MODERN ALGEBRA II SPRING 2013: ELEVENTH PROBLEM SET

1. Let F be a field. Show that F is algebraically closed in $F(t)$, the field of rational functions with coefficients in F, where t is an indeterminate (variable). In other words, show that, if $r(t) \in F(t)$ and $r(t)$ is algebraic over F, then $r(t) \in F$. (Hint: suppose that $r = p(t)/q(t)$ is a rational function in lowest terms, i.e. $p(t)$ and $q(t)$ are relatively prime polynomials in t, and that $f(r) = 0$ for some monic $f(x) \in F[x]$. The case $r = 0$ is clear, so we may assume $r \neq 0$ and hence that the constant term of f is nonzero. Viewing $F[x]$ as a subring of $F[t][x]$ and hence of $F(t)[x]$, conclude by the rational roots test that the numerator and denominator of r are constants, hence that $r \in F$.)

2. Let R be a UFD and let $f(x), g(x) \in R[x]$ be two nonzero polynomials. Show that $c(fg) = c(f)c(g)$.

3. Let E be a finite extension field of a field F, and let $\sigma\colon E \to E$ be a homomorphism such that $\sigma(a) = a$ for all $a \in F$. Show that the image of σ, $\sigma(E)$, is equal to E, i.e. that σ is surjective (and hence σ is an automorphism of E and thus an element of $\mathrm{Gal}(E/F)$). (Hint: using the fact that σ is F-linear, show that the image $\sigma(E)$ is an F-vector subspace of E. Now use the fact that σ is injective.)

4. Consider the field $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, with $\mathbb{Q}$-basis 1, $\sqrt{2}$, $\sqrt{3}$, $\sqrt{6}$. We have seen in class that $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) = \{1, \sigma_1, \sigma_2, \sigma_3\}$, where $\sigma_1(\sqrt{2}) = -\sqrt{2}$, $\sigma_1(\sqrt{3}) = \sqrt{3}$, $\sigma_2(\sqrt{2}) = \sqrt{2}$, $\sigma_2(\sqrt{3}) = -\sqrt{3}$, and $\sigma_3 = \sigma_1\sigma_2$. Find the fixed fields $\mathbb{Q}(\sqrt{2}, \sqrt{3})^{\langle\sigma_1\rangle}$, $\mathbb{Q}(\sqrt{2}, \sqrt{3})^{\langle\sigma_2\rangle}$, $\mathbb{Q}(\sqrt{2}, \sqrt{3})^{\langle\sigma_3\rangle}$.

5. Let σ be complex conjugation acting on the field $\mathbb{Q}(\sqrt[3]{2}, \omega)$, where $\omega = e^{2\pi i/3} = \frac{1}{2}(-1 + \sqrt{-3}) = \frac{1}{2}(-1 + i\sqrt{3})$ is a cube root of unity, and hence is a root of $x^2 + x + 1$. Show that $1, \omega$ is a basis for $\mathbb{Q}(\sqrt[3]{2}, \omega)$ over $\mathbb{Q}(\sqrt[3]{2})$, i.e is a basis for the $\mathbb{Q}(\sqrt[3]{2})$-vector space $\mathbb{Q}(\sqrt[3]{2}, \omega)$. Find the fixed field $\mathbb{Q}(\sqrt[3]{2}, \omega)^{\langle\sigma\rangle}$, where σ is complex conjugation.

6. We have seen that the polynomial $\Phi_5(x) = \dfrac{x^5 - 1}{x - 1}$ is an irreducible polynomial in $\mathbb{Q}[x]$ of degree 4, and hence that $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 4$, where $\zeta = e^{2\pi i/5}$ is a root of $\Phi_5(x)$.

   (a) Show that the four roots of $\Phi_5(x)$ in $\mathbb{C}$ are $\zeta_1 = \zeta$, $\zeta_2 = \zeta^2$, $\zeta_3 = \zeta^3$, and $\zeta_4 = \zeta^4$. Conclude that there is an injective homomorphism from $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ to S_4, viewed as the set of permutations of the set $\{\zeta_1, \zeta_2, \zeta_3, \zeta_4\}$.

(b) Given $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, show that σ is determined by its value on ζ, and that there are at most 4 possibilities for $\sigma(\zeta)$. Hence $\#(\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})) \leq 4$. (In fact, $\#(\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})) = 4$ and that $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is cyclic; we shall see this later.)

7. Show that there is no automorphism $\sigma\colon \mathbb{R} \to \mathbb{R}$ such that $\sigma(\sqrt{2}) = -\sqrt{2}$. (What is $\sigma(\sqrt[4]{2})$?)

(Note: in fact, one can show that $\mathrm{Aut}\,\mathbb{R} = \{\mathrm{Id}\}$ as follows: let $\sigma \in \mathrm{Aut}\,\mathbb{R}$. Then $t \in \mathbb{R}$ is a square $\iff$ $\sigma(t)$ is a square, hence $t > 0$ $\iff$ $\sigma(t) > 0$. Thus $t_1 < t_2 \implies \sigma(t_1) < \sigma(t_2)$. Now use the fact that, if $r \in \mathbb{Q}$, $\sigma(r) = r$ and that, for every real number t and every $\varepsilon > 0$, we can find rational numbers $r_1 < r_2$ with $r_1 < t < r_2$ and $r_2 - r_1 < \varepsilon$, to conclude that $r_1 < \sigma(t) < r_2$ and that $|t - \sigma(t)| < \varepsilon$. Since this is true for all $\varepsilon > 0$, $\sigma(t) = t$ for every $t \in \mathbb{R}$, i.e. $\sigma = \mathrm{Id}$.)