MODERN ALGEBRA II SPRING 2013: SIXTH PROBLEM SET

1. Show that, if $r \in \mathbb{Q}$ and $r = \delta^2$ for some $\delta \in \mathbb{Q}(\sqrt{2})$, then either $r = s^2$ for some $s \in \mathbb{Q}$ or $r = 2s^2$ for some $s \in \mathbb{Q}$. Conclude that there is no $\delta \in \mathbb{Q}(\sqrt{2})$ such that $\delta^2 = 3$, i.e. $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. Conclude that $x^2 - 3$ is irreducible in $\mathbb{Q}(\sqrt{2})[x]$, in other words that $x^2 - 3 = \operatorname{irr}(\sqrt{3}, \mathbb{Q}(\sqrt{2}), x)$

2. Let $\alpha = \sqrt{2} + \sqrt{3}$. Show that α is a root of $x^4 - 10x^2 + 1$ and hence that $\operatorname{irr}(\alpha, \mathbb{Q}, x)$ divides $x^4 - 10x^2 + 1$. Show that $\mathbb{Q}(\alpha)$ is contained in any subfield of $\mathbb{R}$ containing $\sqrt{2}$ and $\sqrt{3}$. By experimentation and direct computation, show that $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\alpha)$ (for example, you can begin by showing that $\sqrt{6} \in \mathbb{Q}(\alpha)$) and hence that $\mathbb{Q}(\alpha)$ is the smallest subfield of $\mathbb{R}$ containing $\sqrt{2}$ and $\sqrt{3}$.

3. (A nested radical.) Let $\alpha = \sqrt{3 + 2\sqrt{2}}$. Show that α is a root of the polynomial $x^4 - 6x^2 + 1 = 0$. However, show that $x^4 - 6x^2 + 1$ is reducible in $\mathbb{Q}[x]$ by writing it as a product $(x^2 + ax + b)(x^2 - ax + b)$ for appropriate a and b. Interpret this fact by showing that $\sqrt{3 + 2\sqrt{2}} = r + s\sqrt{2}$ for some $r, s \in \mathbb{Q}$.

4. In the ring $\mathbb{F}_2[x]$, list all of the irreducible monic polynomials of degree at most three (recall that $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$). (Note: you should find two of degree 1, one of degree 2, and two of degree 3.) Using this information, decide if the polynomial $x^4 + x^3 + x^2 + x + 1$ is irreducible in $\mathbb{F}_2[x]$. (First test to see if it has any roots in $\mathbb{F}_2$.)

5. (Chinese remainder theorem for $F[x]$.) Let F be a field and let $f(x) \in F[x]$ and $g(x) \in F[x]$ be relatively prime. Show that

$$F[x]/(f(x)g(x)) \cong (F[x]/(f(x))) \times (F[x]/(g(x))).$$

as follows: by the Fundamental Homomorphism Theorem (= First Isomorphism Theorem) it is enough to find a surjective homomorphism $\rho \colon F[x] \to (F[x]/(f(x))) \times (F[x]/(g(x)))$ whose kernel is $(f(x)g(x))$. Define ρ via:

$$\rho(h(x)) = (h(x) + (f(x)), h(x) + (g(x))).$$

(i) Show that $\rho(h(x)) = 0 \iff$ both $f(x)$ and $g(x)$ divide $h(x)$ $\iff f(x)g(x)$ divides $h(x) \iff h(x) \in (f(x)g(x))$.

(ii) Show that ρ is surjective using the fact that there exist $r(x), s(x) \in F[x]$ such that $r(x)f(x)+s(x)g(x) = 1$. In fact, given $a(x), b(x) \in F[x]$, show that, if we set

$$h(x) = r(x)b(x)f(x) + s(x)a(x)g(x),$$

then $\rho(h(x)) = (a(x)+(f(x)), b(x)+(g(x)))$. Hence ρ is surjective.

In particular, if $a, b \in F$ and $a \neq b$, conclude that

$$F[x]/((x-a)(x-b)) \cong F \times F,$$

generalizing Problem 3(iii) from HW 5.

6. As in the handout, "An analogy and an example," there exists a field with 4 elements $E = \mathbb{F}_2(\alpha)$, where α is a root of the polynomial $x^2 + x + 1 \in \mathbb{F}_2[x]$. Since $x - \alpha = x + \alpha$ is a root of $x^2 + x + 1$, the polynomial x^2+x+1 must factor into a product of linear polynomials, one of which is $x + \alpha$. In other words, $x^2 + x + 1 = (x + \alpha)(x + \beta)$, where β is another root of $x^2 + x + 1$ (possibly equal to α). Find β, in other words find the complete factorization of $x^2 + x + 1$ into irreducible polynomials in $E[x]$. Why can't α be a repeated root of $x^2 + x + 1$, in other words why can't $x^2 + x + 1 = (x + \alpha)^2$? (Hint: recall the Frobenius homomorphism in characteristic 2.)

7. Let $f(x) = x^2 + 1 \in \mathbb{F}_3[x]$. Show that $f(x)$ is irreducible in $\mathbb{F}_3[x]$, and let $E = \mathbb{F}_3(\alpha) = \mathbb{F}_3[x]/(f(x))$, where $\alpha = x + (f(x))$ and we identify $\mathbb{F}_3$ with its image in E. What is the complete factorization of $f(x)$ into a product of linear factors in $E[x]$? Show that E has 9 elements and that $(E, +) \cong (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$. How many elements are there in $(E^*, \cdot)$? By experiment, show that the multiplicative group $(E^*, \cdot)$ is cyclic by finding a generator. In fact, you can clearly rule out elements of $\mathbb{F}_3$ as generators. Also, α will not work since $\alpha^4 = 1$, and similarly for $2\alpha = -\alpha$. How many generators does E^* have (i.e. what is $\varphi(8)$, where φ is the Euler φ-function)? By counting, any element of E^* not equal to $1, 2, \alpha, 2\alpha$ should be a generator. Verify this directly.