi-set, in general, e.g. consider $f \equiv 1$)

Consider the polynomial:

$$(x - f(\alpha_1))(x - f(\alpha_2)) \dots (x - f(\alpha_n)) =: F(x)$$

The previous lemma shows that $F \in K[x]$.
Since $F(f(\alpha)) = 0$, it follows that $\mu^K_{f(\alpha)} \mid F$.
Thus all roots of $\mu^K_{f(\alpha)}$ are contained between the root of F (i.e. $f(\alpha_1), \dots, f(\alpha_n)$). ∎

Is it true that the number of conjugates of α is $\deg \mu_\alpha = \deg \alpha$? In other words, suppose that $\mu^K_\alpha(x) \stackrel{?}{=} (x-\alpha_1) \dots (x-\alpha_n)$ & $\alpha_j \in L$ (L is an extension of K). Is it true that $\alpha_i \neq \alpha_j$?

Consider $\gcd(\mu_\alpha, \mu_\alpha') = \begin{cases} \text{either } 1 \\ \text{or } \mu_\alpha \end{cases}$

$\deg \mu_\alpha' < \deg \mu_\alpha \Rightarrow \gcd(\mu_\alpha, \mu_\alpha') = 1 \Rightarrow \alpha_j$ are distincts

unfortunately, this is only true if the characteristic K is zero