HONORS ALGEBRA: SOLUTIONS TO HOMEWORK 10

4.1, Q1. These are all of the integers a with $0 \le a \le 23$ and $(a, 24) = 1$, for if $(a, 24) = d > 1$, then it is impossible that there is an integer b with $ab \equiv 1 \pmod{24}$. Thus, since in $\mathbb{Z}_{24}$ one has $b^2 = 1$ for all b with $(b, 24) = 1$, the invertible elements in $\mathbb{Z}_{24}$ are $1, 5, 7, 11, 13, 17, 19, 23$ (there are $8 = \varphi(24)$ elements here).

4.1, Q2. A field F is a ring which is a commutative division ring, so in particular, for each $a \in F \setminus \{0\}$, there exists $a^{-1} \in F$ such that $a^{-1}a = 1$. Consequently, if $ab = 0$ and $a \neq 0$, then $b = a^{-1}ab = a^{-1}0 = 0$. So whenever $ab = 0$, one has either $a = 0$ or $b = 0$, and hence every field F is an integral domain

4.1, Q3. If n is not prime, say $n = ab$ with $a \ge b \ge 2$, then $ab = n \equiv 0 \pmod{n}$. Thus, in $\mathbb{Z}_n$ one has $ab = 0$, so that $\mathbb{Z}_n$ has zero divisors and is not a field. If, meanwhile, one has that n is prime, then given an integer a with $1 \le a < n$ one has $(a, n) = 1$. Thus, there exist integers u and v with $au + nv = (a, n) = 1$, whence $au \equiv 1 \pmod{n}$. It follows that whenever $a \in \mathbb{Z}_n \setminus \{0\}$, then there is an element a^{-1} (the integer congruent to u modulo n with $1 \le u < n$) having the property that $a^{-1}a = 1$. But then, since $\mathbb{Z}_n$ is a commutative ring with 1, and a division ring, when p is prime this ring is a field. Thus $\mathbb{Z}_n$ is a field if and only if n is prime.

4.1, Q13. (a) One has $(i + j)(i - j) = i^2 + ji - ij - j^2 = -1 - k - k - (-1) = -2k$.
(b) One has $(1 - i + 2j - 2k)(1 + 2i - 4j + 6k) = (1 + 2i - 4j + 6k) - (i - 2 - 4k - 6j) + 2(j - 2k + 4 + 6i) - 2(k + 2j + 4i - 6) = 23 + 5i + 4k$.
(c) One has $(2i - 3j + 4k)^2 = 2(-2 - 3k - 4j) - 3(-2k + 3 + 4i) + 4(2j + 3i - 4) = -29$.
(d) One has $i(\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k) - (\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k)i = -2\alpha_3 j + 2\alpha_2 k$.

4.1, Q19. Let n be any natural number, and put $a_n = 1/\sqrt{n^2 + 1}$ and $b_n = n/\sqrt{n^2 + 1}$. Then we see that $(a_n i + b_n j)^2 = a_n^2 i^2 + a_n b_n ij + b_n a_n ji + b_n^2 j^2 = -(a_n^2 + b_n^2) = -(1+n^2)/(1+n^2) = -1$. Thus, over the quaternions we see that the equation $a^2 + b^2 = 1$ has a solution $a = a_n$, $b = b_n$ for every natural number n, and hence infinitely many solutions.

4.1, Q20. (a) The closure axiom follows from observing that $ij = -ji = k$, $jk = -kj = i$ and $ki = -ik = j$. The identity element is 1. Also, every element has an inverse, since $(\pm\alpha)^{-1} = \mp\alpha$ for $\alpha \in \{i, j, k\}$, while $(\pm 1)^{-1} = \pm 1$. Associativity requires checking associativity relations amongst $1, i, j, k$, since the coefficients ± 1 are harmless. Any combination $(\alpha)((\beta)(\gamma))$ with any term equal to 1 or all terms equal is easily checked, and if two terms precisely are equal, then by symmetry it suffices to check that $(ii)j = -j = ik = i(ij)$ and $i(ji) = i(-k) = -ik = j = ki = (ij)i$. Also by symmetry, in the situation in which α, β and γ are all distinct it suffices to check that $(ij)k = k^2 = -1 = i^2 = i(jk)$. Thus G satisfies the group axioms and is a group.
(b) There are the obvious subgroups $\{1\}$, $\{\pm 1\}$, $\{\pm 1, \pm i\}$, $\{\pm 1, \pm j\}$ and $\{\pm 1, \pm k\}$. Notice here that as soon as a subgroup contains i, then it contains $-1 = i^2$ and also $-i = i^3$, with similar comments for $-i$, and $\pm j$, $\pm k$. Meanwhile, if i and j lie in a given subgroup, then that subgroup also contains $ij = k$, and by the above comments, the whole group G, and similar comments apply for j and k, and for k and i, as well as combinations modulo $\pm$. Thus we have already listed all subgroups of G, namely the trivial group $\{1\}$, the whole group G, the groups $\{\pm 1\}$ of order 2, and the 3 subgroups of order 4.

(c) Since $ij = k \neq k = ji$, we find that neither $\pm i$ nor $\pm j$ can lie in the center of G, and one may conclude similarly for $\pm k$ since $jk = i \neq -i = kj$. Meanwhile, one has $(\pm 1)\alpha = \alpha(\pm 1)$ for all $\alpha \in G$. Thus $Z(G) = \{\pm 1\}$.
(d) Since $ij \neq ji$, the group G is of course nonabelian. The subgroups G and $\{1\}$ are trivially normal, and since $\{\pm 1\} = Z(G)$, this too is a normal subgroup of G. This leaves us to consider the 3 subgroups of order 4. Observe that $j^{-1}ij = (-j)i(j) = -jk = -i$ and $k^{-1}ik = -ki(k) = -k(-j) = -i$. From these relations one deduces that whenever $g \in G$, one has $g^{-1}(\pm i)g \in \{\pm 1, \pm i\}$, and even more easily that $g^{-1}(\pm 1)g \in \{\pm 1, \pm i\}$. Thus $\{\pm 1, \pm i\} \lhd G$. The conclusion is similar when j or k replaces i in this argument. Thus G is indeed a nonabelian group all of whose subgroups are normal.

4.1, Q31. If $ad - bc \neq 0$, then as an integer $ad - bc$ is coprime to p and hence is invertible, say $u \in \mathbb{Z}_p$ satisfies $u(ad - bc) = 1$. But then

$$\begin{pmatrix} du & -bu \\ -cu & au \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} u(ad-bc) & 0 \\ 0 & u(ad-bc) \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

and so $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is indeed invertible over R.

4.2, Q1. Suppose first that $n, m \in \mathbb{N}$. We have $na = \sum_{i=1}^{n} a$ and $mb = \sum_{j=1}^{m} b$, and hence the distributive law shows that

$$(na)(mb) = \Big(\sum_{i=1}^{n} a\Big)\Big(\sum_{j=1}^{m} b\Big) = \sum_{i=1}^{n}\sum_{j=1}^{m} ab = (nm)(ab).$$

When $n = 0$, we have instead $(0a)(mb) = 0(mb) = 0 = 0(ab) = (0m)(ab)$, with a similar conclusion when $m = 0$. Meanwhile, when n is negative, say $n = -k$, we have $(na)(mb) = (-ka)(mb) = (k(-a))(mb) = (km)((-a)b) = (km)(-(ab)) = -(km)(ab) = (-(km))(ab) = ((-k)m)(ab) = (nm)(ab)$. Again, the situation with m negative is similar, and when n and m are both negative, say $n = -k$ and $m = -l$, we have $(na)(mb) = (-ka)(-lb) = (k(-a))(l(-b)) = (kl)((-a)(-b)) = (kl)(-(a(-b))) = (kl)(-(-(ab))) = (kl)(ab) = (nm)(ab)$. This completes the proof.

4.2, Q2. If $ab = ac$ then $ab - ac = 0$, whence $a(b - c) = 0$. But R is an integral domain, so either $a = 0$ or $b - c = 0$. The former case is excluded, so $b - c = 0$ and hence $b = c$.

4.2, Q3. Suppose R is a finite integral domain, so R is a commutative ring with no zero divisors. Given $a \in R \setminus \{0\}$, one has $a^n \neq 0$ for all $n \in \mathbb{N}$. For otherwise, if h is the least positive integer with $a^h = 0$, we have $a \neq 0$ and $a^{h-1}a = 0$, and the integral domain property of R implies that $a^{h-1} = 0$, contradicting the minimality of h. Next, since R is finite, the elements a^n cannot all be distinct for $n \in \mathbb{N}$. Suppose temporarily that R contains a 1. Then there are positive integers m and n with $a^m(a^n - 1) = a^{m+n} - a^m = 0$. Since $a^m \neq 0$, the integral domain property of R shows that $a^n - 1 = 0$, and hence $a \cdot a^{n-1} = 1$. Thus, for all $a \in R \setminus \{0\}$, there exists $b \in R$ with $ab = 1$, namely $b = a^{n-1}$. Then R is a division ring that is commutative with 1, and hence a field.

Note that some authors insist that an integral domain contains a 1, and this avoids the last step of proving that R contains a 1. When $a \in R \setminus 0$, and b and c are distinct elements of R, then $ab \neq ac$. Thus, since R is finite, the map $x \mapsto ax$ is a permutation of the elements of R. In particular, there exists an element $e \in R$ with $a = ae$ and then also $a = ea$. This element e is a multiplicative identity on R, for given $b \in R$, there exists $c \in R$ with $b = ac$, and then $eb = eac = ac = b$, whence $eb = be = b$ for all $b \in R$. Thus R does indeed have a 1, namely e.