Solutions to Midterm Exam 2

Math 401

November 11, 2014

1. (20 points) Which of the following polynomials are irreducible in $\mathbb{Z}[x]$?

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

Solution: Reducible: 1 is a root.

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

Solution: Reducible: Factors as $(x^2 - 1)^2$.

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

Solution: Irreducible: Reduce mod 3 to get $x^4 + x^2 + 2$, which is on the list of irreducibles in $\mathbb{Z}_3[x]$.

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

Solution: Irreducible: Use Eisenstein's criterion with $p = 2$.

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.

Solution: Let $d \in F[x]$ be the greatest common divisor of f and g, and write $d(x) = a(x)f(x) + b(x)g(x)$ for some $a, b \in F[x]$. Then plugging in α we get $d(\alpha) = 0$, so $d \neq 1$.

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

Solution: Since f is irreducible, its only divisors are 1 and f. We have seen that $\gcd(f, g) \neq 1$; thus $\gcd(f, g) = f$, so $f \mid g$.

(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.

Solution: Since $f \mid g$ we can write $g = fh$ for some $h \in F[x]$. Every root of f is a root of g: that is, if $g(\alpha) = 0$ then $f(\alpha) = g(\alpha)h(\alpha) = 0$. Every root of g is either a root of f or a root of h: that is, if $f(\alpha) = g(\alpha)h(\alpha) = 0$ then $g(\alpha) = 0$ or $h(\alpha) = 0$. On the one hand, f has most n distinct roots because $\deg f = n$. But if f has $m < n$ distinct roots then h has $q - m > q - n$ distinct roots, which is impossible because $\deg h = q - n$ Thus f has exactly n distinct roots.

(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.

Solution: $\bar{x} \in F[x]/(f)$ is a root of f. You can just say this is obvious, or you can elaborate: if $f = a_n x^n + \cdots + a_1 x + 1$ then

$$\begin{aligned} f(\bar{x}) &= a_n \bar{x}^n + \cdots + a_1 \bar{x} + 1 \\ &= \overline{a_n x^n + \cdots + a_1 x + 1} \\ &= \bar{f} \\ &= 0. \end{aligned}$$

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.

Solution: K is a field because f is irreducible. There are two ways to show that it has p^n elements. We could say that it is a degree-n extension of $\mathbb{Z}_p$, hence is isomorphic as a $\mathbb{Z}_p$-vector space to $(\mathbb{Z}_p)^n$, hence has p^n elements. Alternatively we could say that any $h \in \mathbb{Z}_p[x]$ is congruent $\pmod f$ to a unique polynomial r with $\deg r < n$ (divide h by f and let r be the remainder), and there are p^n choices for the coefficients of such an r.

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

Solution: By the given proposition, every element of K is a root of g, and there are q distinct elements of K.

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

Solution: By problem2(d), f has a root in K. By the given proposition, every element of K is a root of g. Thus f and g have a common root in K. Since f is irreducible, by problem 2(b) we conclude that $f \mid g$.

(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'.

Solution: As part (b) we see that g has q distinct roots in K'. By part (c) we have $f \mid g$, so f has n distinct roots in K' by problem 2(c).

(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.

Solution: We have $\mathrm{ev}_\alpha(f) = f(\alpha) = 0$, so $f \in \ker(\mathrm{ev}_\alpha)$. We also have $\mathrm{ev}_\alpha(1) = 1 \neq 0$, so $1 \notin \ker(\mathrm{ev}_\alpha)$. Thus $\ker(\mathrm{ev}_\alpha)$ is a proper ideal containing an irreducible f, so it equals (f).

Now the fundamental homomorphism theorem (also called the first isomorphism theorem) states that $\mathrm{im}(\mathrm{ev}_\alpha) \cong F[x]/\ker(\mathrm{ev}_\alpha)$, and the latter is $F[x]/(f) = K$.

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

Solution: $\mathrm{im}(\mathrm{ev}_\alpha) \cong K$ has q elements by part (a), and it is contained in K' which has q elements, so $\mathrm{im}(\mathrm{ev}_\alpha) = K'$.

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'.)

Solution: Clearly $1^3 = 1$ and $(\alpha\beta)^3 = \alpha^3\beta^3$. By the binomial theorem we have

$$(\alpha + \beta)^3 = \alpha^3 + 3\alpha^2\beta + 3\alpha\beta^2 + \beta^3,$$

but $3 = 0$ in K', so the middle two terms drop out.

(b) Show that K' is a field.

Solution: We have seen that 3 cannot be written as a^2+b^2, and that this implies that it's irreducible in $\mathbb{Z}[i]$, so $\mathbb{Z}[i]/(3)$ is a field.

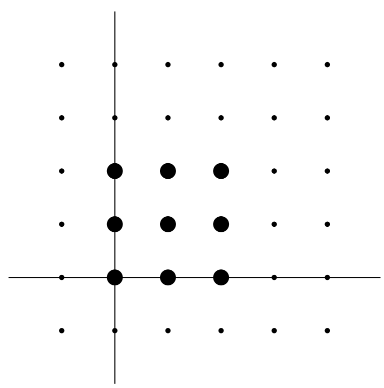
(If you want you can argue that if $a=b=1$ then $a^2+b^2=2$, but if $a \geq 2$ or $b \geq 2$ then $a^2+b^2 \geq 4$; thus there is now way to get 3. Thus if we could write $3 = zw$ for some non-units $z, w \in \mathbb{Z}[i]$ we would have $9 = |z|^2|w|^2$, so $|z|^2 = |w|^2 = 3$; then writing $z = a+bi$ we would have $|z|^2 = a^2+b^2$.)

(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.

Solution: We plot the points $0, 1, 2, i, 1+i, 2+i, 2i, 1+2i, 2+2i \in \mathbb{Z}[i]$:



Let α, β be any two of these nine. Then $|\alpha-\beta|^2 \leq 8$. But $\bar{\alpha} = \bar{\beta}$ if and only if $\alpha - \beta$ is a multiple of 3, which implies that $|\alpha-\beta|^2$ is a multiple of $|3|^2 = 9$. Thus if $\alpha \neq \beta$ then $\bar{\alpha} \neq \bar{\beta}$.

To see that these account for all of K', let $\overline{a+bi} \in K'$ be arbitrary; then a is congruent to 0, 1, or 2 (mod 3), and b is congruent to 0, 1, or 2 (mod 3), so $\overline{a+bi}$ equals one of these nine.

(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.

Solution: We have $0^3 = 0$, $1^3 = 1$, and $2^3 = 8 = 2$. Then $i^3 = -i = 2i$, so $(1+i)^3 = 1^3 + i^3 = 1 + 2i$ and $(2+i)^3 = 2^3 + i^3 = 2 + 2i$. Finally $(2i)^3 = 2^3 \cdot i^3 = 2 \cdot 2i = 4i = i$, so $(1+2i)^3 = 1^3 + (2i)^3 = 1 + i$ and $(2+2i)^3 = 2^3 + (2i)^3 = 2 + i$. In summary, φ acts as follows:

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

This is a bijection, so φ is an isomorphism.

Moreover we see that doing this twice takes us back to where we started, so $\alpha^9 = \varphi(\varphi(\alpha)) = \alpha$ for all $\alpha \in K'$.

(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.

Solution: The roots of f_1 in K' are $\bar{i}$ and $\overline{2i}$, the roots of f_2 are $\overline{1+i}$ and $\overline{1+2i}$, and the roots of f_3 are $\overline{2+i}$ and $\overline{2+2i}$. Observe that φ exchanges the roots of each f_i.

(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

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

Solution: If you choose f_2 and $\overline{1+i}$:

$$\begin{array}{ccccccccc} \bar{0} & \bar{1} & \bar{2} & \bar{x} & \overline{x+1} & \overline{x+2} & \overline{2x} & \overline{2x+1} & \overline{2x+2} \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ \bar{0} & \bar{1} & \bar{2} & \overline{1+i} & \overline{2+i} & \bar{i} & \overline{2+2i} & \overline{3+2i} & \overline{1+2i}. \end{array}$$

If you choose f_2 and $\overline{1+2i}$:

$$\begin{array}{ccccccccc} \bar{0} & \bar{1} & \bar{2} & \bar{x} & \overline{x+1} & \overline{x+2} & \overline{2x} & \overline{2x+1} & \overline{2x+2} \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ \bar{0} & \bar{1} & \bar{2} & \overline{1+2i} & \overline{2+2i} & \overline{2i} & \overline{2+i} & \overline{3+i} & \overline{1+i}. \end{array}$$

If you choose f_3 and $2+i$:

$$\begin{array}{ccccccccc}
\bar{0} & \bar{1} & \bar{2} & \overline{x} & \overline{x+1} & \overline{x+2} & \overline{2x} & \overline{2x+1} & \overline{2x+2} \\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\
\bar{0} & \bar{1} & \bar{2} & \overline{2+i} & \bar{i} & \overline{1+i} & \overline{1+2i} & \overline{2+2i} & \overline{2i}.
\end{array}$$

If you choose f_3 and $2+2i$:

$$\begin{array}{ccccccccc}
\bar{0} & \bar{1} & \bar{2} & \overline{x} & \overline{x+1} & \overline{x+2} & \overline{2x} & \overline{2x+1} & \overline{2x+2} \\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\
\bar{0} & \bar{1} & \bar{2} & \overline{2+2i} & \overline{2i} & \overline{1+2i} & \overline{1+i} & \overline{2+i} & \bar{i}.
\end{array}$$