Midterm Exam 2

Math 401

November 11, 2014

Again feel free to do the problems out of order; even if you don't manage to solve some part, you may quote the result in a later part.

1. (20 points) Which of the following polynomials are irreducible in $\mathbb{Z}[x]$? You may refer to the list of irreducible polynomials in $\mathbb{Z}_2[x]$ and $\mathbb{Z}_3[x]$ on the back page.

(a) $x^4 + x^2 - 2$

(b) $x^4 - 2x^2 + 1$

(c) $x^4 - 2x^2 - 1$

(d) $x^4 - 2x^2 - 2$

2. (20 points) Let $F \subset K$ be a field extension.

(a) Let $f, g \in F[x]$. Show that if f and g have a common root in K, that is, if there is an $\alpha \in K$ such that $f(\alpha) = g(\alpha) = 0$, then their greatest common divisor in $F[x]$ is not 1. (Caution: If α were in F you could use the root-factor theorem, but α is in K.)

(b) Show that if $f, g \in F[x]$ have a common root $\alpha \in K$ and f is irreducible then $f \mid g$.

(c) Let $f, g \in F[x]$, let $n = \deg f$, and let $q = \deg g$. Show that if g has q distinct roots in K and $f \mid g$ then f has n distinct roots in K.

(d) Suppose that $f \in F[x]$ is irreducible, so $F[x]/(f)$ is a field containing F. Show that f has a root in $F[x]/(f)$. Don't work hard.

Later in the term we will prove the following generalization of Fermat's little theorem, but for now we will take it as given:

Proposition. *In a field with q elements, every element α satisfies $\alpha^q = \alpha$.*

3. (30 points) Apply the results of problem 2 to the following situation: let $F = \mathbb{Z}_p$, let $f \in F[x]$ be an irreducible polynomial of degree n, let $K = F[x]/(f)$, let $q = p^n$, and let $g = x^q - x \in F[x]$.

(a) Show that $K = F[x]/(f)$ is a field with $q = p^n$ elements.

(b) Deduce that g has q distinct roots in K.

(c) Show that $f \mid g$ in $F[x]$.

(d) Now let K' be an arbitrary field with q elements. We saw in lecture that K' contains $F = \mathbb{Z}_p$. Show that f has n distinct roots in K'.

(e) Let $\alpha \in K'$ be a root of f, which we know exists by part (d). As usual let $\mathrm{ev}_\alpha\colon F[x] \to K'$ be the evaluation homomorphism $\mathrm{ev}_\alpha(h) = h(\alpha)$. Show that its kernel $\ker(\mathrm{ev}_\alpha) = (f)$. Conclude that its image $\mathrm{im}(\mathrm{ev}_\alpha) \subset K'$ is isomorphic to K.

(f) Argue that $\mathrm{im}(\mathrm{ev}_\alpha)$ is all of K', so $K \cong K'$.

Thus we have proved that if there is an irreducible polynomial $f \in \mathbb{Z}_p[x]$ of degree n then any two fields of $q = p^n$ elements are isomorphic. On Thursday we will prove that such an f exists for all p and n.

4. (30 points) Now we will work out what the previous problem means in an example. Let $K' = \mathbb{Z}[i]/(3)$.

(a) Show that the map $\varphi\colon K' \to K'$ defined by $\varphi(\alpha) = \alpha^3$ is a homomorphism. (It is called the *Frobenius automorphism* of K'.)

(b) Show that K' is a field.

(c) Show that the following nine elements of K' are distinct, and they account for all of K':

$$\begin{array}{ccc} \bar{0} & \bar{1} & \bar{2} \\ \bar{i} & \overline{1+i} & \overline{2+i} \\ \overline{2i} & \overline{1+2i} & \overline{2+2i} \end{array}$$

You may omit the bars if you like.

(d) For each of the nine elements α in part (c), calculate $\varphi(\alpha) = \alpha^3$. Conclude that φ is an isomorphism. Then calculate $\alpha^9 = (\alpha^3)^3$; your answer should agree with proposition given earlier.

(e) Consider the irreducible quadratics in $\mathbb{Z}_3[x]$:

$$f_1 = x^2 + 1 \qquad f_2 = x^2 + x + 2 \qquad f_3 = x^2 + 2x + 2$$

By problem 3(d), each one has two distinct roots in K'. Find them.

(f) We have seen in lecture that $K' = \mathbb{Z}[i]/(3)$ is isomorphic to $\mathbb{Z}_3[x]/(f_1)$. But the previous problem also yields isomorphisms from $\mathbb{Z}_3[x]/(f_2)$ and $\mathbb{Z}_3[x]/(f_3)$ to K'. Choose either f_2 or f_3 and one of its roots $\alpha \in K'$. Let $K = \mathbb{Z}_3[x]/(f_2)$ or $\mathbb{Z}_3[x]/(f_3)$ as appropriate, and describe explicitly the isomorphism from K to K' constructed in the previous problem; that is, where does the isomorphism send

$$\bar{0}, \bar{1}, \bar{2}, \overline{x}, \overline{x+1}, \overline{x+2}, \overline{2x}, \overline{2x+1}, \overline{2x+2} \in K?$$

Monic irreducible polynomials in $\mathbb{Z}_2[x]$:
Degree 2:

$$x^2 + x + 1$$

Degree 3:

$$x^3 + x + 1 \qquad\qquad x^3 + x^2 + 1$$

Degree 4:

$$x^4 + x + 1 \qquad x^4 + x^3 + 1 \qquad x^4 + x^3 + x^2 + x + 1$$

Monic irreducible polynomials $\mathbb{Z}_3[x]$:
Degree 2:

$$x^2 + 1 \qquad x^2 + x + 2 \qquad x^2 + 2x + 2$$

Degree 3:

$$\begin{array}{llll} x^3 + 2x + 1 & x^3 + 2x + 2 & x^3 + x^2 + 2 & x^3 + x^2 + x + 2 \\ x^3 + x^2 + 2x + 1 & x^3 + 2x^2 + 1 & x^3 + 2x^2 + x + 1 & x^3 + 2x^2 + 2x + 2 \end{array}$$

Degree 4:

$$\begin{array}{lll} x^4 + x + 2 & x^4 + 2x + 2 & x^4 + x^2 + 2 \\ x^4 + x^2 + x + 1 & x^4 + x^2 + 2x + 1 & x^4 + 2x^2 + 2 \\ x^4 + x^3 + 2 & x^4 + x^3 + 2x + 1 & x^4 + x^3 + x^2 + 1 \\ x^4 + x^3 + x^2 + x + 1 & x^4 + x^3 + x^2 + 2x + 2 & x^4 + x^3 + 2x^2 + 2x + 2 \\ x^4 + 2x^3 + 2 & x^4 + 2x^3 + x + 1 & x^4 + 2x^3 + x^2 + 1 \\ x^4 + 2x^3 + x^2 + x + 2 & x^4 + 2x^3 + x^2 + 2x + 1 & x^4 + 2x^3 + 2x^2 + x + 2 \end{array}$$