MATH 7752 Homework 11

James Harbour

April 28, 2022

Problem 1

In this problem you will need the following two definitions.

Definition 1: Let L/F be a finite separable extension and let $\overline{F}$ be an algebraic closure of F containing L. A subfield L' of $\overline{F}$ is called **conjugate to** L **over** F if $L' = \sigma(L)$ for some F-embedding $\sigma : L \to \overline{F}$. (Note: L/F is Galois if and only if the only conjugate to L over F is itself.)

Definition 2: A finite extension K/F is called a p**-extension** if K/F is **Galois** and $\mathrm{Gal}(K/F)$ is a p-group.

1. Let L/F be a separable extension of degree n and let K be the Galois closure of L over F. Prove that K can be written as a compositum $L_1 L_2 \cdots L_n$, where $L_1, \ldots, L_n$ are (not necessarily distinct) conjugates of L over F.
2. Let K/F and L/F be finite p-extensions. Prove that KL/F is also a p-extension.
3. Suppose that K/L and L/F are both p-extensions, and let M be the Galois closure of K over F (note: we do not know whether K/F is Galois or not). Prove that M/F is also a p-extension.
4. Now assume only that L/F is a separable extension with $[L : F] = p^r$, for some $r \geq 1$. Let M be the Galois closure of L over F. Prove that $[M : F]$ need not be a power of p.

Problem 2

Let $f(x)$ and $g(x)$ be irreducible polynomials in $\mathbb{F}_p[x]$ of the same degree. Let $F = \mathbb{F}_p[x]/(f(x))$. Prove that $g(x)$ splits completely over F.

Proof. By a vector space counting argument, $|F| = p^n$. By uniqueness of splitting fields, F is $\mathbb{F}_p$-isomorphic to $\mathbb{F}_{p^n}$ which is $\mathbb{F}_p$-isomorphic to $\mathbb{F}_p[x]/(q(x))$ which contains a root of $q(x)$. Thus, F contains a root of $q(x)$ whence by normality of the extensions $F/\mathbb{F}_p$, $q(x)$ splits over F. $\square$

Problem 3

Consider the polynomial $f(x) = x^4 - 2x^2 - 5 \in \mathbb{Q}[x]$.

(a): Determine the Galois group G of the splitting field K of $f(x)$ over $\mathbb{Q}$.

Proof. Let $\alpha = \sqrt{1+\sqrt{6}}$ and $\beta = \sqrt{1-\sqrt{6}}$. Then $f(x) = (x-\alpha)(x+\alpha)(x-\beta)(x+\beta)$ and $K = \mathbb{Q}(\alpha, \beta)$. Noting that $\alpha^2 + \beta^2 = 2$, it follows that $\mu_{\beta,\mathbb{Q}(\alpha)} = x^2 + (\alpha^2 - 2)$ and thus $[K : \mathbb{Q}(\alpha)] = 2$. Note that $f(x)$ is irreducible as none of the choices of pairs of linear factors provide a polynomial in $\mathbb{Q}[x]$ by appealing to Vieta's formulae and the fact that $\alpha^2, \beta^2, \alpha \pm \beta \notin \mathbb{Q}$.
Thus $\mathbb{G}$ is an order 8 subgroup of S_4, whence its isomorphism class is D_8. $\square$

(b): Find all subgroups of G and their corresponding fixed fields. Which of those are normal extensions of $\mathbb{Q}$?

Problem 4

Let p and q be distinct primes with $q > p$, and let K/F be a Galois extension of degree pq. Prove the following:

(a): There exists a field L with $F \subset L \subset K$ and $[L : F] = q$.

Proof. Let $G = \mathrm{Gal}(K/F)$. Then $|G| = pq$, whence by Sylow's existence theorem there is some subgroup $H \subseteq G$ such that $|H| = p$. Setting $L = K^H$, by the fundamental theorem of Galois theory, $p = |H| = [K : K^H]$ whence $[K^H : F] = q$ as desired. $\square$

(b): There exists a **unique** field M with $F \subset M \subset K$ and $[M : F] = p$.

Proof. Let $G = \mathrm{Gal}(K/F)$. Let n_q denote the number of Sylow q-subgroups of G. Then as $n_q \mid p$ and $n_q \equiv 1 mod\ q$, the restriction that $q > p$ forces $n_q = 1$. Thus there is a unique subgroup of Q of G of order q, whence by the fundamental theorem of Galois theory there is a unique intermediate subfield $M = K^Q$ of K/F with $[K : M] = q$ or equivalently $[M : F] = p$ $\square$

Problem 5

Prove the following analogue of Kümmer's theorem for abelian extensions: Let $n \in \mathbb{N}$ and let F be a field containing a primitive n^{th} root of unity.

(a): Let K/F be a finite Galois extension such that $G = \mathrm{Gal}(K/F)$ is abelian of exponent n. Then there exists $a_1, \ldots, a_t \in F$ such that $K = F(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_t})$. More precisely, there exists $\alpha_1, \ldots, \alpha_t \in K$ such that $K = F(\alpha_1, \ldots, \alpha_t)$ and $\alpha_i^n \in F$ for all i.

Proof. Write $G \cong C_{n_1} \times \cdots C_{n_t}$ where $n_i \in \mathbb{N}$ and $C_{n_i} = \mathbb{Z}/n_i\mathbb{Z}$. For $j \in \{1, \ldots, t\}$, set $G_j = \prod_{i \neq j} C_{n_i}$ and $K_j = K^{G_j}$. As $G_j \lhd G$, it follows that K_j/F is Galois and $\mathrm{Gal}(K_j/F) \cong \mathrm{Gal}(K/F)/\mathrm{Gal}(K/K_j) = G/G_j \cong C_{n_j}$. Hence, by Kümmer's theorem, there exists some $\alpha_j \in K_j$ such that $K_j = F(\alpha_j)$ and $\alpha_j^{n_j} \in F$, whence $\alpha_j^n = (\alpha_j^{n_j})^{n/n_j} \in F$.

Observe that

$$K = K^{\{e\}} = K^{\bigcap_{i=1}^t G_i} = K_1 K_2 \cdots K_t = F(\alpha_1, \alpha_2, \cdots, \alpha_t).$$

$\square$

(b): Conversely, suppose that $K = F(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_t})$ for some $a_1, \ldots, a_t \in F$. Prove that K/F is Galois and $G = \mathrm{Gal}(K/F)$ is abelian of exponent n. **Hint:** For part (b) use one of the problems from the previous homework.

Proof. Write $\alpha_i = \sqrt[n]{a_i}$, so $\alpha_i^n = a_i$. As F contains a primitive n^{th} root of unity, Kümmer's theorem implies that each $F(\alpha_i)/F$ is Galois with $\mathrm{Gal}(F(\alpha_i)/F) \cong \mathbb{Z}/n_i\mathbb{Z}$ for some $n_i \mid n$. $\square$

Problem 6

Let F be a field containing a primitive n^{th} root of unity. Let $a, b \in F$ be such that the polynomials $f(x) = x^n - a$, and $g(x) = x^n - b$ are both irreducible over F. Consider the Kümmer extensions $F(\alpha)$, $F(\beta)$, where α is a root of $f(x)$ and β is a root of $g(x)$. Prove that $F(\alpha) = F(\beta)$ if and only if $\beta = c\alpha^r$, for some $c \in F$ and some integer r which is coprime to n (equivalently, if and only if $b = c^n a^r$, for some $c \in F$ and some $(r, n) = 1$).