Kris Harper
MATH 24200
May 17, 2010

Homework 5

Problem 1. *Let F be a field with q element and suppose that $q \equiv 1 \pmod{n}$. Show that for $\alpha \in F^*$ the equation $x^n = \alpha$ has eitehr no solutions or n solutions.*

Proof. We know that $x^n = \alpha$ has solutions if and only if $\alpha^{(q-1)/d} = 1$, where $d = (n, q-1)$ and if there are solutions then there are precisely d solutions. So the equation either has no solutions, or, if it has a solution then it has $(n, q-1)$ solutions. But since $n \mid q-1$, we see that $(n, q-1) = n$. □

Problem 2. *Show that the set of $\alpha \in F^*$ such that $x^n = \alpha$ is solvable is a subgroup with $(q-1)/n$ elements.*

Proof. Let G be the set in question and let $\alpha, \beta \in G$. Then there exist $x, y \in F^*$ such that $x^n = \alpha$ and $y^n = \beta$. But then $(xy)^n = x^n y^n = \alpha\beta$ so $\alpha\beta \in G$ as well. Also if $x^n = \alpha$ and $(x^{-1})^n = (x^n)^{-1} = \alpha^{-1}$ so $\alpha^{-1} \in G$. Since $n \mid q-1$ there are exactly $(q-1)/n$ elements with $x^n = \alpha$ so G is nonempty and thus a subgroup with order $(q-1)/n$. □

Problem 3. *Let K be a field containing F such that $[K : F] = n$. For all $\alpha \in F^*$ show that the equation $x^n = \alpha$ has n solutions in K.*

Proof. Note that $q^n - 1 = (q-1)(q^{n-1} + \cdots + q + 1)$ and since $q \equiv 1 \pmod{n}$ we have $q^{n-1} + \cdots + q + 1 \equiv n \equiv 0 \pmod{n}$. Therefore $n(q-1) \mid q^n - 1$. We know K has q^n elements, so the equation $x^n = \alpha$ is solvable if and only if $\alpha^{(q^n-1)/d} = 1$ where $d = (n, q^n - 1)$. We've seen that $d = n$ and that $\alpha^{(q^n-1)/n} = \alpha^{q-1} = 1$ since $\alpha \in F^*$. Thus, this equation is solvable and there are precisely $d = n$ solutions. □

Problem 4. *Let $K \supseteq F$ be finite fields with $[K : F] = 3$. Show that if $\alpha \in F$ is not a square in F, it is not a square in K.*

Proof. If α is not a square in F then $(\alpha/p^n) = -1$. But then $(\alpha/p^n)^3 = (\alpha/(p^n)^3) = -1$ as well so α is not a square in K either. □

Problem 5. *Use Proposition 7.2.1 to show that given a field k and a polynomial $f(x) \in k[x]$ there is a field $K \supseteq k$ such that $[K : k]$ is finite and $f(x) = (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n)$ in $K[x]$.*

Proof. Suppose that $\deg f(x) = n$ and let the roots of $f(x)$ be $\alpha_1, \dots, \alpha_n$. Then there exists a field $K_1 \supseteq k$ containing α_1 such that $f(\alpha_1) = 0$ in K_1. But then $f(x) = (x - \alpha_1) f_1(x)$ in K_1 for some degree $n-1$ polynomial $f_1(x) \in K_1[x]$. By the same proposition, we know there exists a field $K_2 \supseteq K_1 \supseteq k$ containing α_2 such that $f_1(\alpha_2) = 0$ which means $f_1(x) = (x - \alpha_2) f_2(x)$ for some degree $n-2$ polynomial $f_2(x) \in K_2[x]$. Continue in this way until we reach a field $K_n \supseteq K_{n-1} \supseteq \cdots \supseteq K_1 \supseteq k$ in which $f(x) = (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n)$. □

Problem 6. *Apply Exercise 12 to $k = \mathbb{Z}/p\mathbb{Z}$ and $f(x) = x^{p^n} - x$ to obtain another proof of Theorem 2.*

Proof. We know there exists a field $K \supseteq k$ with $[K : k]$ finite such that $f(x) = x^{p^n} - x = (x - \alpha_1) \dots (x - \alpha_n)$ in $K[x]$. Then for each $d \mid n$ if $g(x)$ is an irreducible polynomial of degree d, it must split into linear factors in K. These linear factors are a subset of $\{(x - \alpha_1), \dots, (x - \alpha_n)\}$ so that if we group these factors by the divisors of n, we get $f(x) = \prod_{d \mid n} F_d(x)$. □

Problem 7. *Let F be a field with q elements and n a positive integer. Show that there exist irreducible polynomials in $F[x]$ of degree n.*

Proof. Let $q = p^m$ for some prime p and let K be the field with p elements. Then let $f(x) \in K[x]$ be an irreducible polynomial of degree mn and let $g(x)$ be an irreducible factor of $f(x)$ in $F[x]$. Let α be a root of $g(x)$. Since $g(x)$ is irreducible in F, we know $\deg g(x) \geq m$. Thus $K(\alpha) = K[x]/(g(x))$ is an extension of degree at least m. Therefore $F \subseteq K(\alpha)$ and since we already have $K \subseteq F$, we now have $F(\alpha) = K(\alpha)$. Furthermore, this means $[F(\alpha) : F] = n$ which means $\deg g(x) = n$. □

Problem 8. *Let q and p be distinct odd primes. Show that the number of monic irreducibles of degree q in $\mathbb{Z}/p\mathbb{Z}[x]$ is $q^{-1}(p^q - p)$.*

Proof. Note that we already know $N_q = q^{-1} \sum d \mid q\mu(q/d)p^d$. But q is prime so this sum only includes the terms $d = 1$ and $d = q$. We then have $N_q = q^{-1}(\mu(q)p + \mu(1)p^q) = q^{-1}(p^q - p)$ as desired. □

Problem 9. *Let p be a prime with $p \equiv 3 \pmod 4$. Show that the residue classes modulo p in $\mathbb{Z}[i]$ form a field with p^2 elements.*

Proof. Consider the residue classes $\{\overline{a + bi} | 0 \leq a \leq p-1, 0 \leq b \leq p-1\}$. If $x + yi \in \mathbb{Z}$ then we can find $a \in \{0, \ldots, p-1\}$ with $npx - a$ for some $n \in \mathbb{Z}$. Then $(n+mi)p = (x-a)+(y-b)i$ for an appropriate $m \in \mathbb{Z}$ so that these constitute a complete residue system modulo p. We've already seen that these classes are closed under addition and multiplication and that they form a commutative ring with 1. We need only to show that there are multiplicative inverses. Note that $\overline{a + bic + di} = \overline{(ac - bd) + (ad + bc)i}$. If $ac - bd = ad + bc = 0$ then $0 = bd^2 + bc^2 = b(c^2 + d^2)$ which means either $c = d = 0$ or $b = 0$. In the later case we have $ac = ad = 0$ so $a(c - d) = 0$. But in the case $c = d$ we're reduced the case of residue classes in the integers and since p is prime if follows that $c + di$ is not a zero-divisor in $\mathbb{Z}[i]$. Thus $a = 0$ and $a + bi = 0$. Therefore the residue classes form an integral domain. We can take a nonzero class and multiply if by every other class and this map will be injective because if the integral domain property and by finiteness, also surjective. Thus, every nonzero element has some inverse since 1 is in the image of this multiplication map. This shows that the residue classes form a field and there are p^2 residues classes. □