Math 120 Homework 7 Solutions

May 29, 2008

p. 230

11.) By the distributive law, $(x+1)(x-1) = x(x-1)+(x-1) = x^2-x+x-1 = x^2-1 = 0$. Since R does not contain zero dividers, one of $x+1$ or $x-1$ is zero so $x = \pm 1$.

13.) a. We have $\overline{ab}^k = \overline{a^k b^k}$ since $\mathbb{Z}/n\mathbb{Z}$ is commutative. But $\overline{a^k b^k} = \overline{a^k b b^{k-1}} = \overline{0}\overline{b^{k-1}} = \overline{0}$ and hence $\overline{ab}$ is nilpotent.

b. Let $n = p_1^{e_1} \dots p_k^{e_k}$ with each $e_i \geq 1$ and suppose $a = p_1^{f_1} \dots p_k^{f_k} m$ with each $f_k \geq 1$. Let $e = \max e_i$. Then $a^e = p_1^{ef_1} \dots p_k^{ef_k} m^e$ is divisible by n since $e_i \leq ef_i$ for each i, i.e. because $e \geq e_i$ and $f_i \geq 1$. Thus $\overline{a^e} = \overline{a}^e = 0$ and $\overline{a}$ is nilpotent.

On the other hand, suppose that prime p divides n but p does not divide a. Then p does not divide a^e for any $e \geq 1$ and so n does not divide a^e for any $e \geq 1$, so $\overline{a}^e = \overline{a^e} \neq \overline{0}$ for all e, and $\overline{a}$ is not nilpotent. Since $72 = 2^3 \times 3^2$, the nilpotent elements are (the reductions mod 72) of those $0 \leq a < 72$ that are divisible by 6.

c. Suppose $f : X \to F$ satisfies $f^m = 0$. Then $f^m(x) = f(x)^m = 0$ for all x. For any given x, let m_x be the minimal power of $f(x)$ for which $f(x) = 0$. For each x, m_x exists and $m_x < m$ since $f(x)^m = 0$. If $m_x > 1$ then $f(x)f^{m_x-1}(x) = f^{m_x}(x) = 0$ which implies $f(x) = 0$ or $f^{m_x-1}(x) = 0$ since fields don't have zero divisors. But this contradicts the minimality of m_x so we must have $m_x = 1$. Hence $f(x) = 0$ for all x and $f = 0$.

29.) We first check that as defined, $(R, +)$ is an abelian group. Let f_1, f_2 be two homomorphisms $A \to A$. Let $x, y \in A$. Then

$$(f_1 + f_2)(x + y) = f_1(x + y) + f_2(x + y) = f_1(x) + f_1(y) + f_2(x) + f_2(y).$$

We can regroup these terms because A is an abelian group under addition, to arrive at

$$f_1(x) + f_2(x) + f_1(y) + f_2(y) = (f_1 + f_2)(x) + (f_1 + f_2)(y),$$

that is, $f_1 + f_2$ is indeed a group homomorphism of $(A, +)$.

To check that $+$ is associative in R, note that

$$((f_1 + f_2) + f_3)(x) = (f_1 + f_2)(x) + f_3(x) = (f_1(x) + f_2(x)) + f_3(x)$$

which is equal to

$$f_1(x) + (f_2(x) + f_3(x)) = (f_1 + (f_2 + f_3))(x)$$

because addition in A is associative. That addition in R is commutative follows similarly:

$$(f_1 + f_2)(x) = f_1(x) + f_2(x) = f_2(x) + f_1(x) = (f_2 + f_1)(x).$$

The additive identity of R is the map $0(x) = 0$ for all x. Trivially $f + 0 = 0 + f = f$ for all f. The additive inverse of f is the homomorphism $(-f)(x) = -f(x)$ for all x. That this is a homomorphism follows by

$$(-f)(x+y) = -f(x+y) = -(f(x) + f(y)) = -f(x) - f(y) = (-f)(x) + (-f)(y).$$

It is indeed the additive inverse of f because $(f + (-f))(x) = f(x) - f(x) = 0$ for all x (we already checked that $R, +$ is commutative so $(-f)$ is also a left inverse). Thus we have checked all the axioms required to show that $(R, +)$ is an abelian group.

We know that the composition of two group homomorphisms is again a group homomorphism, so the multiplication on R is well defined. Associativity of products follows from associativity of function composition. To check the distributive laws, let $f_1, f_2, f_3 \in R$. Then $(f_1 + f_2)f_3(x) = f_1(f_3(x)) + f_2(f_3(x))$ which implies $(f_1 + f_2)f_3 = f_1f_3 + f_2f_3$. Again $f_1(f_2 + f_3)(x) = f_1(f_2(x) + f_3(x)) = f_1(f_2(x)) + f_1(f_3(x))$ because f_1 is a group homomorphism. But then this implies $f_1(f_2 + f_3) = f_1f_2 + f_1f_3$. Thus we've checked that R is a ring.

The unit in R is the identity homomorphism $1(x) = x$ for all x. Indeed, $f(1(x)) = f(x)$ and $1(f(x)) = f(x)$ so $f1 = 1f = f$.

Let f be an automorphism of A. Then f has an inverse automorphism f^{-1} such that $ff^{-1}(x) = f^{-1}f(x) = x$, that is $ff^{-1} = f^{-1}f = 1$ and so f is a unit. On the other hand, if f is a unit, then there exists homomorphism g such that $fg(x) = gf(x) = x$ for all x. In particular, this implies that f has g as a set-theoretic inverse, so f must be a bijection $A \to A$, which proves that f is an automorphism.

p. 247

10.) In each case, call the subset in question I. Since $\mathbb{Z}[x]$ is commutative, it suffices to check whether I is a left ideal.

a. This is an ideal. It is non-empty because it contains 3. If $P(x)$ and $Q(x)$ have constant terms $3a$ and $3b$, then the constant term of $P - Q$ is $3(a - b)$, which is a multiple of 3, so that I satisfies the subgroup criterion for the additive group $\mathbb{Z}[x]$. Then if $R(x) \in Z[x]$ has constant term c, we get $R(x)P(x)$ has constant term $3ac$ so $RP \in I$ and I is a left ideal.

b. This is not an ideal because it is not closed under multiplication on the left: $x(3x^2 + x) = 3x^3 + x^2 \notin I$.

c. This is an ideal. I is non-empty since $x^3 \in I$. The difference of two such polynomials also has no constant, linear or quadratic term, hence also is in I, so that I is an additive subgroup. If $P(x) \in I$ and $Q(x) \in \mathbb{Z}[x]$ then $P(x) = x^3P'(x)$ for another polynomial $P'(x)$. We get $Q(x)P(x) = x^3Q(x)P'(x)$, so $Q(x)P'(x)$ also has no constant, linear, or quadratic term. Thus $\mathbb{Z}[x]I \subset I$.

d. This is not an ideal because it is not closed under multiplication on the left: $x(1) = x \notin I$ even though $1 \in I$ and $x \in \mathbb{Z}[x]$.

e. This is an ideal. The condition is equivalent to $\{P : P(1) = 0\}$. This is not empty since it contains $x - 1$. Clearly if $P(1) = Q(1) = 0$ then $(P - Q)(1) = P(1) - Q(1) = 0$ so this is an additive subgroup. Also if $P(1) = 0$ and $R \in \mathbb{Z}[x]$ then $RP(1) = R(1)P(1) = 0$ so $RP \in I$ which proves that I is an ideal.

f. This is not an ideal. The condition is the same as that p should have vanishing linear term. This is not closed under multiplication on the left, since $x \in \mathbb{Z}[x]$, $1 \in I$ and $x1 = x \notin I$.

26.) a. Let ϕ be the map. We have ϕ is an additive group homomorphism because it is the usual homomorphism from $\mathbb{Z}$ to the cyclic group generated by an element, (in this case, 1 in R). To check that $\phi(ab) = \phi(a)\phi(b)$ apply the distributive law and observe that $|ab|$ terms will result, each having the appropriate sign. If the characteristic n of R is finite, the kernel of our map clearly contains n, since $\phi(n)$ is the sum of n 1's which is 0. Since the kernel is a subgroup of $\mathbb{Z}$ containing n, it must have form $r\mathbb{Z}$ for $r > 0$ dividing n. But then we get $r \geq n$ or else $\phi(r) = 0$ implies r sums of 1 is zero, which would contradict the minimality of n. This proves that the kernel is $n\mathbb{Z}$. On the other hand, if R has characteristic 0 then for each $n \in \mathbb{Z}$, $n > 0$, $\phi(n) \neq 0$ so $n \notin \ker \phi$ which implies $\ker \phi = 0\mathbb{Z}$ as desired.

b. The map ϕ maps $\mathbb{Z}$ to itself (viewed as a subring of $\mathbb{Q}$) isomorphically, so the kernel is trivial and $\mathbb{Q}$ has characteristic 0. In $\mathbb{Z}[x]$, ϕ also maps $\mathbb{Z}$ to itself isomorphically, this time with $\mathbb{Z}$ identified with the constant polynomials. It follows that $\mathbb{Z}[x]$ has characteristic 0. In $\mathbb{Z}/n\mathbb{Z}[x]$, $\phi(n) = \overline{0}$ while for any $0 < m < n$, $\overline{m} \neq \overline{0}$ (i.e. m is not divisible by n). Thus the characteristic of $\mathbb{Z}/n\mathbb{Z}[x]$ is n.

c. We make use of the binomial theorem $(a+b)^n = \sum_{j=0}^{n} \binom{n}{j} a^j b^{n-j}$ where $\binom{n}{j}$ is the sum of $\binom{n}{j}$ 1's in R. This could be proven e.g. by induction on n. Note that if $n = p$, a prime, and $j \neq 0, p$ then $\binom{p}{j} = \frac{p!}{j!(p-j)!}$ is divisible by p, since the numerator is while the denominator is not. Thus if R has characteristic p, then viewed as an element of R, $\binom{p}{j} = 0$ for $j \neq 0, p$. It follows that if R has characteristic p, then

$$(a+b)^p = \sum_{j=0}^{p} \binom{p}{j} a^j b^{p-j} = a^p + b^p$$

since all other terms are multiplied by 0.