Modern Algebra II: Problem Set 11

Nilay Kumar

Last updated: April 22, 2013

Problem 1

Let F be a field. Let $F(t)$ be the field of rational functions with coefficients in F, where t is an indeterminate. We wish to show that F is algebraically closed in $F(t)$, i.e. that if $r(t) \in F(t)$ and $r(t)$ is algebraic over F, then $r(t) \in F$. So suppose that $r = p(t)/q(t)$ where p, q are relatively prime in $F[t]$, as well as that $f(r) = 0$ for some monic $f(x) \in F[x]$. If $r = 0$, it's clear that $r \in F$, and thus we may assume that $r \neq 0$. Now note that $F[x]$ is a subring of $F[t][x]$ and thus of $F(t)[x]$. Hence, we may view $f(x) = \sum_{i=0}^{n} a_i x^i$ as a polynomial in $F[t][x]$ with $a_i \in F$. The rational roots test then tells us that any rational root (in $F(t)[x]$, now) must have its numerator divide a_0 and its denominator divide $a_n = 1$ (we have assumed without loss of generality that $f(x)$ is monic). This means that out chosen $r(t)$ must be of the form $r(t) = p$ where $p \in F$ divides a_0 as the only elements of $F[t]$ that divide $a_0 \in F$ must be in F. Hence, $r \in F$ and thus F is algebraically closed in $F(t)$.

Problem 2

Let R be a UFD and let $f(x), g(x) \in R[x]$ be two nonzero polynomials. Then we can write $f(x) = c(f)f_0(x)$ and $g(x) = c(g)g_0(x)$ where f_0, g_0 are primitive. Taking the product, we find $f(x)g(x) = c(f)c(g)f_0(x)g_0(x)$. By the lemma we proved in class, $f_0(x)g_0(x)$ is primitive, and thus the content $c(fg) = c(f)c(g)$.

Problem 3

Let E be a finite extension field of a field F, and let $\sigma : E \to E$ be a homomorphism such that $\sigma(a) = a$ for all $a \in F$. Note that E is an F-vector space, and thus, since σ is an F-linear map (as we discussed in class), Im σ must be a vector subspace; this follows simply by linearity of σ and the fact that Im σ contains the identity $0 \in F$: if $f(a), f(b) \in \text{Im } \sigma$, then $f(a)+f(b) = f(a+b) \in \text{Im } \sigma$ as well. Using the fact that E is a field and all homorphisms between fields are injective (and E is a finite F-vector space), we must have that σ is surjective as well as injective by dimension-counting, as injectivity implies that $\dim_F \sigma(E) = \dim_F E$.

Problem 4

Consider the field $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ with $\mathbb{Q}$-basis $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$. Using the definitions for $\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) = \{1, \sigma_1, \sigma_2, \sigma_3\}$ from class, it is clear that the fixed fields can be found as follows. For σ_1, which flips the sign of the $\sqrt{2}$, the fixed field consists of the elements that are mapped to themselves under σ_1, i.e. elements that are independent of $\sqrt{2}$, i.e. the subfield $\mathbb{Q}(\sqrt{3}) \in \mathbb{Q}(\sqrt{3}, \sqrt{2})$. For σ_2 we have those that are independent of the $\sqrt{3}$, i.e. the subfield $\mathbb{Q}(\sqrt{2}) \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Finally, for σ_3 we need elements that don't change when we change the sign of both $\sqrt{2}$ and $\sqrt{3}$, i.e. elements in the subfield $\mathbb{Q}(\sqrt{6}) \in \mathbb{Q}(\sqrt{3}, \sqrt{2})$.

Problem 5

Let σ be complex conjugation acting on the field $\mathbb{Q}(\sqrt[3]{2}, \omega)$, where $\omega = e^{2\pi i/3}$ is a cube root of unity, and hence a root of $x^2 + x + 1$. If we look at this field as an extension of $Q(\sqrt[3]{2})$, it's clearly a finite extension of degree 2, as the degree of the irreducible polynomial for ω is 2. For the same reason, 1 and ω are linearly independent, as no $\mathbb{Q}(\sqrt[3]{2})$-linear combination of them can yield zero (all such combinations would be necessarily quadratic). By linear algebra, then, $1, \omega$ must be a $\mathbb{Q}(\sqrt[3]{2})$-basis for $\mathbb{Q}(\sqrt[3]{2}, \omega)$. To find the fixed field $\mathbb{Q}(\sqrt[3]{2}, \omega)^{\langle \sigma \rangle}$, we must find the subfield of elements that is fixed by complex conjugation. Clearly any element with an imaginary part cannot be in the fixed field, as it would suffer a sign change. Consequently the fixed field cannot have a component in the ω direction, so to speak, and thus must be wholly in $\mathbb{Q}(\sqrt[3]{2})$, which is the fixed field.

Problem 6

Take the polynomial $\Phi_5(x) = (x^5 - 1)/(x - 1)$, irreducible in $\mathbb{Q}[x]$ of degree 4, where $\zeta = e^{2\pi i/5}$ is a root of $\Phi_5(x)$.

(a) Given ζ as above, we can check that ζ^α for $\alpha = 1, 2, 3, 4$ is a root of

$\Phi_5(x)$:

$$\Phi_5(\zeta) = \frac{e^{2\pi i} - 1}{e^{2\pi i/5} - 1} = 0$$
$$\Phi_5(\zeta^2) = \frac{e^{4\pi i} - 1}{e^{4\pi i/5} - 1} = 0$$
$$\Phi_5(\zeta^3) = \frac{e^{6\pi i} - 1}{e^{6\pi i/5} - 1} = 0$$
$$\Phi_5(\zeta^4) = \frac{e^{8\pi i} - 1}{e^{8\pi i/5} - 1} = 0$$

simply because the numerator goes to zero. Now take the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, which is the group of automorphisms of $\mathbb{Q}(\zeta)$ that fixes $\mathbb{Q}$. By the theorem we proved in class, then, since $\mathbb{Q}(\zeta)$ is generated over $\mathbb{Q}$ by the roots of $\Phi_5(x)$ that lie in $\mathbb{Q}(\zeta)$, the homomorphism from the Galois group to the symmetric group S_4, viewed as the set of permutations of the set $\{\zeta_1, \zeta_2, \zeta_3, \zeta_4\}$, is injective.

(b) Given $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, since σ must fix elements of $\mathbb{Q}$, it must only act non-trivially on powers of ζ. Note however, that since σ is a homomorphism, once we know how it acts on ζ, namely, $\sigma(\zeta)$, it follows trivially that $\sigma(\zeta^2) = \sigma^2(\zeta)$ and similarly for higher powers. Thus, since any element of $\mathbb{Q}(\zeta)$ can be written as a $\mathbb{Q}$-linear combination of elements of $\mathbb{Q}$ and powers of ζ, σ is completely determined by its value on ζ. Of course, even this value is restricted, as from the previous part of the problem, σ can only take ζ to one of $\zeta, \zeta^2, \zeta^3, \zeta^4$, and thus there are at most four possibilities for $\sigma(\zeta)$.

Problem 7

Suppose such an automorphism existed. Then consider $\sigma(\sqrt[4]{2}) \in \mathbb{R}$. We must have that $\sigma^2(\sqrt[4]{2}) > 0$ as it is the square of a real number. But by the homomorphism property, we know that $\sigma^2(\sqrt[4]{2}) = \sigma(\sqrt{2}) = -\sqrt{2} < 0$, which is a contradiction.