Abstract Algebra Homework 10

Michael Nelson

Problem 1

Proposition 0.1. *Let F/K be a finite field extension of degree n. Suppose K has characteristic $p > 0$ and p does not divide n. Then F is separable over K.*

Proof. Assume for a contradiction that F/K is inseparable. Choose $\alpha \in F$ such that α is inseparable over K. Then the minimal polynomial of α over K must have the form

$$\pi_{\alpha,K}(X) = X^{pm} + a_{m-1}X^{p(m-1)} + \cdots + a_1X^p + a_0,$$

where $a_0, a_1, \ldots, a_{m-1} \in K$ and $d > 0$. Here we are using the fact that an irreducible polynomial over a field is separable if and only if its derivative is not equal zero (if you need to see a proof of this, then please see the Appendix problem 1.a). In particular, $[K(\alpha) : K] = pm$. But this implies $p \mid n$ since

$$\begin{aligned} n &= [F : K] \\ &= [F : K(\alpha)][K(\alpha) : K] \\ &= [F : K(\alpha)]pm. \end{aligned}$$

This is a contradiction. □

Proposition 0.2. *Let F/K be a field extension and suppose K has characteristic $p > 0$. Let $\alpha \in F$ be algebraic over K. The α is separable if and only if $K(\alpha) = K(\alpha^{p^n})$ for all $n \geq 1$.*

Proof. Suppose α is separable. Then since $K(\alpha)/K$ is a separable extension. This implies $K(\alpha)/K(\alpha^p)$ is a separable extension (if you need to see a proof of this, then please see the Appendix problem 1.b). Let $\pi(X)$ be the minimal polynomial of α over $K(\alpha^p)$. Observe that α is a root of the polynomial $X^p - \alpha^p = (X - \alpha)^p$ over $K(\alpha^p)$. This implies $\pi(X) \mid (X - \alpha)^p$ which implies $\pi(X) \mid (X - \alpha)$ since π is irreducible. Thus $\pi(X) = X - \alpha$ which implies $[K(\alpha) : K(\alpha^p)] = 1$ and hence $K(\alpha) = K(\alpha^p)$. Since α^p is also separable over K, we can proceed by induction and obtain

$$\begin{aligned} K(\alpha) &= K(\alpha^p) \\ &= K(\alpha^{p^2}) \\ &\vdots \\ &= K(\alpha^{p^n}) \end{aligned}$$

for all $n \geq 1$.

Conversely, suppose $K(\alpha) = K(\alpha^{p^n})$ for all $n \geq 1$ and assume for a contradiction that α is not separable. Then the minimal polynomial of α over K must have the form

$$\pi_{\alpha,K}(X) = X^{pm} + a_{m-1}X^{p(m-1)} + \cdots + a_1X^p + a_0.$$

Observe that α^p is a root of the monic polynomial

$$\pi_{\alpha,K}(X^{1/p}) = X^m + a_{m-1}X^{(m-1)} + \cdots + a_1X + a_0.$$

In fact, $\pi_{\alpha,K}(X^{1/p})$ is irreducible since $\pi_{\alpha,K}(X)$ is irreducible (if $\pi_{\alpha,K}(X^{1/p}) = fg$ with $\deg f, \deg g < \deg \pi_{\alpha,K}(X^{1/p})$ then $\pi_{\alpha,K} = f(X^p)g(X^p)$). Thus $\pi_{\alpha,K}(X^{1/p})$ is the minimal polynomial of α^p. In particular, this implies

$$\begin{aligned} [K(\alpha) : K] &= pm \\ &> m \\ &\geq [K(\alpha^p) : K] \\ &= [K(\alpha) : K], \end{aligned}$$

which is a contradiction. □

Problem 2

Problem 2.a

Proposition 0.3. *Let K be a finite field and let F be an algebraic closure of K. Then $\mathrm{Gal}(F/K)$ is abelian.*

Proof. Let $\sigma, \tau \in \mathrm{Gal}(F/K)$ and suppose $\sigma\tau \neq \tau\sigma$. Choose $\alpha \in F$ such that $\sigma\tau(\alpha) \neq \tau\sigma(\alpha)$. Let E/K be a finite Galois extension such that $\alpha \in E$. Then $\sigma|_E\tau|_E \neq \tau|_E\sigma|_E$ since $\sigma\tau(\alpha) \neq \tau\sigma(\alpha)$. This is a contradiction since every finite Galois extension over K is cyclic (and in particular abelian). □

Problem 2.b

Proposition 0.4. *Let K be a finite field, let F be an algebraic closure of K, and let $\sigma \in \mathrm{Gal}(F/K)\backslash\{1\}$. Then σ has infinite order.*

Proof. Assume for a contradiction that σ has finite order, say $\mathrm{ord}(\sigma) = m$. Choose an element $\alpha \in F$ such that $\sigma(\alpha) \neq \alpha$ (this is possible since $\sigma \neq 1$). Also, choose a positive integer n which relatively prime to m and choose a finite field extension L/F of degree $[L : F] = n$ such that $\alpha \in L$. Note that L/F is necessarily a Galois extension (by classification theorem of finite fields) with Galois group $\mathrm{Gal}(L/F) \cong \mathbb{Z}/n\mathbb{Z}$. Define $\rho_L : \mathrm{Gal}(F/K) \to \mathrm{Gal}(L/K)$ to be the restriction map, given by

$$\rho_L(\tau) = \tau|_L$$

for all $\tau \in \mathrm{Gal}(F/K)$. Then ρ_L is clearly a homomorphism of groups, and so in particular, $\mathrm{ord}(\rho_L(\sigma)) \mid m$. Since $\mathrm{Gal}(L/K)$ is cyclic of order n (which is relatively prime to m), we see that $\mathrm{ord}(\rho_L(\sigma)) = 1$. But $\alpha \in L$ and

$$\begin{aligned}\alpha &\neq \sigma(\alpha)\\ &= \sigma|_L(\alpha)\\ &= \rho_L(\sigma)(\alpha).\end{aligned}$$

Thus $\rho_L(\sigma)$ cannot have order 1, which is a contradiction. □

Problem 3

Proposition 0.5. *Let F be an extension of K and $\alpha, \beta \in F$ such that α is separable over K and β is totally inseparable over K. Then $K(\alpha + \beta) = K(\alpha, \beta)$. Moreover, if both α and β are nonzero, then $K(\alpha, \beta) = K(\alpha\beta)$.*

Proof. First we show $K(\alpha + \beta) = K(\alpha, \beta)$. The direction $K(\alpha + \beta) \subseteq K(\alpha, \beta)$ is clear, so it suffices to show $K(\alpha + \beta) \supseteq K(\alpha, \beta)$. To do this, we just need to show that $\alpha, \beta \in K(\alpha + \beta)$. We may assume $\mathrm{char}\, K = p$. Since β is totally inseparable over K, we have $\beta^{p^m} = b$ for some $m \geq 0$ and $b \in K$. Observe that

$$\begin{aligned}\alpha^{p^m} &= ((\alpha + \beta) - \beta)^{p^m}\\ &= (\alpha + \beta)^{p^m} - b\\ &\in K(\alpha + \beta).\end{aligned}$$

Therefore the element α is purely inseparable over $K(\alpha + \beta)$; but since α is separable over K, then α is also separable over $K(\alpha + \beta)$. Thus $\alpha \in K(\alpha + \beta)$, which implies $\beta = (\alpha + \beta) - \alpha \in K(\alpha + \beta)$.

Now suppose $\alpha \neq 0 \neq \beta$. We will show $K(\alpha\beta) = K(\alpha, \beta)$. The direction $K(\alpha\beta) \subseteq K(\alpha, \beta)$ is clear, so it suffices to show $K(\alpha\beta) \supseteq K(\alpha, \beta)$. To do this, we just need to show that $\alpha, \beta \in K(\alpha\beta)$. Observe that

$$\begin{aligned}\alpha^{p^m} &= (\alpha\beta\beta^{-1})^{p^m}\\ &= (\alpha\beta)^{p^m} b^{-1}\\ &\in K(\alpha\beta).\end{aligned}$$

Therefore the element α is purely inseparable over $K(\alpha\beta)$; but since α is separable over K, then α is also separable over $K(\alpha\beta)$. Thus $\alpha \in K(\alpha\beta)$, which implies $\beta = \alpha\beta\alpha^{-1} \in K(\alpha\beta)$. □

Appendix

Problem 1.a

Proposition 0.6. *Let K be a field and let $\pi(X)$ be an irreducible polynomial in $K[X]$. Then $\pi(X)$ is separable over K if and only if $\pi'(X) \neq 0$. In particular, when K has characteristic p, then $\pi(X)$ is separable if and only if it is not a polynomial in X^p.*

Proof. Separability is equivalent to $\gcd(\pi(X), \pi'(X)) = 1$. If $\pi(X)$ and $\pi'(X)$ are not relatively prime, then $\pi(X) \mid \pi'(X)$ since $\pi(X)$ is irreducible. Taking the derivative drops degrees, so having $\pi'(X)$ being divisible by $\pi(X)$ forces $\pi'(X) = 0$. Conversely, if $\pi'(X) = 0$, then $\gcd(\pi(X), \pi'(X)) = \pi(X)$ is nonconstant, so $\pi(X)$ is inseparable. Thus separability of $\pi(X)$ is equivalent to $\pi'(X) \neq 0$.

When K has characteristic 0, every irreducible over K has nonzero derivative since any nonconstant polynomial has nonzero derivative. So all irreducibles over K are separable.

Now suppose K has characteristic p. Writing

$$\pi(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 T + a_0,$$

the condition $\pi'(X) = 0$ means $ia_i = 0$ in K for $0 \leq i \leq n$. This implies $p \mid i$ whenever $a_i \neq 0$, so the only nonzero terms in $\pi(X)$ occur in degrees divisible by p. In particular, $n = \deg \pi$ is a multiple of p, say $n = pm$. Write each exponent of a nonzero term in $\pi(X)$ as a multiple of p:

$$\pi(X) = X^{pm} + a_{p(m-1)}X^{p(m-1)} + \cdots + a_p X^p + a_0 = g(X^p)$$

where $g(X) \in K[X]$. So $\pi(X) \in K[X^p]$. Conversely, if $\pi(X) = g(X^p)$ is a polynomial in X^p, then $\pi'(X) = g'(X^p)pX^{p-1} = 0$, so $\pi(X)$ is inseparable in $K[X]$. □

Problem 1.b

Proposition 0.7. *Let $F \subseteq K \subseteq L$ be an extension of fields. Suppose L/F is a separable extension. Then L/K is a separable extension.*

Proof. Let $\alpha \in L$, let $\pi_{\alpha,K}(X)$ be the minimal polynomial of α over K, and let $\pi_{\alpha,F}(X)$ be the minimal polynomial of α over F. Then $\pi_{\alpha,K} \mid \pi_{\alpha,F}$ in $K[X]$, so

$$\pi_{\alpha,K}(X)g(X) = \pi_{\alpha,F}(X) \tag{1}$$

for some $g(X) \in K[X]$. Now differentiate both sides of (1) and set $X = \alpha$ to get

$$\pi'_{\alpha,K}(\alpha)g(\alpha) = \pi'_{\alpha,F}(\alpha).$$

Observe that $\pi'_{\alpha,F}(\alpha) \neq 0$ since this would imply $\pi_{\alpha,F} \mid \pi'_{\alpha,F}$ would contradict separability of α over F. Similarly $g(\alpha) \neq 0$ since this would imply $\pi_{\alpha,K} \mid g$ which would imply $\pi^2_{\alpha,K} \mid \pi_{\alpha,F}$ which would again contradict separability of α over F. Thus we have $\pi'_{\alpha,K}(\alpha) \neq 0$. In particular $\pi'_{\alpha,K}(X) \neq 0$, which implies α is separable over K. □

Problem 3

Proposition 0.8. *Let K be a field and let K^{sep} be a separable closure of K. We define a preordered set $(\mathcal{G}_{K^{\text{sep}}/K}, \subseteq_K)$ as follows: the underlying set is defined to be*

$$\mathcal{G}_{K^{\text{sep}}/K} = \{L/K \mid L/K \text{ is finite Galois extension such that } K \subseteq L \subseteq K^{\text{sep}}\}.$$

If K^{sep} and K are understood, then we simply write $\mathcal{G}$ instead of $\mathcal{G}_{K^{\text{sep}}/K}$. The preorder $\subseteq_K$ is set inclusion: we shall write write $L \subseteq_K L'$ as shorthand for saying $K \subseteq L \subseteq L' \subseteq K^{\text{sep}}$ with L/K and L'/K Galois. Finally, for each $L \subseteq_K L'$, we define $\rho_{L,L'} \colon \text{Gal}(L'/K) \to \text{Gal}(L/K)$ to be the restriction map:

$$\rho_{L,L'}(\sigma) = \sigma|_L$$

for all $\sigma \in \text{Gal}(L'/K)$. With this terminology fixed, let $(\text{Gal}(L/K), \rho_{L,L'})$ be an inverse system indexed over $(\mathcal{G}, \subseteq_K)$. Then

$$\text{Gal}(K^{\text{sep}}/K) \cong \varprojlim \text{Gal}(L/K).$$

Proof. We define $\Psi : \mathrm{Gal}(K^{\mathrm{sep}}/K) \to \varprojlim \mathrm{Gal}(L/K)$ by

$$\Psi(\sigma) = (\sigma|_L)_{\mathcal{G}}$$

for all $\sigma \in \mathrm{Gal}(K^{\mathrm{sep}}/K)$. It's easy to see that the collection $(\sigma|_L)_{\mathcal{G}}$ really is an element of $\varprojlim \mathrm{Gal}(L/K)$. Indeed, if $L \subseteq_K L'$, then $\rho_{L,L'}(\sigma|_{L'}) = \sigma|_L$. It's also easy to see that Ψ is a group homomorphism: if $\sigma, \tau \in \mathrm{Gal}(K^{\mathrm{sep}}/K)$, then

$$\begin{aligned}\Psi(\sigma\tau) &= ((\sigma\tau)|_L)_{\mathcal{G}} \\ &= (\sigma|_L \tau|_L)_{\mathcal{G}} \\ &= (\sigma|_L)_{\mathcal{G}}(\tau|_L)_{\mathcal{G}} \\ &= \Psi(\sigma)\Psi(\tau).\end{aligned}$$

Let us check that Ψ is injective. Suppose $\sigma \in \mathrm{Gal}(K^{\mathrm{sep}}/K)$ and $\sigma|_L = 1|_L$ for all $L \in \mathcal{G}$. To see that σ is the identity, we assume for a contradiction that $\sigma \neq 1$. Choose $\alpha \in \overline{K}$ such that $\sigma(\alpha) \neq \alpha$ (such an α must exist since $\sigma \neq 1$). Then α must be contained in some finite Galois extension, say L/K, but $\sigma|_L = 1|_L$, which contradicts the fact that $\sigma(\alpha) \neq \alpha$. Thus Ψ is injective.

Now let us check that Ψ is surjective. Let $(\sigma_L)_{\mathcal{G}}$ be an element in $\varprojlim \mathrm{Gal}(L/K)$. We *define* $\sigma \colon K^{\mathrm{sep}} \to K^{\mathrm{sep}}$ as follows: for any $\alpha \in K^{\mathrm{sep}}$, we choose a finite Galois extension L/K such that $\alpha \in L$. Then we set

$$\sigma(\alpha) = \sigma_L(\alpha). \tag{2}$$

We must check that (2) is well-defined. Suppose L'/K is another finite Galois extension such that $\alpha \in L'$. Then $L \cap L'/K$ is a finite Galois extension with $\alpha \in L \cap L'$, and moreover we have

$$\begin{aligned}\sigma_{L'}(\alpha) &= \sigma_{L'}(\alpha)|_{L\cap L'} \\ &= \sigma_{L\cap L'}(\alpha) \\ &= \sigma_L(\alpha)|_{L\cap L'} \\ &= \sigma_L(\alpha).\end{aligned}$$

Thus (2) is well-defined. □

Corollary 1. *Let F be a finite and let $\overline{F}$ be a choice of an algebraic closure of F. Then*

$$\mathrm{Gal}(\overline{F}/F) \cong \varprojlim_n (\mathbb{Z}/n\mathbb{Z}) \cong \prod_p \mathbb{Z}_p.$$

Proof. First note that since F is a finite field (and hence perfect), our choice of an algebraic closure of F is also a separable closure of F. By the classification result for finite fields, there exists a prime p and a positive integer k such that $F \cong \mathbb{F}_q$ where $q = p^k$. Let $\sigma \colon F \to \mathbb{F}_q$ denote this isomorphism. We can extend σ to an isomorphism $\widetilde{\sigma} \colon \overline{F} \to \mathbb{F}_{q^\infty}$ which restrict to $\sigma \colon F \to \mathbb{F}_q$. Then observe that

$$\mathrm{Gal}(\mathbb{F}_{q^\infty}/\mathbb{F}_q) = \widetilde{\sigma}\mathrm{Gal}(\overline{F}/F)\widetilde{\sigma}^{-1}.$$

So it suffices to show that

$$\mathrm{Gal}(\mathbb{F}_{q^\infty}/\mathbb{F}_q) \cong \varprojlim_n (\mathbb{Z}/n\mathbb{Z}) \cong \prod_p \mathbb{Z}_p.$$

Now the isomorphism on left holds since every every $L \in \mathcal{G}_{\mathbb{F}_{q^\infty}/\mathbb{F}_q}$ has the form $L = \mathbb{F}_{q^n}$ where $n \geq 1$ and moreover, $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z}$. The isomorphism on the right holds because the Chinese Remainder Theorem and the fact inverse limits commute with finite products:

$$\begin{aligned}\varprojlim_n (\mathbb{Z}/n\mathbb{Z}) &\cong \varprojlim_{n=p_1^{e_1}\cdots p_k^{e_k}} (\mathbb{Z}/p_1^{e_1}\cdots p_k^{e_K}\mathbb{Z}) \\ &\cong \varprojlim_{n=p_1^{e_1}\cdots p_k^{e_k}} (\mathbb{Z}/(p_1^{e_1}\mathbb{Z}) \times \cdots\cdots \mathbb{Z}/(p_k^{e_K}\mathbb{Z})) \\ &\cong \varprojlim_{p_1^{e_k}} (\mathbb{Z}/(p_1^{e_1}\mathbb{Z})) \times \cdots\cdots \varprojlim_{p_1^{e_k}} (\mathbb{Z}/(p_k^{e_K}\mathbb{Z})) \\ &\cong \prod_p \mathbb{Z}_p\end{aligned}$$

□