3.6 Tutorial 2: NEW MAST30005 Semester 1: Last week's theorems

Last week we covered the following theorems. Write careful proofs of each.

Proposition 3.5. *Let $\mathbb{F}$ be a field and let $\overline{\mathbb{F}}$ be an algebraically closed field containing $\mathbb{F}$. Let $\alpha, \beta \in \overline{\mathbb{F}}$ and let $c \in \mathbb{F}$. Let $\alpha_1, \ldots, \alpha_r$ be the roots of $m_{\alpha,\mathbb{F}}(x)$ and let $\beta_1, \ldots, \beta_s$ be the roots of $m_{\beta,\mathbb{F}}(x)$ so that*

$$m_{\alpha,\mathbb{F}}(x) = (x-\alpha_1)\cdots(x-\alpha_r) \qquad \text{and} \qquad m_{\beta,\mathbb{F}}(x) = (x-\beta_1)\cdots(x-\beta_s) \qquad \text{in } \overline{\mathbb{F}}[x],$$

and $\alpha = \alpha_1$ and $\beta = \beta_1$. Assume that

$$c \notin \left\{ \frac{-(\beta-\beta_j)}{(\alpha-\alpha_i)} \mid i \in \{1,\ldots,r\}, j \in \{1,\ldots,s\} \text{ with } (i,j) \neq (1,1) \right\}.$$

then

$$\mathbb{F}(\alpha,\beta) = \mathbb{F}(\alpha + c\beta).$$

Theorem 3.6. *Let $\mathbb{F}$ be a field and let $\mathbb{K}$ be the splitting field of a polynomial $f(x) \in \mathbb{F}[x]$. Then there exists $\gamma \in \mathbb{K}$ such that*

$$\mathbb{K} = \mathbb{F}(\gamma).$$

Theorem 3.7. *(Classification of finite fields). The map*

$$\begin{array}{rccc} \mathbb{F}: & \{p^k \mid p,k \in \mathbb{Z}_{>0} \text{ and } p \text{ is prime}\} & \leftrightarrow & \{\text{finite fields}\} \\ & \mathrm{Card}(\mathbb{K}) & \longleftarrow & \mathbb{K} \\ & p & \longmapsto & \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \\ & p^k & \longmapsto & \mathbb{F}_{p^k} = \{\alpha \in \overline{\mathbb{F}_p} \mid \alpha^{p^k} = \alpha\} \end{array}$$

is a bijection.

(b) Let $n, d, m \in \mathbb{Z}_{>0}$ with $n = dm$. Then $\mathbb{F}_{p^n} \supseteq \mathbb{F}_{p^d}$ and

$$\mathrm{Aut}_{\mathbb{F}_{p^d}}(\mathbb{F}_{p^n}) = \{1, F^d, F^{2d}, \ldots, F^{(m-1)d}\}, \qquad \text{where} \qquad \begin{array}{rccc} F: & \overline{\mathbb{F}_p} & \to & \overline{\mathbb{F}_p} \\ & \alpha & \mapsto & \alpha^p \end{array}$$

is the Frobenius automorphism.

Theorem 3.8. *Let $n \in \mathbb{Z}_{>0}$. Let $\omega = e^{2\pi i/n}$ and let $\Phi_n(x)$ be the nth cyclotomic polynomial.*

(a) $\mathbb{Q}(\omega)$ is the splitting field of $f(x) = x^n - 1$ over $\mathbb{Q}$.

(b) $x^n - 1 = \prod_{d|n} \Phi_d(x)$.

(c) $\Phi_n(x) \in \mathbb{Z}[x]$ and $\Phi_n(x) = m_{\omega,\mathbb{Q}}(x)$.

(d) $\deg(\Phi_n(x)) = \mathrm{Card}((\mathbb{Z}/n\mathbb{Z})^\times) =$ (the number of primitive nth roots of unity).

(e) $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\omega)) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

Proposition 3.9. *The map given by*

$$\begin{array}{ccc} GL_2(\mathbb{C}) & \longrightarrow & \mathrm{Aut}_{\mathbb{C}}(\mathbb{C}(\epsilon)) \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} & \longmapsto & \sigma_{\substack{ab\\cd}} \end{array} \qquad \text{where} \qquad \begin{array}{rcc} \sigma_{\substack{ab\\cd}}: \mathbb{C}(\epsilon) & \longrightarrow & \mathbb{C}(\epsilon) \\ \frac{f(\epsilon)}{g(\epsilon)} & \longmapsto & \frac{f\left(\frac{a\epsilon+b}{c\epsilon+d}\right)}{g\left(\frac{a\epsilon+b}{c\epsilon+d}\right)} \end{array}$$

is a group homomorphism.

3.6.1 Small tasks for the proof of Proposition 3.5

HW: Show that $\mathbb{F}(\alpha + c\beta) \subseteq \mathbb{F}(\alpha, \beta)$.

HW: Show that $m_{\alpha,\mathbb{F}(\alpha+c\beta)}(x) = x - \alpha$.

HW: Show that $\alpha \in \mathbb{F}(\alpha + c\beta)$.

HW: Show that $m_{\beta,\mathbb{F}(\alpha+c\beta)}(x) = x - \beta$.

HW: Show that $\beta \in \mathbb{F}(\alpha + c\beta)$.

HW: Show that $\mathbb{F}(\alpha, \beta) \subseteq \mathbb{F}(\alpha + c\beta)$.

3.6.2 Small tasks for the proof of Proposition 3.6

Carefully set up the induction to use Proposition 3.5 to prove Proposition 3.6.

3.6.3 Small tasks for the proof of Proposition 3.7

HW: Let $\mathbb{K}$ be a finite field. Show that there exists $p \in \mathbb{Z}_{>0}$ such that p is prime and $\mathbb{F}_p$ is a subfield of $\mathbb{K}$.

HW: Let $\mathbb{K}$ be a finite field. Show that there exists $p, k \in \mathbb{Z}_{>0}$ such that p is prime and $\mathrm{Card}(\mathbb{K}) = p^k$.

HW: Let $\mathbb{K}$ be a finite field with q elements. Show that $\mathbb{K}^\times$ is an abelian group with $q - 1$ elements.

HW: Let G be a group with r elements. Show that if $g \in G$ then $g^r = 1$.

HW: Let $\mathbb{K}$ be a finite field with q elements. Show that if $\alpha \in \mathbb{K}$ and $\alpha \neq 0$ then $\alpha^{q-1} = 1$.

HW: Let $\mathbb{K}$ be a finite field with q elements. Show that if $\alpha \in \mathbb{K}$ then $\alpha^q = \alpha$.

HW: Let $\mathbb{K}$ be a finite field that contains $\mathbb{F}_p$ as a subfield. Show that the function

$$\begin{array}{rccc} F\colon & \mathbb{K} & \to & \mathbb{K} \\ & \alpha & \mapsto & \alpha^p \end{array} \quad \text{is an automorphism.}$$

3.6.4 Small tasks for the proof of Proposition 3.8

HW: Show that $\mathbb{Q}(\omega)$ is the splitting field of $x^n - 1$ over $\mathbb{Q}$.

HW: Show that $x^n - 1 = \prod_{d|n} \Phi_d(x)$.

HW: Show that $\Phi_n(x) \in \mathbb{Q}[x]$

HW: Show that $\Phi_n(x)$ divides $m_{\omega,\mathbb{Q}}(x)$.

HW: Show that $\Phi_n(x)$ divides $m_{\omega,\mathbb{Q}}(x)$.

HW: Let $\sigma \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\omega))$. Show that $\sigma(\omega)$ is a primitive nth root of unity.

HW: Show that $\deg(m_{\omega,\mathbb{Q}}(x)) =$ (the number of primitive nth roots of unity).

HW: Show that $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\omega)) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

3.6.5 Small tasks for the proof of Proposition 3.9

HW: Show that if $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{C})$ then $\sigma_{\substack{ab\\cd}} \in \mathrm{Aut}_{\mathbb{C}}(\mathbb{C}(\epsilon))$.

Proposition 3.10. *Let $\mathbb{F}$ be a field and let $\overline{\mathbb{F}}$ be an algebraically closed field containing $\mathbb{F}$. Let $\alpha, \beta \in \overline{\mathbb{F}}$ and let $c \in \mathbb{F}$. Let $\alpha_1, \ldots, \alpha_r$ be the roots of $m_{\alpha,\mathbb{F}}(x)$ and let $\beta_1, \ldots, \beta_s$ be the roots of $m_{\beta,\mathbb{F}}(x)$ so that*

$$m_{\alpha,\mathbb{F}}(x) = (x-\alpha_1)\cdots(x-\alpha_r) \qquad \textit{and} \qquad m_{\beta,\mathbb{F}}(x) = (x-\beta_1)\cdots(x-\beta_s) \qquad \textit{in } \overline{\mathbb{F}}[x],$$

and $\alpha = \alpha_1$ and $\beta = \beta_1$. Assume that

$$c \notin \left\{ \frac{-(\beta-\beta_j)}{(\alpha-\alpha_i)} \mid i \in \{1,\ldots,r\}, j \in \{1,\ldots,s\} \textit{ with } (i,j) \neq (1,1) \right\}.$$

then

$$\mathbb{F}(\alpha,\beta) = \mathbb{F}(\alpha + c\beta).$$

Proof.
To show: (a) $\mathbb{F}(\alpha + c\beta) \subseteq \mathbb{F}(\alpha,\beta)$.
(b) $\mathbb{F}(\alpha,\beta) \subseteq \mathbb{F}(\alpha + c\beta)$.

(a) To show: $\alpha + c\beta \in \mathbb{F}(\alpha,\beta)$.
Since $\alpha \in \mathbb{F}(\alpha,\beta)$ and $\beta \in \mathbb{F}(\alpha,\beta)$ and $c \in \mathbb{F}$ and $\mathbb{F}(\alpha,\beta)$ is a field then $\alpha + c\beta \in \mathbb{F}(\alpha,\beta)$.
So $\mathbb{F}(\alpha,\beta)$ is a field containing $\mathbb{F}$ and $\alpha + c\beta$.
Since $\mathbb{F}(\alpha + c\beta)$ is the smallest field containing $\mathbb{F}$ and $\alpha + c\beta$ then $\mathbb{F}(\alpha + c\beta) \subseteq \mathbb{F}(\alpha,\beta)$.

(b) To show: (ba) $\alpha \in \mathbb{F}(\alpha + c\beta)$
(bb) $\beta \in \mathbb{F}(\alpha + c\beta)$.

(ba) To show: $m_{\alpha,\mathbb{F}(\alpha+c\beta)}(x) = x - \alpha$.
Since

$$m_{\alpha,\mathbb{F}}(x) \in \mathbb{F}(\alpha,\beta)[x] \qquad \text{and} \qquad h(x) = m_{\beta,\mathbb{F}}(\beta + c\alpha - cx) \in \mathbb{F}(\alpha,\beta)[x]$$

and

$$m_{\alpha,\mathbb{F}}(\alpha) = 0, \qquad \text{and} \qquad h(\alpha) = 0,$$

then $m_{\alpha,\mathbb{F}(\alpha+c\beta)}(x)$ is a common divisor of $m_{\alpha,\mathbb{F}}(x)$ and $h(x) = m_{\beta,\mathbb{F}}(\beta + c\alpha - cx)$.
As elements of $\overline{\mathbb{F}}[x]$,

$$\begin{array}{rlc} m_{\alpha,\mathbb{F}}(x) \text{ factors as} & m_{\alpha\mathbb{F}}(x) = (x-\alpha)(x-\alpha_2)\ldots(x-\alpha_r) & \text{and} \\ h(x) \text{ factors as} & h(x) = (\beta + c\alpha - cx - \beta_1)\cdots(\beta + c\alpha - cx - \beta_s). & \end{array}$$

Since $c^{-1}\beta + \alpha - c^{-1}\beta_j \neq \alpha_i$ except when $i = 1$ and $j = 1$ then

$$\gcd(m_{\alpha,\mathbb{F}}(x), h(x)) = x - \alpha.$$

So $m_{\alpha,\mathbb{F}(\alpha+c\beta)}(x) = x - \alpha$.
So $\alpha \in \mathbb{F}(\alpha + c\beta)$. □

Theorem 3.11. *Let $\mathbb{F}$ be a field and let $\mathbb{K}$ be the splitting field of a polynomial $f(x) \in \mathbb{F}[x]$. Then there exists $\gamma \in \mathbb{F}$ such that*

$$\mathbb{K} = \mathbb{F}(\gamma).$$

Proof. Let $\alpha_1, \ldots, \alpha_k \in \mathbb{K}$ be the roots of $f(x)$ so that $f(x) = (x-\alpha_1)\cdots(x-\alpha_k)$ in $\mathbb{K}[x]$. Then

$$\mathbb{K} = \mathbb{F}(\alpha_1, \ldots, \alpha_k).$$

By induction on ℓ, the theorem of the primitive element gives that if $\ell \in \{1,\ldots,k\}$ then there exists $\gamma_\ell \in \mathbb{K}$ such that

$$\mathbb{F}(\alpha_1,\ldots,\alpha_\ell) = \mathbb{F}(\gamma_{\ell-1},\alpha_\ell) = \mathbb{F}(\gamma_\ell).$$

Let $\gamma = \gamma_k$. □

Theorem 3.12. *(Classification of finite fields). The map*

$$\begin{array}{cccc} \mathbb{F}\colon & \{p^k \mid p,k\in\mathbb{Z}_{>0},\ p \text{ is prime}\} & \leftrightarrow & \{\text{finite fields}\} \\ & \mathrm{Card}(\mathbb{K}) & \longleftarrow & \mathbb{K} \\ & p & \longmapsto & \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \\ & p^k & \longmapsto & \mathbb{F}_{p^k} = \{\alpha\in\overline{\mathbb{F}_p} \mid \alpha^{p^k}=\alpha\} \end{array}$$

Proof. Let $\mathbb{K}$ be a finite field.
Since $\mathbb{K}$ is finite then the ring homomorphism

$$\begin{array}{cccc} \varphi\colon & \mathbb{Z} & \to & \mathbb{K} \\ & 1 & \mapsto & 1 \end{array} \quad \text{is not injective.}$$

Let $p\in\mathbb{Z}_{>0}$ be minimal such that $\varphi(m)=0$.
If $q,r\in\mathbb{Z}_{>0}$ and $p=qr$ then $\varphi(q)\varphi(r)=\varphi(qr)=\varphi(p)=0$.
So $q=1$ and $r=p$ or vice versa and p is prime.
So $\{0,1,2,\ldots,p-1\}=\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z}$ is a subfield of $\mathbb{K}$.

So $\mathbb{K}$ is a finite dimensional $\mathbb{F}_p$-vector space.
So there exists $k\in\mathbb{Z}_{>0}$ such that $\dim_{\mathbb{F}_p}(\mathbb{K})=k$.
So $|\mathbb{K}|=p^k$.

Let $\alpha\in\mathbb{K}$ with $\alpha\neq 0$.
Since $\mathbb{K}^\times$ is an abeliangroup of order p^k-1 then $\alpha^{p^k-1}=1$.
So α is a root of $x^{p_k-1}-1$.
There are p^k-1 roots of $x^{p^k-1}-1$ (the (p^k-1)th roots of unity) and

$$\mathrm{Card}(\mathbb{K})=\mathrm{Card}(\mathbb{K}^\times\cup\{0\})=\mathrm{Card}(\mathbb{K}^\times)+\mathrm{Card}(\{0\})=(p^k-1)+1=p^k.$$

So

$$\mathbb{K}=\{\alpha\in\overline{\mathbb{F}_p} \mid \alpha^{p^k}=\alpha\}.$$

□

Theorem 3.13. *Let $n\in\mathbb{Z}_{>0}$. Let $\omega=e^{2\pi i/n}$ and let $\Phi_n(x)$ be the nth cyclotomic polynomial.*

(a) $\mathbb{Q}(\omega)$ *is the splitting field of* $f(x)=x^n-1$ *over* $\mathbb{Q}$.

(b) $x^n-1=\prod_{d|n}\Phi_d(x)$.

(c) $\Phi_n(x)\in\mathbb{Z}[x]$ *and* $\Phi_n(x)=m_{\omega,\mathbb{Q}}(x)$.

(d) $\deg(\Phi_n(x))=\mathrm{Card}((\mathbb{Z}/n\mathbb{Z})^\times)=($*the number of primitive nth roots of unity*$)$.

(e) $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\omega))\cong(\mathbb{Z}/n\mathbb{Z})^\times$.

Proposition 3.14. *The map given by*

$$\begin{array}{ccc} GL_2(\mathbb{C}) & \longrightarrow & \mathrm{Aut}_{\mathbb{C}}(\mathbb{C}(\epsilon)) \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} & \longmapsto & \sigma_{\substack{ab\\cd}} \end{array} \quad \text{where} \quad \begin{array}{ccc} \sigma_{\substack{ab\\cd}}\colon \mathbb{C}(\epsilon) & \longrightarrow & \mathbb{C}(\epsilon) \\ \frac{f(\epsilon)}{g(\epsilon)} & \longmapsto & \frac{f\left(\frac{a\epsilon+b}{c\epsilon+d}\right)}{g\left(\frac{a\epsilon+b}{c\epsilon+d}\right)} \end{array}$$

is a group homomorphism.