Problem Set 8 Solutions

Math 120

7.1.1 This just follows from the distributive law in R:

$$-1+1=0 \Rightarrow (-1)(-1+1)=0 \Rightarrow (-1)^2-1=0 \Rightarrow (-1)^2=1.$$

7.1.5 (a) The set of all rational numbers with odd denominators is indeed a subring of $\mathbb{Q}$ since it is easily seen to be a subgroup of $\mathbb{Q}$ (under addition, of course), and it is obviously closed under multiplication.

(b) The set of all rational numbers with even denominators is not a subring of $\mathbb{Q}$ since it is not closed under addition and therefore not a subgroup. For example, $1/6+1/6=1/3$.

(c) The set of nonnegative rational numbers is not a subring of $\mathbb{Q}$ because it is not closed under inversion (in the group $(\mathbb{Q},+)$).

(d) The set of squares of rational numbers is not a subring of $\mathbb{Q}$ because it is not closed under addition and therefore not a subgroup. For example, $4/9+1/9=5/9$.

(e) The set of rational numbers with odd numerators is not a subring of $\mathbb{Q}$ because it is not closed under addition. For example, $3/5+1/5=4/5$.

(f) The set of all rational numbers with even numerators is easily checked to be a subgroup of $\mathbb{Q}$ and closed under multiplication, so it is therefore a subring.

7.1.11 We have $x^2=1 \Rightarrow (x-1)(x+1)=0$ as usual by the distributive law. Since R is an integral domain this implies either $x-1=0$ or $x+1=0$, proving the claim.

7.1.12 A field is commutative, and therefore any subring is commutative. Moreover, since a field has no zero divisors (as it is a division ring), neither do its subrings. Hence any subring is a commutative division ring, so if it contains the identity it is an integral domain.

7.1.13 (a) We have $(\overline{ab})^k=\overline{a}^k\overline{b}^k=(\overline{a}^k\overline{b})\overline{b}^{k-1}=\overline{n}\overline{b}^{k-1}=0$, so $\overline{ab}$ is nilpotent in $\mathbb{Z}/n\mathbb{Z}$.

(b) First suppose every prime divisor of n is also a prime divisor of a. Say $n=p_1^{r_1}\dots p_k^{r_k}$ and $a=p_1^{s_1}\dots p_k^{s_k}p_{k+1}^{s_{k+1}}\dots p_l^{s_l}$ where the p_i are all distinct primes. Then there is some N such that $Ns_i>r_i$ for all $i=1,...,k$, and hence a^N is a multiple of n and therefore $\overline{a}^N=0\in\mathbb{Z}/n\mathbb{Z}$. On the other hand, if $\overline{a}$ is nilpotent, then a^N is a multiple of n for some N. Since a^N has precisely the same set of prime divisors as a, every prime divisor of n must also divide a. In particular, since

72 has prime factorization $2^3 3^2$, the only nilpotent elements in $\mathbb{Z}/72\mathbb{Z}$ are those $\overline{a}$ such that a is a multiple of 6 (for any representative choice of a).

(c) Let φ be a nonzero element of R. Then there exists some $x \in X$ such that $\varphi(x) \neq 0$. But $\varphi(x)$ is a nonzero element of a field, which has no zero divisors, and so $\varphi(x)^k$ is nonzero for all k. Hence φ^k is nonzero for all k and thus φ is not nilpotent.

7.2.1 (a) $p(x) + q(x) = 9x^3 - 3x^2 + 37x - 9$ and $p(x)q(x) = 14x^6 - 21x^5 + 94x^4 - 142x^3 + 144x^2 - 181x + 20$.

(b) $p(x) + q(x) = x^3 + x^2 + x + 1$ and $p(x)q(x) = x^5 + x$. When comparing these answers to yours, remember that in $\mathbb{Z}/2\mathbb{Z}$, $1 = -1$.

(c) $p(x) + q(x) = x$ and $p(x)q(x) = 2x^6 + x^4 + 2x^3 + 2x + 2$.

7.3.1 Suppose there exists a ring isomorphism $\varphi : 2\mathbb{Z} \to 3\mathbb{Z}$. Then $\varphi(0) = 0$ and $\varphi(2) = 3n$ for some nonzero integer n. But then $6n = \varphi(2 + 2) = \varphi(2 \times 2) = 9n^2$, and this equation has no nonzero integer solutions. This contradiction proves that no such isomorphism exists.

7.3.2 Suppose we had an isomorphism $\varphi : \mathbb{Q}[x] \to \mathbb{Z}[x]$. Now both of these rings have an identity element, so if $p \in \mathbb{Q}[x]$ is any nonzero polynomial we have $\varphi(p) = \varphi(1 \cdot p) = \varphi(1)\varphi(p) \Rightarrow \varphi(p)(\varphi(1) - 1) = 0$. Since $\mathbb{Z}[x]$ is an integral domain, this implies $\varphi(1) = 1$. Now as $1/2 + 1/2 = 1$, we must have $\varphi(1/2) + \varphi(1/2) = 1$. Since this equation has no solutions in $\mathbb{Z}[x]$, we have a contradiction. Hence $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$ are not isomorphic.

7.3.6 (a) The given map $\varphi : M_2(\mathbb{Z}) \to \mathbb{Z}$ is not a ring homomorphism, for consider the matrices $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $B = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$ where $b, g \neq 0$. We have

$$AB = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{pmatrix}$$

and hence $\varphi(AB) = ae + bg \neq ae = \varphi(A)\varphi(B)$.

(b) We see that the trace of AB is given by $ae + bg + cf + dh$, which is not, in general, the product of the traces of A and B. Hence the given map is not a ring homomorphism.

(c) The determinant map is also not a ring homomorphism since, for example, $\det(I + I) = 4 \neq 2 = \det(I) + \det(I)$.

7.3.10 (a) The set of all polynomials whose constant term is a multiple of 3 is an ideal in $\mathbb{Z}[x]$. It is closed under addition, and the product of any polynomial in $\mathbb{Z}[x]$ and one of this subset will have constant term a multiple of 3.

(b) The set of all polynomials whose coefficient of x^2 is a multiple of 3 is not an ideal in $\mathbb{Z}[x]$, for although $3x^2 + 2x$ belongs to this set, $3x^3 + 2x^2 = x(3x^2 + 2x)$ does not.

(c) The set of all polynomials whose constant term, coefficient of x, and coefficient of x^2 are all zero does represent an ideal in $\mathbb{Z}[x]$. It is easily seen to be a subring of $\mathbb{Z}[x]$, and the product of any polynomial with a polynomial in this subset will also have 0 as the coefficient of its constant, x, and x^2 terms.

(d) $\mathbb{Z}[x^2]$ is not an ideal in $\mathbb{Z}[x]$, for while the polynomial x^2 belongs to this set, $x^3 = xx^2$ does not.

(e) The set of polynomials whose coefficients sum to zero is an ideal in $\mathbb{Z}[x]$. It is easily checked to be closed under addition. Moreover, suppose $p(x) = a_n x^n + \cdots + a_1 x + a_0$ lies in this set. Then clearly $cx^k p(x)$ also lies in this set for all $c \in \mathbb{Z}$ and $k \in \mathbb{Z}^+$. But if $r(x) = b_m x^m + \cdots + b_1 x + b_0$ is any polynomial in $\mathbb{Z}[x]$, the sum of the coefficients of $r(x)p(x)$ is just the sum of the sums of coefficients in $b_k x^k p(x)$, which are all zero. This set is thus closed under multiplication by any element in $\mathbb{Z}[x]$.

(f) The set of all polynomials p satisfying $p'(0) = 0$ is not an ideal in $\mathbb{Z}[x]$ since it is not closed under left multiplication by elements in $\mathbb{Z}[x]$. For example, the constant polynomial 1 lies in this set, but the polynomial $x = x \cdot 1$ does not.

7.4.8 First suppose $a = ub$ for some unit u. Then if v is a unit such that $vu = 1$, for any $r \in R$, we have $rb = rva \in (a)$ and so $(b) \subset (a)$. Since $va = b$, the exact same argument shows that $(a) \subset (b)$ and so $(a) = (b)$. Conversely, if $(a) = (b)$, then there is some $r \in R$ such $a = rb$ and some $s \in R$ such that $b = sa$. Therefore $a = rb = rsa \Rightarrow a(1 - rs) = 0$. If a is nonzero, then since R is an integral domain we must have $rs = 1$ and hence r is a unit. If $a = 0$, we clearly must have $b = 0$ so we can take $u = 1$ in the claim and we are finished.

7.4.15 (a) 0, 1, x, and $x + 1$ are the only four degree < 1 polynomials in $\mathbb{F}_2[x]$. Moreover, in the quotient ring $\mathbb{F}_2[x]/(x^2 + x + 1)$ we may use the relation $\overline{x}^2 = \overline{x} + \overline{1}$ to write the equivalence class of all higher degree polynomials in $\mathbb{F}_2[x]$ as the equivalence classes of a degree < 1 polynomial. Since there are four of these, $\overline{E}$ has at most four elements. However, the equivalence class of any two distinct degree < 1 polynomials in $\mathbb{F}_2[x]$ are distinct in $\overline{E}$ since the difference of two such polynomials cannot possibly be a multiple of the degree two polynomial $x^2 + x + 1$.

(b) This is straightforward: the element $\overline{0}$ is the identity element, each element has additive order 2, and adding two distinct non-identity elements gives the third.

(c) Writing out the multiplication table for $\overline{E}$, we see that $\overline{E}$ has no zero divisors, so $\overline{E}^\times$ has order three and is thus cyclic. In particular, $\overline{x}^2 = \overline{x} + \overline{1}$ and $\overline{x}^3 = \overline{x}\overline{x}^2 = \overline{x}^2 + \overline{x} = 1$, so each nonzero element of $\overline{E}$ is a unit.

7.6.3 This is just a consequence of how the operations in the ring direct product are defined. Let $\mathcal{I}$ be an ideal in $R \times S$, and define I to be the set of all $r \in R$ such that there is some

$s \in S$ such that $(r, s) \in \mathcal{I}$. I is closed under addition, for if $r_1, r_2 \in I$, and s_1, s_2 are elements in S such that $(r_1, s_1), (r_2, s_2) \in \mathcal{I}$, we have $(r_1 + r_2, s_1 + s_2) \in \mathcal{I} \Rightarrow r_1 + r_2 \in I$. I is also closed under left multiplication since $\mathcal{I}$ is. Hence I is an ideal of R. If we similarly define J to be those elements $s \in S$ such that there is some $r \in R$ such that $(r, s) \in \mathcal{I}$, we also find that J is an ideal in S. Then by construction, clearly $(r, s) \in \mathcal{I} \Rightarrow (r, s) \in I \times J$, so $\mathcal{I} \subset I \times J$. On the other hand, suppose $(r, s) \in I \times J$. Then there exists $r' \in R$ and $s' \in S$ such that $(r', s), (r, s') \in \mathcal{I}$. But $\mathcal{I}$ is an ideal in $R \times S$, and thus closed under left multiplication. Hence $(0, 1)(r', s) = (0, s) \in \mathcal{I}$ and $(0, 1)(r, s') = (0, s') \in \mathcal{I}$. Therefore $(0, s) - (0, s') = (0, s - s') \in \mathcal{I}$, and so $(r, s') + (0, s - s') = (r, s) \in \mathcal{I}$, so we conclude $I \times J \in \mathcal{I}$ and hence $I \times J = \mathcal{I}$, proving the assertion. Notice the importance of the condition that R and S have indentities.