Modern Algebra II: Problem Set 5

Nilay Kumar

Last updated: February 25, 2013

Problem 1

Let $f(x) = x^2+3x+2 = (x+1)(x+2) \in (\mathbb{Z}/6\mathbb{Z})[x]$. Note that $f(1) = 6 \equiv 0$, and so we can long divide $f(x)$ by $x-1$ to get $x+4$ with a remainder of $6 \equiv 0$. Thus, $-4 \equiv 2$ is another root of $f(x)$, and we can write

$$f(x) = (x-1)(x-2).$$

Problem 2

Let R be the subring $\mathbb{Z}[2] = \left\{a + b\sqrt{2} : a, b \in \mathbb{Z}\right\}$ of $\mathbb{R}$. Let $I = (6+\sqrt{2})$ be the principal ideal generated by $6+\sqrt{2}$. Similar to the last problem set, let us show that $\mathbb{Z} \cap I = 34\mathbb{Z}$. First we can show that $34\mathbb{Z} \subset \mathbb{Z} \cap I$. For some $n \in \mathbb{Z}$,

$$\frac{34n}{6+\sqrt{2}} \cdot \frac{6-\sqrt{2}}{6-\sqrt{2}} = n(6-\sqrt{2}),$$

which is in $(6+\sqrt{2})$, as $34n$ can be written as a $\mathbb{Z}\sqrt{2}$-multiple of $6+\sqrt{2}$. To show that $\mathbb{Z} \cap I \subset 34\mathbb{Z}$, we take some $n \in \mathbb{Z} \cap I$,

$$\frac{n}{6+\sqrt{2}} \cdot \frac{6-\sqrt{2}}{6-\sqrt{2}} = \frac{6n - n\sqrt{2}}{34},$$

and so $6n$ and n must be divisble by 34. Thus, $34|n$ and so $n \in 34\mathbb{Z}$ and $\mathbb{Z} \cap I = 34\mathbb{Z}$.

Now, by problem 6 on the last problem set, we know that there exists an injective homomorphism $f : \mathbb{Z}/34\mathbb{Z} \to \mathbb{Z}[\sqrt{2}]/(6+\sqrt{2})$ defined by $f(n + 34\mathbb{Z}) = n + (6+\sqrt{2})$. Note additionally, that since $\sqrt{2} \equiv -6 \mod I$, we have

$$a + b\sqrt{2} = a - 6b \mod I.$$

Thus, f is surjective (again by problem 6 of the last set), because for some $a + b\sqrt{2} \mod I = a - 6b$, we can take $n = a - 6b \in \mathbb{Z}$, and its (quotient) projection down to $\mathbb{Z}/34\mathbb{Z}$ will get sent to $a - 6b \in \mathbb{Z}[\sqrt{2}]/(6+\sqrt{2})$. Consequently, f is an isomorphism, and thus $\mathbb{Z}[\sqrt{2}]/(6+\sqrt{2}) \cong \mathbb{Z}/34\mathbb{Z}$. As $\mathbb{Z}/34\mathbb{Z}$ and $\mathbb{Z}[\sqrt{2}]/(6+\sqrt{2})$ are fields, it follows that $(6+\sqrt{2})$ is a maximal (and prime) ideal.

Problem 3

Let F be a field, and consider the ring (integral domain) $F[x]$.

(i) Let I be the principal ideal $(x - r)$ in $F[x]$. Every coset $p(x) + I \in F[x]/I$ contains a unique constant polynomial representative $a \in F$ (by what we showed about polynomial long division in class, since $x - r$ has degree 1), so $F[x]/I \subset F$. Of course, since $F \subset F[x]$, $F \subset F[x]/I$, so it is clear that $F[x]/I \cong F$. In fact, take the homomorphism $\phi : F \to F[x]/I$ defined by $\phi(a) = a + I$. It is injective, as only multiples of $x - r$ are sent to zero, but the only multiple of $x - r$ in F is 0. It is surjective as well, since for any $b + I \in F[x]/I$, $\phi(b) = b + I$. Consequently, ϕ is an isomorphism. This agrees with the fact that if $\mathrm{ev}_r : F[x] \to F$ is the evaluation homomorphism, then $I = \ker \mathrm{ev}_r$, so that $F[x]/I \cong \mathrm{Im}\ \mathrm{ev}_r = F$. Since F is a field, $F[x]/I$ is as well, and I must be a maximal ideal.

(ii) Let I be the principal ideal (x^2) in $F[x]$. Take any non-zero polynomial $p(x) \in F[x]$ (the zero case is trivial). By the long division algorithm, we we know that there exist unique $q(x), r(x)$ such that $p(x) = x^2 q(x) + r(x)$, where $\deg r(x) < 2$ (or $r(x) = 0$). In terms of cosets, we can write $p(x) = r(x) + I = a_0 + a_1 x + I$, where a_0, a_1 are unique. Consequently, every coset $p(x) + I$ contains a unique representative of the form $a_0 + a_1 x$, which we can write as $a_0 + a_1\alpha$, if we let $\alpha = x + I$. In this notation,

$$(a_0 + a_1\alpha) + (b_0 + b_1\alpha) = a_0 + b_0 + (a_1 + b_1)\alpha$$

by the distributive property, and for multiplication:

$$\begin{aligned}(a_0 + a_1\alpha) \cdot (b_0 + b_1\alpha) &= a_0 b_0 + (a_0 b_1 + a_1 b_0)\alpha + a_1 b_1 \alpha^2 \\ &= a_0 b_0 + (a_0 b_1 + a_1 b_0)\alpha + a_1 b_1 (x^2 + I) \\ &\equiv a_0 b_0 + (a_0 b_1 + a_1 b_0)\alpha \mod I\end{aligned}$$

Note that we have used the fact that $\alpha^2 = (x+I)^2$, which, by coset multiplication, is simply $x^2 + I \equiv 0 \mod I$. Thus, I is not a prime (maximal) ideal, as there exist elements not in I (namely, α) that when multiplied together, yield a member of I.

(iii) Let I be the principal ideal (x^2-1) in $F[x]$. Similar to above, take any non-zero polynomial $p(x) \in F[x]$. By the long division algorithm, we know that there exist unique $q(x), r(x)$ such that $p(x) = (x^2 - 1)q(x) + r(x)$, where $\deg r(x) < 2$ (or $r(x) = 0$). Thus we can write uniquely $p(x) = r(x) + I = a_0 + a_1 x + I$, or in terms of $\alpha = x + I$, $p(x) = a_0 + a_1\alpha$. In this notation,

$$(a_0 + a_1\alpha) + (b_0 + b_1\alpha) = a_0 + b_0 + (a_1 + b_1)\alpha$$

by the distributive property, and

$$\begin{aligned}(a_0 + a_1\alpha)\cdot(b_0 + b_1\alpha) &= a_0b_0 + (a_0b_1 + a_1b_0)\alpha + a_1b_1\alpha^2 \\ &= a_0b_0 + (a_0b_1 + a_1b_0)\alpha + a_1b_1x^2 \\ &= (a_0b_0 + a_1b_1) + (a_0b_1 + a_1b_0)\alpha,\end{aligned}$$

where we have used the fact that, in $F[x]/I$, $x^2 - 1 = 0$, so $\alpha^2 = x^2 = 1$. Still, I is not a prime (maximal) ideal, as we can take $x-1$ and $x+1$ not in I and multiply them to get and element of I:

$$(x-1)(x+1) = x^2 - 1 \equiv 0 \mod I$$

(iv) Continuing with $I = (x^2 - 1)$, and now assuming that F is not of characteristic 2, we consider the ring homomorphism $F[x] \to F \times F$ defined by $p(x) \mapsto (p(1), p(-1))$. In other words, we consider the homomorphism $(\mathrm{ev}_1, \mathrm{ev}_{-1})$. First note that any element $f(x) = (x^2 - 1)g(x) \in I$, with $g(x) \in F[x]$, is sent to $(0,0)$ in the product ring:

$$(x^2-1)g(x) \mapsto (0\cdot g(1), 0\cdot g(-1)) = (0,0),$$

so $I \subset \ker \mathrm{ev}_1$ and $I \subset \ker \mathrm{ev}_{-1}$. Now, if we define $\phi : F[x]/I \to F \times F$, such that $\phi(p(x) + I) = (p(1), p(-1))$, then ϕ is a homomorphism (considering $F \times F$ as a product ring):

$$\begin{aligned}\phi(p+I+q+I) =&((p+I+q+I)(1), (p+I+q+I)(-1)) \\ =&(p(1)+q(1), p(-1)+q(-1)) = \phi(p+I) + \phi(q+I) \\ \phi((p+I)(q+I)) =&((p+I)(q+I)(1), (p+I)(q+I)(-1)) \\ =&(p(1)q(1), p(-1)q(-1)) = \phi(p+I)\phi(q+I) \\ \phi(0+I) =&(0,0) \\ \phi(1+I) =&(1,1).\end{aligned}$$

Note also that

$$\phi(\alpha) = \phi(x + I) = (1, -1).$$

To find elements that get mapped to $(0,1)$ and $(1,0)$, let us take

$$\phi(a_0 + a_1\alpha + I) = (a_0 + a_1, a_0 - a_1) = (1,0)$$
$$\phi(b_0 + b_1\alpha + I) = (b_0 + b_1, b_0 - b_1) = (0,1).$$

One solution to this system is $1/2 + \alpha/2$ and $1/2 - \alpha/2$ respectively. Here, in using $1/2$, we have used the fact that the field is not of characteristic. It follows immediately that ϕ is surjective, for we have, in some sense created a basis for $F \times F$: $(a, b) = a(1, 0) + b(0, 1) = \phi(a(1/2 + \alpha/2) + b(1/2 - \alpha/2) + I)$.

We already know that $I \subset \ker \phi$. It is clear that $\ker \phi \subset I$ using the formula for (a, b) that we just derived:

$$(0,0) = \phi(0 + I).$$

Hence, since the homomorphism ϕ is both injective and surjective, it is an isomorphism from $F[x]/I$ to $F \times F$.

Problem 4

Let F be an infinite field, and let $E : F[x] \to F^F$ be the homomorphism from polynomials with coefficients in F to the ring of all functions from F to F. Take any polynomial $p \in \ker E$, i.e. polynomials for which $E(p) = 0$. However, since a non-zero polynomial can never be zero on infinitely many elements of F, $p \equiv 0$, the zero polynomial. Consequently, $\ker E = \{0\}$, and E is injective. It follows similarly that E is not surjective – take the function $f \in F^F$ that takes all but one element of F to zero. By the above logic, there is no polynomial that corresponds to this function, and thus E cannot be surjective.

Now let $F = \{a_1 \cdots a_n\}$ be a finite field, with E defined identically as above. The ring of functions F^F, must now be finite, since F is finite. Then, since E is mapping elements of an infinite field $F[x]$ to elements of a finite one, E cannot be injective.

To see that E must be surjective, let

$$q_i(x) = \prod_{j \neq i}(x - a_j)$$
$$p_i(x) = \frac{q_i(x)}{q_i(a_i)}.$$

$p_i(x) \in F[x]$ has the property that it evaluates to zero for all members of F, except for a_i, at which it evaluates to unity. Any function $f \in F^F$ is specified by its action on the elements of F: let $f(a_i) = c_i$. Then we can write

$$f(x) = \sum_{i=1}^{n} c_i p_i(x),$$

because for some $x \in F$, every term will vanish except for the p_i that corresponds to x, which will yields $c_i \cdot 1 = c_i$, as desired. Hence, E is surjective.