HONORS ALGEBRA: SOLUTIONS TO HOMEWORK 11

4.2, Q8. (a) If F is a finite field, say $|F| = n$, we have $n \geq 2$ since $1 \neq 0$. Let p be any prime divisor of n. Then as an additive group, we see by Cauchy's theorem that F contains a non-zero element a of order p, and we have $pa = 0$. But F is a field, so there is an element $a^{-1} \in F$ with $aa^{-1} = 1$. Thus, given any $b \in F \setminus \{0\}$, we have $pb = (pa)(a^{-1}b) = 0$. Since $p0 = 0$, it follows that $pb = 0$ for all $b \in F$.
(b) Suppose that F has q elements. Suppose, by way of deriving a contradiction, that q is divisible by two distinct primes p_1 and p_2. Then for all $a \in F \setminus \{0\}$, we have $p_1 a = 0 = p_2 a$, whence $(p_1, p_2)a = 0$. But $(p_1, p_2) = 1$, and we deduce that $a = 0$. This yields a contradiction, and so q is divisible by only one prime, say p, and consequently $q = p^n$ for some $n \in \mathbb{N}$.

4.3, Q1. Since $0 \in L(a)$, the set $L(a)$ is non-empty. Given $x, y \in L(a)$, moreover, one has $xa = 0$ and $ya = 0$, and hence $(x - y)a = xa - ya = 0$, so that $x - y \in L(a)$. Thus $L(a)$ is an additive subgroup of R, by the subgroup criterion. Finally, whenever $r \in R$ and $x \in L(a)$, using the commutativity of R, we have $(rx)a = r(xa) = r0 = 0$, so that $rx \in R$, and also $xr = rx \in R$. Thus $L(a)$ is an ideal of R.

4.3, Q2. If $R = \{0, 1\}$, then R is trivially a field. Suppose then that R contains an element a distinct from 0 and 1. Then $(a) = \{xa : x \in R\}$ is an ideal of R. If R contains no ideals other than (0) and R, then since $a = 1a \in (a)$, we have $(a) = R$. But then $1 \in (a)$, and there is an element $b \in R$ for which $ba = 1$. Since this implies, by commutativity, that for each $a \in R \setminus \{0\}$ there exists $b \in R$ with $ab = 1 = ba$, it follows that R is a field.

4.3, Q3. Since φ is surjective, given $b \in R'$ there exists $a \in R$ with $\varphi(a) = b$. The homomorphism property of φ then shows that $\varphi(1)b = \varphi(1)\varphi(a) = \varphi(1a) = \varphi(a) = b$ and similarly $b\varphi(1) = \varphi(a)\varphi(1) = \varphi(a1) = \varphi(a) = b$. Since this relation holds for all $b \in R'$, we see that $\varphi(1)$ does indeed serve as the unit element of R'.

4.3, Q4. If $a, b \in I + J$, then $a = i_1 + j_1$ and $b = i_2 + j_2$ for some $i_1, i_2 \in I$ and $j_1, j_2 \in J$. Since I and J are both ideals of R, and hence are additive subgroups of R, we see that $i_1 - i_2 \in I$ and $j_1 - j_2 \in J$, so that $a - b = (i_1 - i_2) + (j_1 - j_2) \in I + J$. Also, we have $0 \in I + J$, so it follows that $I + J$ is an additive subgroup of R by the subgroup criterion. Moreover, given any $a \in I + J$, we have $a = i + j$ for some $i \in I$ and $j \in J$. Since I and J are ideals, it follows that for all $r \in R$ we have $ri \in I$ and $rj \in J$, and hence $ra = r(i+j) = ri + rj \in I + J$. Similarly, we have $ar = (i+j)r = ir + jr \in I + J$. Thus we conclude that $I + J$ is an ideal of R.

4.3, Q18. The set $R \oplus S$ equipped with coordinatewise addition is the external direct product of the abelian additive groups of R and S, so is automatically an abelian additive group with identity element (zero) $(0, 0)$. Coordinatewise multiplication is closed and associative in $R \oplus S$, since multiplication is closed and associative in R and in S, owing to their ring properties. It remains to check that $R \oplus S$ satisfies the distributive properties, but again these are inherited from the corresponding properties of R and S, since addition and multiplication on $R \oplus S$ are defined coordinatewise.

Next, define $\varphi : R \oplus S \to R$ by taking $\varphi((r,s)) = r$ for each $(r,s) \in R \oplus S$. The map φ is well-defined, and satisfies the homomorphism property on the corresponding additive groups, since the additive group of $R \oplus S$ is the external direct product of R and S. For each (r_1, s_1) and (r_2, s_2) lying in $R \oplus S$, moreover, one has $\varphi((r_1,s_1)(r_2,s_2)) = \varphi((r_1r_2, s_1s_2)) = r_1r_2 = \varphi((r_1,s_1))\varphi((r_2,s_2))$, so that φ satisfies the multiplicative homomorphism property. Then φ is a homomorphism of rings that is self-evidently surjective. We have $\ker(\varphi) = \{(0,s) : s \in S\}$, and since φ is a homomorphism, we have $\ker(\varphi) \lhd R \oplus S$. Thus $\{(0,s) : s \in S\}$ is an ideal of $R \oplus S$. Defining $\psi : R \oplus S \to S$ by taking $\psi((r,s)) = s$ for each $(r,s) \in R \oplus S$, we find in symmetrical manner that $\ker(\psi) \lhd R \oplus S$, whence $\{(r,0) : r \in R\}$ is an ideal of $R \oplus S$. The restriction mapping $\varphi' : R \oplus 0 \to R$ defined by taking $\varphi'((r,0)) = r$ inherits the surjective homomorphism properties of φ, and is injective because $\varphi'(r_1) = \varphi'(r_2)$ if and only if $r_1 = r_2$, and this holds if and only if $(r_1, 0) = (r_2, 0)$. Thus φ' is an isomorphism, and $\{(r,0) : r \in R\}$ is isomorphic to R. A symmetrical argument shows that $\{(0,s) : s \in S\}$ is isomorphic to S.

4.3, Q20. Suppose that $I \lhd R$ and $J \lhd R$, and put $R_1 = R/I$ and $R_2 = R/J$. Define $\varphi : R \to R_1 \oplus R_2$ by taking $\varphi(r) = (r+I, r+J)$. Then for all $r, s \in R$, one has $\varphi(r+s) = (r+s+I, r+s+J) = (r+I, r+J) + (s+I, s+J) = \varphi(r) + \varphi(s)$ and $\varphi(rs) = (rs+I, rs+J) = (r+I, r+J)(s+I, s+J) = \varphi(r)\varphi(s)$. Then φ is a homomorphism of rings. Moreover, one has $\ker(\varphi) = \{r \in R : (r+I, r+J) = (I, J)\} = \{r \in R : r \in I \text{ and } r \in J\} = I \cap J$.

4.3, Q21. Consider the ideals $I = (3)$ and $J = (5)$ of $R = \mathbb{Z}_{15}$. One has $R_1 = R/I = \mathbb{Z}_{15}/(3) \cong \mathbb{Z}_3$ and $R_2 = R/J = \mathbb{Z}_{15}/(5) \cong \mathbb{Z}_5$. Define the map φ as in Q20, and note that $\ker(\varphi) = I \cap J = (3) \cap (5) = \{0\}$, so that φ is injective. Since $\text{card}(R_1 \oplus R_2) = |R_1| \cdot |R_2| = 3 \cdot 5 = \text{card}(R)$, we see that φ is also surjective and hence is an isomorphism. Then we conclude in this case that $R \cong R_1 \oplus R_2$, which is to say that $\mathbb{Z}_{15} \cong \mathbb{Z}_3 \oplus \mathbb{Z}_5$.

4.3, Q22. (a) We have $I_m \cap I_n = \{x \in \mathbb{Z} : m|x \text{ and } n|x\}$. Since $(m,n) = 1$, it follows that whenever $m|x$ and $n|x$, then $mn|x$, so we have $I_m \cap I_n = I_{mn}$.
(b) Put $R = \mathbb{Z}$, and then take $I = I_m$ and $J = I_n$, and define the map φ as in Q20. We see that φ is a homomorphism of rings and $\ker(\varphi) = I_m \cap I_n = I_{mn}$. Thus, from the First Homomorphism Theorem, we see that $\mathbb{Z}/I_{mn} = \mathbb{Z}/\ker(\varphi) \cong \text{Im}(\varphi) \subseteq \mathbb{Z}/I_m \oplus \mathbb{Z}/I_n$. Thus, indeed, there is an injective homomorphism from $\mathbb{Z}/I_{mn}$ into $\mathbb{Z}/I_m \oplus \mathbb{Z}/I_n$.

4.3, Q23. In Q22(b) we see that there is an injective homomorphism $\psi : \mathbb{Z}/I_{mn} \to \mathbb{Z}/I_m \oplus \mathbb{Z}/I_n$. But $\text{card}(\mathbb{Z}/I_{mn}) = mn = \text{card}(\mathbb{Z}/I_m) \cdot \text{card}(\mathbb{Z}/I_n) = \text{card}(\mathbb{Z}/I_m \oplus \mathbb{Z}/I_n)$, and so ψ must be surjective. Thus ψ is an isomorphism, and we have $\mathbb{Z}/I_{mn} \cong \mathbb{Z}/I_m \oplus \mathbb{Z}/I_n$.

4.3, Q24 Suppose that m and n are relatively prime integers. Consider the isomorphism $\psi : \mathbb{Z}/I_{mn} \to \mathbb{Z}/I_m \oplus \mathbb{Z}/I_n$ from Q23. By surjectivity, there exist elements $c_1, c_2 \in \mathbb{Z}/I_{mn}$ for which $\psi(c_1) = (1,0)$ and $\psi(c_2) = (0,1)$. If $a, b \in \mathbb{Z}$, then there are integers a_0 and b_0 with $a_0 \in \{0, 1, \ldots, m-1\}$ and $b_0 \in \{0, 1, \ldots, n-1\}$ such that $a \equiv a_0 \pmod{m}$ and $b \equiv b_0 \pmod{n}$. We may regard c_1 and c_2 as integers, put $x = ac_1 + bc_2$, and then take x_0 to be the integer with $0 \le x_0 < mn$ satisfying $x_0 \equiv x \pmod{mn}$. The homomorphism property of ψ then ensures that one has $(x_0, x_0) = x\psi(1) = \psi(x) = \psi(ac_1 + bc_2) = a\psi(c_1) + b\psi(c_2) = a(1,0) + b(0,1) = (a_0, 0) + (0, b_0) = (a_0, b_0)$. Thus, we have $x \equiv x_0 \equiv a_0 \equiv a \pmod{m}$ and $x \equiv x_0 \equiv b_0 \equiv b \pmod{n}$. This confirms the Chinese Remainder Theorem.