Modern Algebra II: Problem Set 9

Nilay Kumar

Last updated: March 31, 2013

Problem 1

Let F be a field of a characteristic $p \geq 0$.

(i) Suppose that every element of F is a pth power, i.e. for all $a \in F$, there exists an element $b \in F$ such that $b^p = a$. Equivalently, the Frobenius homomorphism $\sigma_p : F \to F$ is surjective. Such a field is called **perfect**. We wish to show that if $f(x) \in F[x]$ is irreducible, then $f(x)$ does not have multiple roots. Let us assume for the sake of contradiction that $f(x) = \sum_{i=0}^{n} a_i x^i$ irreducible has multiple roots. Then $Df(x) = 0$ by a corollary proved in class. Since $f(x)$ is not a constant, in order for the derivative to be identically zero we must have that f is of the form $f(x) = \sum_{i=0}^{n} a_i x^{ip}$, i.e. bringing down the exponents annihilates each term. Using the fact that F is perfect, we can now rewrite, for some $b_i \in F$:

$$\begin{aligned} f(x) &= \sum_{i=0}^{n} a_i x^{ip} = \sum_{i=0}^{n} b_i^p x^{ip} = \sum_{i=0}^{n} (b_i x)^p \\ &= \sum_{i=0}^{n} \sigma_p(b_i x) = \sigma_p\left(\sum_{i=0}^{n} b_i x\right) = \left(\sum_{i=0}^{n} b_i x\right)^p, \end{aligned}$$

and thus f is a pth power. This contradicts that f is irreducible, and thus f cannot have multiple roots.

(ii) Given F finite, we wish to show that F is perfect. Consider the Frobenius homomorphism $\sigma_p : F \to F$. Suppose $\sigma_p(a) = \sigma_p(b) = c$ for some $a, b, c \in F$. Then,

$$\sigma_p(a) - \sigma_p(b) = \sigma_p(a - b) = (a - b)^p = 0,$$

and thus $a = b$, as there are no zero divisors in a field. Consequently, σ_p is injective. Furthermore, since σ_p is a map from a finite F to itself, injectivity implies surjectivity. Consequently, every element of F can be written as a pth power, and thus F is perfect.

(iii) Let F be a finite field and let k be a positive integer. In general, then, $a \mapsto a^k$ is not a homomorphism, as the binomial coefficients do not disappear as usual when taking $(p+q)^k$. It is thus not necessarily true that for all $a \in F$ there exists an element $b \in F$ such that $b^k = a$.

Problem 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. Note that since α satisfies a polynomial of degree 2, α^2 and higher powers can be written using $\mathbb{F}_2$ and α. Thus $[\mathbb{F}_2(\alpha):\mathbb{F}_2]=2$, as we can write a basis $\{1,\alpha\}$. In addition, note that

$$(\alpha+1)^2+(\alpha+1)+1=(\alpha+1+1)+(\alpha+1)+1=0.$$

Consequently, we can write

$$x^2+x+1=(x+\alpha)(x+\alpha+1).$$

(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. In this case, we can write β^3 and all higher powers in terms of elements of $\mathbb{F}_2$ and β. Then, $[\mathbb{F}_2(\beta):\mathbb{F}_2]=3$, as we can write a basis $\left\{1,\beta,\beta^2\right\}$. $\mathbb{F}_2(\beta)$ then has $2^3=8$ elements. Note that we can compute

$$\sigma_2(\beta^3+\beta+1)=\beta^6+\beta^2+1=(\beta^2)^3+\beta^2+1=0$$

and thus β^2 is also a root of x^3+x+1. The same can be shown for β^4,

$$\sigma_2(\beta^6+\beta^2+1)=\beta^{12}+\beta^4+1=(\beta^4)^3+\beta^4+1=0.$$

In fact, we can express

$$\beta^4=\beta\beta^3=\beta(\beta+1)=0+\beta+\beta^2.$$

Consequently, we can write

$$\begin{aligned} x^3+x+1 &= (x+\beta)(x+\beta^2)(x+\beta^4) \\ &= (x+\beta)(x+\beta^2)(x+\beta^2+\beta). \end{aligned}$$

(iii) Since $x^3 + x^2 + 1$ is irreducible, take γ to be a root in some extension field. Then we can construct an extension $\mathbb{F}_2(\gamma)$ of degree three over $\mathbb{F}_2$ that has 8 elements. But we know that two finite fields with the same number of elements are isomorphic to each other, i.e. there exists an isomorphism $\phi : \mathbb{F}_2(\beta) \to \mathbb{F}_2(\gamma)$. Thus, if we take $\alpha = \phi(\gamma)$, we have

$$0 = \phi(\gamma^3 + \gamma^2 + 1) = \alpha^3 + \alpha^2 + 1$$

and $x^3 + x^2 + 1$ thus has a root in $\mathbb{F}_2(\beta)$. Now note that the roots of x^3+x+1 are all different that the roots of x^3+x^2+1 (this can be shown by explicit computation or by noticing that since β is not a root, the Frobenius homomorphism used as above will show that β^2, β^4 are not roots). Consequently, since we have 8 elements, 6 are roots of either $x^3 + x^2 + 1$ or $x^3 + x + 1$, and the other 2 (since these polynomials are irreducible in $\mathbb{F}_2$) must be the elements of $\mathbb{F}_2$. In other words, every element's irreducible polynomial is of degree either 1 or 3. Indeed, we can see explicitly that no element of $\mathbb{F}_2(\beta)$ could possibly have an irreducible polynomial of degree two, because if there were such an element, α, the extension $\mathbb{F}_2(\alpha) \subset \mathbb{F}_2(\beta)$ and $\mathbb{F}_2(\alpha)(\beta) = \mathbb{F}_2(\beta)(\alpha) = \mathbb{F}_2(\beta)$. But $[\mathbb{F}_2(\alpha, \beta) = \mathbb{F}_2(\beta) : \mathbb{F}_2] = [\mathbb{F}_2(\alpha, \beta) : \mathbb{F}_2(\alpha)][\mathbb{F}_2(\alpha) : \mathbb{F}_2]$ and the left hand side is equal to the three while the right hand side is 2 times some natural number. This is impossible, and thus, such an α cannot exist.

Recall that we know that any finite field with q elements is defined by the roots of the polynomial $x^q - x$, and thus, in our case, the polynomial $x^8 - x$ has every element of $\mathbb{F}_2(\beta)$ as its roots. Consequently, in $\mathbb{F}_2(\beta)[x]$, $x^8 - x = \prod_i^8 (x - a_i)$ where a_i are the elements. In $F_2[x]$, then, we can write (using above computations) $x^8 - x = x(x+1)(x^3 + x+1)(x^3+x^2+1)$ because these irreducible polynomials must all divide $x^8 - x$.

Problem 3

Let R be a PID. We assume that R is not a field and so (0) is not a maximal ideal. Let I be an ideal in R. Let us prove that the following three statements 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.

(i) $\implies$ (ii): Suppose I is maximal. Then I is non-zero and must be prime, as every maximal ideal is prime.

(ii) $\implies$ (iii): Now suppose that $I \neq (0)$ is a prime ideal. Since every ideal in R is principal, $I = (r)$ for some $r \in R$. We wish to show that r is irreducible. First of all, r cannot be a unit, because otherwise the ideal would contain 1, and thus all of R, which would contradict that I is prime. Furthermore $r \neq 0$, because this would contradict $I \neq (0)$. To show that r is irreducible, we must show that if $r = st$, then one of s, t is a unit. Since (r) is prime, one of s, t must be in (r), and thus $r = qrt$ (we've chosen s, the other case follows similarly). Cancelling, we find that $qt = 1$, i.e. that s is a unit, and thus r is irreducible.

(iii) $\implies$ (i): Assuming that r is irreducible, we wish to show that $I = (r)$ is a maximal ideal, i.e. $(r) \neq R$ and if $(r) \subset J$ some ideal then either $J = (r)$ or $J = R$. First note that $(r) \neq R$ because this would imply that $1 \in (r)$, but this is not possible as r is not a unit. Since J is a principal ideal (working in a PID), $J = (s)$ for some $s \in R$. If $(r) \subset (s)$, then $r \in (s)$ so $r = st$ for some $t \in R$. But r is irreducible so either t is a unit, in which case $J = (t) = R$, or $t = cr$ for c a unit, in which case $J = (t) = (r)$. Consequently, I is maximal.

Problem 4

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

(a) Since N is submultiplicative, it should be clear that $N(1) \leq N(r) = N(r \cdot 1)$.

(b) If r is a unit, then by the lemma proven in class, $N(r) = N(rs)$ for any $s \in R$. If we choose $s = r^{-1}$, we find that $N(r) = N(rr^{-1}) = N(1)$. Conversely, we know that $N(r) = N(1)$ is only true if r is unit, also by the lemma proven in class.

(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. Assume for the sake of contradiction that r is not irreducible, i.e. that it can be written as a product $p_1 \cdots p_n$. We also assume that r is not a unit, because if it were, we'd reach a contradiction immediately (as $N(r) = N(1)$). We have $N(r) = N(p_1 \cdots p_n) > N(p_1)$, i.e. that $N(p_1) < N(r)$, and we reach a contradiction. Thus, r must be irreducible.