Math 210B Algebra: Homework 2

Jan 30th, 2019

Professor Sharifi

Anish Chedalavada

Exercise 1. *Let p be an odd prime dividing $\Phi_n(a)$ for some $a \in \mathbb{Z}$. Show that either $p \mid n$ or $p \equiv 1 \bmod n$.*

Proof. We may assume $a \neq 0$. If $p \mid \Phi_n(a)$ then $p \mid (a^n - 1)$. If $n < p$ then $n \mid (p-1)$, as $a^n \equiv 1 \mod p$, and a must have order $p-1$ in $\mathbb{Z}/p\mathbb{Z}^\times$. Suppose the order of $\overline{a} \in \mathbb{Z}/p\mathbb{Z}^\times$ is $e \leq (p-1) < n$. We have that $p \mid \Phi_e(a)$, (as $p \mid a^e - 1$, so $p \mid \prod_{d|e} \Phi_d(a)$, and if it divides $\Phi_d(a)$ for $d < e$ then it divides $a^d - 1$, contradiciting that e was the order of $a \mod p$. Thus, a is a root of $\Phi_e, \Phi_n \mod p$, which in $\mathbb{Z}[t]$are relatively prime polynomials dividing $t^n - 1 \in \mathbb{Z}[t]$. Consider the canonical surjection $\mathbb{Z}[t] \to \mathbb{Z}/p\mathbb{Z}[t]$, We have that the images of both of these polynomials must divide $t^n - 1 + (p) \equiv t^n - 1 \mod (p)$, and thus $t^n - 1$ has multiple roots, which is only possible if $t^n - 1$ and nt^{n-1} are not relatively prime. Assuming $\overline{n}$ is invertible in $\mathbb{Z}/p\mathbb{Z}$, clearly, $t^n - 1 - \bar{n}^{-1}t(\overline{n}t^{n-1}) = -1$, a contradiction. Thus, $\overline{n}$ cannot be invertible $\implies p \mid n$. □

Exercise 2 (Problem 2)**.**

Proof. a) Suppose α is transcendental over $F(S)$. It is clear that α does not satisfy any polynomial in $F(S)[t]$: in particular, there does not exist a polynomial $f \in F[t_1, ..., t_n]$ for any arbitrary n s.t. $f(\alpha, s_1, ..., s_{n-1}) = 0$ for any $s_1, ..., s_{n-1} \in S$ for if there did then we may view this as a polynomial in $F(S)[t]$ for which α is a root. The converse is also clear from this logic, as if $S \cup \alpha$ is F-algebraically independent then there is no polynomial in $F(S)[t]$ for which α is a root: else for some supposed f we may view this as some polynomial $\overline{f} \in F[t_1, ..., t_n]$ for every s_1 that appears in f, which is zero under evaluation at each s_i in f and α.
b) The forward direction applies from application of the previous result to each $s \in S$: if S is algebraically independent then $S - s$ is a subset and therefore algebraically independent, and $S - \{s\} \cup \{s\}$ algebraically independent $\iff$ s is transcendental over $F(S - \{s\}$. Suppose now that s is transcendental over $F(S - \{s\})$ for every $s \in S$. If S was not algebraically independent, then there would exist some polynomial $f \in F[t_1, ..., t_n]$ s.t. $f(s_1, ..., s_n) = 0$ for some $s_1, ..., s_n \in S$. However, as s_n is transcendental over $F(S)$ we have that $f(s_1, ..., s_{n-1})(t) \in F(S - \{s\})[t]$ cannot have s_n as a root, which is a contradiction. Thus, there cannot exist such a polynomial, and S must be F-algebraically indepedent. □

Exercise 3 (Problem 3)**.**

Proof. We have that $\alpha^{p^r - 1}$ is inseparable over F, and in particular purely inseparable over the separable closure K/F in E. We have that α lives in a degree p^r extension over K as this is the degree of inseparability, and thus as the associated polynomial to any element in a purely inseparable extension is of the form $\alpha^{p^k} - \gamma^{p^k}$, we have that r must be minimal s.t. $\alpha^{p^r} \in K$ (as $\alpha^{p^r - 1} \notin K$. Thus,$\alpha$ is degree p^r in E/K, and thus $E = K(\alpha)$. Furthermore, by the primitive element theorem, we have that $K = F(\beta)$ for some $\beta \in F$, and thus $K = F(\beta, \alpha)$. □

Exercise 4. *Let K/F be a normal field extension and $f \in F[x]$ be irreducible. Show that every two monic irreducible factors of $f \in K[x]$ are conjugate over F.*

Proof. Suppose $f = h_1 h_2 ... h_n \in K[t]$ irreducible. Let α_i, α_j roots of h_i, h_j for arbitrary i, j. In $\overline{F}$ there exists an F-embedding sending $\alpha_j \mapsto \alpha_i$. As K is normal, this embedding into $\overline{F}$ restricts to an automorphism of K. Thus, there is an automorphism ϕ of K such that $\phi(a_k)\alpha_i^k + ... + \phi(a_0) = 0$ for $a_k, ..., a_0$ the coefficients of h_j, which we can extend to an automorphism $\overline{\phi}$ of $K[t]$ by permuting the coefficients, i.e. having $\overline{\phi}(t) = t$. By assumption, $h_1, ..., h_n$ are irreducible, and as any automorphism of $K[t]$ must take irreducibles to irreducibles, $\overline{\phi}(h_j)(\alpha) = 0 \implies \overline{\phi}(h_j) = m_K(\alpha_i) = h_i$, and thus h_i and h_j are conjugate. □

Exercise 5 (Problem 5)**.**

Proof. a) Consider the field $K(x)/K$ for x transcendental, K an algebraically closed field of characteristic p. We have that any finitely generated intermediate field for this extension $K(x)/E/K$ must be isomorphic to $K(p_1, p_2, ..., p_n)$ for $p_1, .., p_n$ rational functions in $K(x)$. We may select $p_1, ..., p_n$ s.t. they are a maximally algebraically independent subset in E, and thus they form a transcendence basis for E/K s.t. $E/K(S) \cong E/E$ is separable (being a trivial extension). However, we have that the extension $K(x)/K(x^p)$ is inseparable as the minimal polynomial of x is $t^p - x^p \in K(x^p)[t]$ from rationale given in the previous homework for $F(t_1, t_2)/F(t_1^p, t_2^p)$ with F arbitrary. Thus, this example holds.

□

Exercise 6 (Problem 6).

Proof. We have that the extension $F(x)/F(x^n + x^{-n})$ is separable as characteristic 0. We have that x is a solution to the polynomial $t^{2n} - 1 - t^n(x^n + x^{-n})$. In addition, we have that F is algebraically closed, and so in particular every nth root of unity ζ_n belongs in F; thus, $\zeta_n x$ is also a root of this polynomial for every ζ_n. Finally. we have that x^{-1} is also a root of this polynomial (clearly by evaluation), and thus $\zeta_n x^{-1}$ is also a root of this polynomial for every nth root of unity. Thus, we have $2n$ distinct roots in $F(x)$, implying that this polynomial splits in $F(x)$. Furthermore, any splitting field of this polynomial must contain a natural embedding from $F(x)$, as x is a root of the polynomial. Thus, $F(x)$ must be the unique splitting field of the polynomial given above, implying this is a normal, separable, and in particular Galois extension. Thus, the Galois group has order $2n$. We have an $F(x)$ automorphism of order 2, given by sending $x \mapsto x^{-1}$ and acting trivially on the field by extending linearly: this fixes the subfield $F(x^n + x^{-n})$. Fixing a primitive nth root of unity ζ_n, We have an $F(x)$ automorphism given by sending $\phi : x \mapsto \zeta_n x$ and acting trivially on the field, and extending linearly. This map is well defined, as given arbitrary $y \in F(x)$, we have that $y = ax^i$ for some $i \in \mathbb{Z}$. Thus, $\phi(ax^i) = a\phi(x^i) = a\zeta_n^i x^i$. It is a homomorphism by definition and is invertible and thus surjective, and thus is an automorphism: in particular, it fixes x^n, x^{-n} and thus fixes the subfield $F(x^n + x^{-n})$. This is an order n automorphism that we shall call σ, while we refer to the order 2 automorphism as τ. Collectively, σ, τ must generate the Galois group as $< \sigma >< \tau >$ is a product of two disjoint groups of order n and 2 respectively. We have that $\tau\sigma(x) = \zeta_n^{n-1} x \neq \zeta_n x^{-1} = \sigma\tau(x)$, so τ, σ do not commute with each other: furthermore, $< \sigma >$ must be a normal subgroup as it has index equal to the smallest prime dividing G. Thus, we may present it as a semidirect product $\mathbb{Z}_n \rtimes \mathbb{Z}_2$ with the only nontrivial map of $\mathbb{Z}_2$ into $Z_n^\times$ being the semidirect product of the dihedral group of order n. Thus, $G \cong D_n$. □

Exercise 7 (Problem 7).

Proof. Viewing $f = x^6 + 3x^4 + 3x^2 - 2$ as a polynomial in x^2, we see that x^2 can have the values $\sqrt[3]{3} - 1, -1 - \zeta_3 \sqrt[3]{3}, \zeta_3^2 \sqrt[3]{3} - 1$. Thus, x is $\pm$ the square root of each of these solutions. □