Galois theory - Problem Set 5

To be solved on Monday 17.04

Problem 1. Let $n \in \mathbb{Z}$, $n \geq 1$. Show that the following hold.

(a) For every $m \in \mathbb{Z}_n$ we have that the order of m is $o(m) = \frac{n}{\gcd(m,n)}$. In particular, $m \in \mathbb{Z}_n$ is a generator of $\mathbb{Z}_n$ if and only if $\gcd(m, n) = 1$.

(b) The number of generators of the cyclic group $\mathbb{Z}_n$ is $\phi(n)$.

(c) $n = \sum\limits_{d|n} \phi(d)$.

Problem 2. (Exam May 2013, Problem 1)

(a) Let E be the splitting field of $f(x) = x^{14} - 1$ over $\mathbb{Q}$. Show that the Galois group $G = \mathrm{Gal}(E/\mathbb{Q})$ is abelian.

(b) Let $\tilde{E}$ be the splitting field of $g(x) = x^7 + 1$ over $\mathbb{Q}$. Show that the Galois group $\tilde{G} = \mathrm{Gal}(\tilde{E}/\mathbb{Q})$ is abelian.

Problem 3. (Exam May 2004, Problem 3) Let p be a prime. Let E be the splitting field of $x^p - 1 \in \mathbb{Q}[x]$ over $\mathbb{Q}$.

(a) Prove that $\mathrm{Gal}(E/\mathbb{Q})$ is abelian of order $p - 1$.

(b) Let $\omega = e^{\frac{2\pi i}{31}}$. Prove that there exists a subfield F of $\mathbb{C}$ such that $[F(\omega) : F] = 5$.

Problem 4. (Exam May 2009, Problem 5.) Let $F \subseteq K$ be a Galois extension such that $G(K/F)$ is cyclic of order n and let σ be a generator for $G(K/F)$. Assume that F contains a primitive n-th root ω of unity. Let $\alpha \in K \setminus F$ and let $(\omega, \alpha) \neq 0$ be the Lagrange resolvent defined by

$$(\omega, \alpha) = \alpha + \omega\sigma(\alpha) + \cdots + \omega^{n-1}\sigma^{n-1}(\alpha).$$

(a) Show that $a = \alpha + \sigma(\alpha) + \cdots + \sigma^{n-1}(\alpha)$ is an element in F.

(b) Show that $K = F((\omega, \alpha))$.

(c) Let $b = (\omega, \alpha)^n$. Show that $b \in F$ and that K is the splitting field of $x^n - b \in F[x]$ over F.

(d) Give an argument why $x^n - b$ is an irreducible polynomial over F.

Problem 5. (Exam June 2014, Problem 2.) Let $F \subseteq E$ where $F = \mathrm{GF}(5^3)$ and $E = \mathrm{GF}(5^{24})$. Describe the Galois group $G = \mathrm{Gal}(E/F)$ and list the fields K such that $F \subseteq K \subseteq E$.

Problem 6. (Exercise 18.2.4 in the book.) Let E be a finite separable normal extension over F and let $G(E/F) = \{\sigma_1 = 1, \sigma_2, \ldots, \sigma_n\}$. If $\alpha \in E$ we define

$$T_{E/F}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha) \text{ and } N_{E/F}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$$

and call these respectively the *trace* and *norm* of α in E over F. Show:

(a) $T_{E/F}(\alpha) \in F$, $N_{E/F}(\alpha) \in F$.

(b) $T_{E/F}$ is an F-linear map of the vector space E over F.

(c) $N_{E/F}$ is a group homomorphism from the group $E^* = E \setminus \{0\}$ to the group $F^* = F \setminus \{0\}$.

(d) If $G(E/F)$ is a cyclic group generated by σ, then $N_{E/F}(\alpha) = 1$ if and only if there exists $b \in E$ such that $\alpha = (\sigma(b))^{-1}b$. (*Hint*: Generalize Lemma 2.4 (Lemma 15.3 in our notes).)

Problem 7. (Exam June 2014, Problem 4.)

(a) Let $F \subseteq F(\theta)$ and $F \subseteq F(\gamma)$ be two Galois extensions of the field F, where $\mathrm{char}(F) = 0$. Show that $F \subseteq F(\theta, \gamma)$ is a Galois extension of F.

(b) Assume $\mathrm{Gal}(F(\theta)/F)$ and $\mathrm{Gal}(F(\gamma)/F)$ are both abelian groups. Show that $\mathrm{Gal}(F(\theta,\gamma)/F))$ is an abelian group.

Problem 8. (Exercise 18.2.3 in the book.) Let p be a prime and let F be a field. Prove that $x^p - b \in F[x]$ is reducible if and only if its splitting field is F or $F(\omega)$ according to whether $\mathrm{char}(F) = p$ or $\mathrm{char}(F) \neq p$, where ω is a primitive p-th root of unity.

Extra problems

The following problems may be a bit more challenging, in case you feel like you need something more.

Problem 9. (a) Show that for every $n \in \mathbb{Z}$, $n \geq 1$ we have

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

where $\Phi_d(x)$ is the d-th cyclotomic polynomial. Conclude that the constant term of $\Phi_n(x)$ is ± 1.

(b) Let $n \in \mathbb{Z}$, $n \geq 1$. Let $p \geq 2$. Show that if $p \mid \Phi_n(\alpha)$, then $p \nmid \alpha$.

(c) Let $n \in \mathbb{Z}$, $n \geq 1$. Let $\alpha \in \mathbb{Z}$ and let p be a prime such that $\gcd(p, n) = 1$. Show that p divides $\Phi_n(\alpha)$ if and only if the order of $\overline{\alpha} \in \mathbb{Z}_p^\times$ is n.

(d) (Special case of Dirichlet's theorem) Show that for any $n \geq 1$ there are infinitely many prime numbers p such that $n \mid (p-1)$.

(e) Let G be a finite abelian group. Show that there exists a Galois extension E of $\mathbb{Q}$ such that $\mathrm{Gal}(E/\mathbb{Q}) \cong G$.

Problem 10. Let $F \subseteq E$ be a Galois extension with Galois group G. As in Problem 6, for any $\alpha \in E$ define the norm of α in E over F via

$$N_{E/F}(\alpha) = \prod_{\sigma \in G} \sigma(\alpha).$$

(a) Find $n \in \mathbb{Z}$ such that $i \in \mathbb{Q}(\omega)$, where $\omega \in \mathbb{C}$ is a primitive n-th root of unity.

(b) Show that $\sqrt{2} \in \mathbb{Q}(\omega)$ where $\omega \in \mathbb{C}$ is a primitive 8-th root of unity.

(c) Let $p \geq 3$ be a prime number. Let $\omega \in \mathbb{C}$ be a primitive p-th root of unity.

  (i) Show that $N_{\mathbb{Q}(\omega)/\mathbb{Q}}(-1) = 1$, $N_{\mathbb{Q}(\omega)/\mathbb{Q}}(p) = p^{p-1}$, $N_{\mathbb{Q}(\omega)/\mathbb{Q}}(\omega) = 1$ and $N_{\mathbb{Q}(\omega)/\mathbb{Q}}(1-\omega) = p$.

  (ii) Show that $N_{\mathbb{Q}(\omega)/\mathbb{Q}}(\Phi_p'(\omega)) = p^{p-2}$.

  (iii) Show that the *discriminant* $\Delta := \prod_{1 \leq i < j \leq p-1} (\omega^i - \omega^j)^2$ satisfies $\Delta = (-1)^{\frac{p-1}{2}} p^{p-2}$.

  (iv) Show that if $p \equiv 1 \mod 4$, then $\sqrt{p} \in \mathbb{Q}(\omega)$, while if $p \equiv 3 \mod 4$, then $i\sqrt{p} \in \mathbb{Q}(\omega)$.

(d) Let $n, m \geq 1$. Let $\omega_n \in \mathbb{C}$ be a primitive n-th root of unity and $\omega_m \in \mathbb{C}$ be a primitive m-th root of unity. Let $l = \mathrm{lcm}(n, m)$ and let $\omega_l \in \mathbb{C}$ be a primitive l-th root of unity. Show that $\mathbb{Q}(\omega_n, \omega_m) = \mathbb{Q}(\omega_l)$.

(e) Let $k \in \mathbb{Z}$ be an integer. Show that there exists an $n \in \mathbb{Z}$, $n \geq 1$ such that $\sqrt{k} \in \mathbb{Q}(\omega_n)$ where ω_n is a primitive n-th root of unity.