MODERN ALGEBRA II SPRING 2013: NINTH PROBLEM SET

1. Let F be a field of characteristic $p > 0$.

   (i) Suppose that every element of F is a p^{th} power, i.e. for all $a \in F$, there exists an element $b \in F$ such that $b^p = a$. Equivalently, the Frobenius homomorphism $\sigma_p \colon F \to F$ is surjective. Such a field is called *perfect*. Show that, if $f(x) \in F[x]$ is irreducible, then $f(x)$ does not have multiple roots. (Hint: if it did, then $f(x)$ would have derivative zero and hence be of the form $\sum_{i=0}^{n} a_i x^{ip}$ for some $a_i \in F$. Since F is perfect, there exist $b_i \in F$ such that $a_i = b_i^p$. Now show that the polynomial $f(x) = \sum_{i=0}^{n} a_i x^{ip} = \sum_{i=0}^{n} b_i^p x^{ip}$ is a p^{th} power and hence is not irreducible, a contradiction.)

   (ii) Show that a finite field is perfect. (Hint: consider the Frobenius homomorphism $\sigma_p \colon F \to F$. Using the fact that σ_p is a homomorphism, show that σ_p is injective. Now using the fact that F is finite, conclude that σ_p is surjective.)

   (iii) Let F be a finite field and let k be a positive integer. Is it necessarily true that every element of F is a k^{th} power, i.e. for all $a \in F$, there exists an element $b \in F$ such that $b^k = a$? Where does the argument in (ii) break down?

2. Throughout this problem, $\mathbb{F}_2$ denotes the finite field with 2 elements.

   (i) Let $\mathbb{F}_2(\alpha)$ be a simple extension of $\mathbb{F}_2$, generated by an element α such that $\alpha^2 + \alpha + 1 = 0$, i.e. α is a root of the polynomial $x^2 + x + 1$. What is $[\mathbb{F}_2(\alpha) : \mathbb{F}_2]$? Show that $\alpha^2 = \alpha + 1$ is also a root of $x^2 + x + 1$, and hence $x^2 + x + 1$ factors into linear factors in $\mathbb{F}_2(\alpha)[x]$.

   (ii) Let $\mathbb{F}_2(\beta)$ be a simple extension of $\mathbb{F}_2$, generated by an element β such that $\beta^3 + \beta + 1 = 0$, i.e. β is a root of the polynomial $x^3 + x + 1$. What is $[\mathbb{F}_2(\beta) : \mathbb{F}_2]$? How many elements does $\mathbb{F}_2(\beta)$ have? Show (without any computation) that β^2 and β^4 are also roots of $x^3 + x + 1$. (Hint: apply the Frobenius homomorphism to the relation $\beta^3 + \beta + 1 = 0$.) Express β^4 as an element of the form $a_0 + a_1\beta + a_2\beta^2$, with $a_i = 0$ or 1, and verify directly that $x^3 + x + 1$ factors into linear factors in $\mathbb{F}_2(\beta)[x]$.

   (iii) Let β be as in (ii). Since $x^3 + x^2 + 1$ is irreducible over $\mathbb{F}_2$, argue that there is a root of $x^3 + x^2 + 1$ in $\mathbb{F}_2(\beta)$. In fact, simply by counting, every element of $\mathbb{F}_2(\beta)$ either lies in $\mathbb{F}_2$ or is a root of x^3+x+1 or of x^3+x^2+1, in other words its irreducible polynomial is of degree one or three. How do you know this without any computation, in particular how do you know that there is no element of $\mathbb{F}_2(\beta)$ which satisfies an irreducible quadratic polynomial over $\mathbb{F}_2$? Conclude that, in $\mathbb{F}_2[x]$,

$$x^8 - x = x^8 + x = x(x+1)(x^3+x+1)(x^3+x^2+1).$$

3. Let R be a PID. Assume that R is not a field (in other words, the ideal (0) is not a maximal ideal). Let I be an ideal in R. Arguing as we did for the polynomial ring $F[x]$, show that the following are equivalent:

    (i) I is a maximal ideal.

    (ii) I is a prime ideal and $I \neq (0)$.

    (iii) $I = (r)$, where r is irreducible.

4. Let R be an integral domain and let N be a submultiplicative Euclidean norm on R.

    (a) Show that, for all $r \in R - \{0\}$, $N(1) \leq N(r)$.

    (b) Show that, for all $r \in R - \{0\}$, $N(r) = N(1) \iff r$ is a unit.

    (c) Let $r \in R$, with $r \neq 0$, and suppose that $N(r) > N(1)$ and that $N(r)$ is minimal with respect to this property (i.e. if $s \in R - \{0\}$ and $N(s) < N(r)$, then $N(s) = N(1)$). Show that r is irreducible.