MNS Group Theory Solutions. (SKD version)

1. (a) No. Associative law fails, for example $0-(1-1)\neq(0-1)-1$.
(b) No. The element 0 does not have an inverse.
(c) Yes. The sum of two even integers is even, addition of integers is associative, the identity is 0 (which is even), and the inverse of the even integer n is the even integer $-n$.
(d) No. The only element with an inverse is 1.
(e) Yes. Check the axioms:
(i) If p/q and p'/q' are rationals with q and q' odd, then the denominator of

$$\frac{p}{q}+\frac{p'}{q'}=\frac{pq'+p'q}{qq'}$$

is also odd (since it is a divisor of qq'). So the group operation is closed.
(ii) The associative law holds as it does for addition of arbitrary rational numbers.
(iii) $0=0/1$ is an identity.
(iv) The denominator of $-x$ is the same as that of x, so that inverses exist.
(f) Yes. For any prime p the integers $1,2,\ldots,p-1$ always form a group under multiplication modulo p. This is just the group $U(\mathbf{Z}_p)$ defined in your notes; since $\mathbf{Z}_p$ is a field, $U(\mathbf{Z}_p)=\mathbf{Z}_p-\{0\}$.
(g) No. For example $2\times 3\equiv 0 \pmod 6$, but 0 is not in the given set.

2. The associative and commutative laws follow from those for multiplication of complex numbers. It suffices to check that the sets are closed under multiplication, inverse and that each contains 1. For multiplication this follows from the identities:

$$2^n\times 2^{n'}=2^{n+n'};$$
$$\frac{1+2m}{1+2n}\times\frac{1+2m'}{1+2n'}=\frac{1+2m''}{1+2n''}\quad\text{where } m''=m+m'+2mm',\ n''=n+n'+2nn';$$
$$(\cos\theta+i\sin\theta)(\cos\phi+i\sin\phi)=\cos(\theta+\phi)+i\sin(\theta+\phi).$$

The number 1 belongs to each of these sets because

$$1=2^0,\qquad 1=\frac{1+(2\times 0)}{1+(2\times 0)},\qquad 1=\cos 0+i\sin 0.$$

The inverse of 2^n is 2^{-n}, that of $(1+2m)/(1+2n)$ is $(1+2n)/(1+2m)$, and that of $\cos\theta+i\sin\theta$ is $\cos(-\theta)+i\sin(-\theta)$. Each of these sets is clearly infinite.

3. (a) No (the zero matrix does not have an inverse, for example).
(b) No. The product of two symmetric matrices need not be symmetric. For example,

$$\begin{pmatrix}1&2\\2&3\end{pmatrix}\begin{pmatrix}0&1\\1&0\end{pmatrix}=\begin{pmatrix}2&1\\3&2\end{pmatrix}.$$

(c) Yes. Follows from the formulae:

$$\begin{pmatrix}a_1&0&\ldots&0\\0&a_2&\ldots&0\\\vdots&\vdots&\ddots&\vdots\\0&0&\ldots&a_n\end{pmatrix}\begin{pmatrix}b_1&0&\ldots&0\\0&b_2&\ldots&0\\\vdots&\vdots&\ddots&\vdots\\0&0&\ldots&b_n\end{pmatrix}=\begin{pmatrix}a_1b_1&0&\ldots&0\\0&a_2b_2&\ldots&0\\\vdots&\vdots&\ddots&\vdots\\0&0&\ldots&a_nb_n\end{pmatrix}$$

and

$$\begin{pmatrix} a_1 & 0 & \dots & 0 \\ 0 & a_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a_n \end{pmatrix}^{-1} = \begin{pmatrix} a_1^{-1} & 0 & \dots & 0 \\ 0 & a_2^{-1} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a_n^{-1} \end{pmatrix}$$

(d) Yes, though checking closure and inverses is quite fiddly. (- On a separate handout, if I have time.)
(e) No (if $\det A$ is not ± 1, then $\det(A^{-1}) = (\det A)^{-1}$ is not an integer, so A^{-1} cannot have integer entries).
(f) Yes (since product and inverse of non-singular rational matrices have rational entries).
(g) Yes. The only axiom which is at all difficult to check is the inverse axiom. For this, use the fact that if $\operatorname{adj}(A)$ is the adjioint matrix of A then $A \operatorname{adj}(A) = \det(A).I$. So if $\det(A) = \pm 1$, then $A^{-1} = \pm \operatorname{adj}(A)$ has integer entries.

4. It is completely routine to check the axioms, remembering of course that the associative law holds for addition of real or complex numbers (so you need not check it again), and that 0 belongs to all of these sets (just take $a = b = 0$ in each case).

5. If $a + b\sqrt{2} \neq 0$ then $a - b\sqrt{2} \neq 0$ also (if it were zero, then since $\sqrt{2}$ is irrational we would have $a = b = 0$). Therefore we can write

$$\begin{aligned} \frac{1}{a + b\sqrt{2}} &= \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} \\ &= \frac{a}{a^2 - 2b^2} + \frac{(-b)}{a^2 - 2b^2}\sqrt{2} \quad \in \mathbf{Q}[\sqrt{2}] - \{0\}. \end{aligned}$$

So every element has an inverse under multiplication. Moreover

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2} \quad \in \mathbf{Q}[\sqrt{2}] - \{0\}.$$

so the set is closed under multiplication. Finally, $1 = 1 + 0.\sqrt{2}$ lies in the given set, and multiplication of real numbers is associative. (Notice that **4.**(b) and **5.** follow from the fact that $\mathbf{Q}[\sqrt{2}]$ is a field.)

6. The first set is not closed under multiplication mod 14 (3×3 undefined). The second and third sets do not satisfy the inverse axiom (no inverse for 7). The fourth set does form a group under multiplication modulo 14.

7. $(12)(23) = (123)$; $(12)(1234) = (234)$; $(1234)(12) = 134)$; $(145)(3524) = (143)(25)$;
$(123 \dots r)(r\ r+1) = (123 \dots r\ r+1)$.

8.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 6 & 4 & 1 & 8 & 2 & 3 & 5 \end{pmatrix} = (1734)(26)(58) = (14)(13)(17)(26)(58) = (17)(73)(34)(26)(58)$$

$$(4568)(1245) = (125)(468) = (15)(12)(48)(46) = (12)(25)(46)(68)$$

$$(624)(253)(876)(45) = (25687)(34) = (27)(28)(26)(25)(34) = (25)(56)(68)(87)(34)$$

(Of course, there are many alternative ways to express them as products of transpositions.)

9. Check the axioms one at a time: (i) The composite of T_b^a and T_d^c is the map

$$x \mapsto T_b^a(T_d^c(x)) = T_b^a(cx + d) = a(cx + d) + b = (ac)x + (ad + b).$$

Therefore $T_b^a \circ T_d^c = T_{ad+b}^{ac}$ is in the set of functions considered, so the group operation is defined on the set.
(ii) The associative law holds for composition of arbitrary mappings; so it holds in this set.

(iii) The mapping T_0^1 is the identity mapping on $\mathbf{R}$, so $T_b^a \circ T_0^1 = T_b^a = T_0^1 \circ T_b^a$. Therefore T_0^1 is an identity.
(iv) From the formula in (i) we see that $T_b^a \circ T_{-b/a}^{1/a} = T_0^1 = T_{-b/a}^{1/a} \circ T_b^a$, so each element has an inverse in the set. So the set of mappings indeed forms a group.

10. Let G be the group, and H the set of elements of finite order. Since $\mathrm{ord}(e) = 1$, H is nonempty. Suppose x, $y \in H$, and let their orders be m, n respectively. Then $(x^{-1})^m = x^{-m} = e$ and $(xy)^{mn} = x^{mn}y^{mn}$ (since G is abelian) which means $(xy)^{mn} = e$. Therefore xy and x^{-1} have finite order and are thus in H. So H is a subgroup.

11. (i) $\bar{1}$, $\bar{2}$, $\bar{4}$, $\bar{5}$, $\bar{7}$, $\bar{8}$ have order 9; $\bar{3}$ and $\bar{6}$ have order 3; and $\bar{0}$ has order 1.
(ii) $\bar{a}$ has order 8 if a is odd; $\bar{2}$ and $\bar{6}$ have order 4; $\bar{4}$ has order 2; and $\bar{0}$ has order 1.
(iii) D_n is the group of symmetries of the regular n-gon. We write r for rotation by $2\pi/n$, and s for a fixed reflection in an axis containing a vertex. Then $D_n = \{r^i, sr^i \mid 0 \leq i \leq n-1\}$. The reflections sr^i have order 2. If $n = 6$ then r and $r^5 = r^{-1}$ have order 6, r^2 and r^4 have order 3, and r^3 has order 2.
(iv) If $x \in \mathbf{C}^* = \mathbf{C} - \{0\}$ and $x = e^{2\pi i p/q}$ for a rational number p/q in lowest terms ($q > 0$ and $\mathbf{gcd}(p,q) = 1$) then x has order q. Otherwise x has infinite order.

12. The main tool to simplify this calculation is Lagrange's theorem.
(i) Let $G = \mathbf{Z}_{12}$, and $H < G$. Then by Lagrange's theorem, $|H|$ divides 12. If $|H| = 1$ then $H = \{\bar{1}\}$, and if $|H| = 12$ then $H = G$. Before going further, write down the orders of the elements of $\mathbf{Z}_{12}$:

Elements:	$\bar{0}$	$\bar{6}$	$\bar{4}$, $\bar{8}$	$\bar{3}$, $\bar{9}$	$\bar{2}$, $\overline{10}$	$\bar{1}$, $\bar{5}$, $\bar{7}$, $\overline{11}$
Order:	1	2	3	4	6	12

If $|H| = m$ and m is one of 2, 3, 4 or 6, then every element of H has order dividing m. But in each case the table shows that there are only m elements with order dividing m. Thus the only subsets which could be subgroups are

$$\{\bar{0}\}, \quad \{\bar{0},\bar{6}\}, \quad \{\bar{0},\bar{4},\bar{8}\}, \quad \{\bar{0},\bar{3},\bar{6},\bar{9}\}, \quad \{\bar{0},\bar{2},\bar{4},\bar{6},\bar{8},\overline{10}\} \quad \text{and } H.$$

It is quick to check that each of these is in fact a subgroup.
(ii) Let $G = V$, which has 4 elements. If $H < G$ then $|H| = 1$, 2 or 4. So either $H = \{e\}$ or $H = V$ or $H = \{e, x\}$ with $\mathrm{ord}(x) = 2$. In this last case x can be any of the three non-identity elements of V. So there are three subgroups of order 2:

$$\{e,(12)(34)\}, \quad \{e,(13)(24)\} \quad \text{and } \{e,(14)(23)\}.$$

(iii) Let $G = D_4$, which has order 8. So any subgroup H has order dividing 8. Apart from the trivial cases this implies $|H| = 2$ or 4. If $|H| = 2$ then $H = \{e, x\}$ with $o(x) = 2$. Now D_4 has 5 elements of order 2: the 4 reflections sr^i $(0 \leq i \leq 3)$ and the rotation r^2 through π. This gives 5 subgroups of order 2.

If $|H| = 4$ then either H contains an element of order 4 or all the non-identity elements have order 2. The first case implies that one of r, r^3 is in H, and since $r^3 = r^{-1}$ there is only one possibility, namely $H = \langle r \rangle = \{1, r, r^2, r^3\}$.

In the second case, H contains 3 elements of order 2, so at least two of them must be reflections, say sr^i and sr^j, with $0 \leq i < j \leq 3$. But their product is $sr^isr^j = r^{j-i}$, and $0 < j - i \leq 3$. The product therefore has order dividing 2 if and only if $j - i = 2$, so the only possibilities are:

$$H = \begin{cases} \{e, s, sr^2, r^2\} & \text{if } i = 0,\ j = 2; \text{ or} \\ \{e, sr, sr^3, r^2\} & \text{if } i = 1,\ j = 3. \end{cases}$$

It is easily checked that these are indeed subgroups.
(iv) Let $G = S_3$. If $H < G$ then $|H|$ divides 6, and the possibilities are:
$|H| = 1$ or 6: $H = \{e\}$ or S_3 respectively.
$|H| = 2$: then $H = \{e, x\}$ where x is one of (12), (13) or (23).
$|H| = 3$: then $H = \{e, (123), (132)\}$ as the order of each element of H is 1 or 3.

13. By matrix multiplication we see that $\text{ord}(A) = 4$ and $\text{ord}(B) = 3$. Now

$$AB = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad BA = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$$

so that

$$(AB)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad (BA)^n = \begin{pmatrix} 1 & 0 \\ -n & 1 \end{pmatrix}$$

hence AB and BA have infinite order in $GL_2(\mathbf{R})$. In $M_2(\mathbf{R})$ the group operation is addition, so each element has infinite order.

14. (NOT SET) (i) Since $xy = yx$ we can write $(xy)^r = x^r y^r$, so if $\text{ord}(x) = m$ and $\text{ord}(y) = n$, then $(xy)^{mn} = e$. Moreover, if k is the least common multiple of m and n we have $(xy)^k = x^k y^k = e$, so $\text{ord}(xy)$ divides k. That is all that can be said in general; sometimes $\text{ord}(xy) = k$ and sometimes not. For example, in $\mathbf{Z}_8^*$, the elements $\bar{3}$, $\bar{5}$ have order 2, but $\bar{3}.\bar{5} = \bar{7}$ has order 2 whereas $\bar{3}.\bar{3} = \bar{1}$ has order 1.
(ii) By the first part the group must be nonabelian, and clearly it must also be infinite.

15. The left cosets are:

$$V, \quad (123)V = \{(123), (134), (243), (142)\} \quad \text{and} \quad (132)V = \{(132), (234), (124), (143)\}.$$

So $A_4 = eV \cup (123)V \cup (132)V$ (disjoint union). Check also that $(123)V = V(123)$ and $(132)V = V(132)$, and obviously $eV = Ve$. So left and right cosets are equal.

16. Write $H = \{e, r^3, s, r^3s\}$. Then

$$rH = \{r, r^4, rs, r^4s\} \quad \text{and} \quad r^2H = \{r^2, r^5, r^2s, r^5s\}.$$

The coset decomposition is $D_6 = H \cup rH \cup r^2H$. Now

$$Hr = \{r, r^4, r^5s, r^2s\} \quad \text{and} \quad Hr^2 = \{r^2, r^5, r^4s, rs\}$$

(using $sr = r^5s$) so left and right cosets are not equal.
(Note: this answer writes all group elements with s on the right (i.e. do s first). It is equally correct to write s always on the left, but you must decide on one standard way for the whole question.)

17. In each case you just have to check whether $\phi(xy) = \phi(x)\phi(y)$ holds for every x, $y \in \mathbf{R}^* = \mathbf{R} - \{0\}$ (ϕ being the respective function). The answers are:
(a) Yes; (b) No; (c) No; (d) Yes; (e) No.

18. (i) No; (ii) No; (iii) Yes, since $|zw| = |z|\,|w|$;
(iv) Yes, as $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+y \\ 0 & 1 \end{pmatrix}$.

19. No, they are not isomorphic. If they were, $\mathbf{Z} \times \mathbf{Z}$ would be cyclic, hence there would exists $x = (a, b) \in \mathbf{Z} \times \mathbf{Z}$ such that $\mathbf{Z} \times \mathbf{Z} = <x>$. So in particular, for some integers m and n:

$$\begin{aligned} m(a,b) &= (1,0) \quad \text{so that} \quad ma = 1,\ mb = 0; \\ n(a,b) &= (0,1) \quad \text{so that} \quad na = 0,\ nb = 1. \end{aligned}$$

These equations are inconsistent, so $\mathbf{Z} \times \mathbf{Z}$ is not cyclic.

20. (NOT SET) Label the vertices of T with the integers 1, 2, 3, 4. Let $r_{i,j}$ denote reflection in the plane which passes through the mid point of the edge joining vertices i and j, and through the other two vertices. Then the composition $r_{1,4}r_{1,3}r_{1,2}$ induces the permutation $(1\,2\,3\,4)$. Each symmetry of T induces a permutation of the vertices. If two symmetries u, v induce the permutations α and β respectively, then uv clearly induces $\alpha\beta$. Therefore the correspondence *symmetry* $\rightarrow$ *induced permutation* is a homomorphism from G to S_4. The only symmetry which fixes all four vertices is the identity. Consequently two symmetries which induce the same permutation must be equal. (For if u and v lead to the same permutation, then uv^{-1} induces the identity permutation and is the identity symmetry. Then $uv^{-1} = e$ gives $u = v$.) Therefore our correspondence is one-one. It is also onto, since $r_{i,j}$ realises the transposition $(i\,j)$, $r_{i,k}r_{i,j}$ realises the 3-cycle $(i\,j\,k)$, $r_{i,l}r_{i,k}r_{i,j}$ realises $(i\,j\,k\,l)$, and $r_{i,j}r_{k,l}$ realises $(i\,j)(k\,l)$. So G is isomorphic to S_4.

21. $|A_4| = 12$, so A_4 is not isomorphic to any of the others (which have order 8). Of the rest, D_4 is nonabelian and so is not isomorphic to either $\mathbf{Z}_8$ or $\mathbf{Z}_4 \times \mathbf{Z}_2$, which are abelian. Finally, if $(x, y) \in \mathbf{Z}_4 \times \mathbf{Z}_2$ then $4(x, y) = (4x, 4y) = (0, 0)$, so the order of every element divides 4; but $\bar{1} \in \mathbf{Z}_8$ has order 8. (OR $\mathbf{Z}_8 \not\cong \mathbf{Z}_4 \times \mathbf{Z}_2$ because $\gcd(4, 2) \neq 1$.) So no two of the groups are isomorphic. Alternatively, consider elements of order 2: $\mathbf{Z}_8$ has 1, $\mathbf{Z}_4 \times \mathbf{Z}_2$ has 3 and D_4 has 5. So no two of these groups are isomorphic.

22. (i) Define $\phi : \mathbf{C} \to \mathbf{R} \times \mathbf{R}$ by $\phi(a + ib) = (a, b)$. Then ϕ is clearly a bijection, and

$$\phi((a + ib) + (c + id)) = \phi((a + c) + i(b + d)) = (a + c, b + d) = (a, b) + (c, d) = \phi(a + ib) + \phi(c + id).$$

(ii) Define $\psi : \mathbf{C}^* \to \mathbf{R}^{pos} \times C$ by $\psi(re^{i\theta}) = (r, e^{i\theta})$. Then ψ is a bijection and

$$\psi(r_1e^{i\theta_1}.r_2e^{i\theta_2}) = \psi(r_1r_2e^{i(\theta_1+\theta_2)}) = (r_1r_2, e^{i(\theta_1+\theta_2)}) = (r_1, e^{i\theta_1}).(r_2e^{i\theta_2}) = \psi(r_1e^{i\theta_1}).\psi(r_2e^{i\theta_2}).$$

23. (a) A 3- cycle in A_4 corresponds to a rotation through $2\pi/3$ about a vertex-face axis. The associated permutation of T is a product of two disjoint 3-cycles.
(b) This is a rotation through π round an edge-edge axis. Those two edges are sent to themselves, and the remaining 4 are swapped in pairs. So we have a product of two disjoint transpositions.

24. S_4 has 4 subgroups of order 6, each one isomorphic to S_3: $\{e, (123), (132), (12), (13), (23)\}$, $\{e, (124), (142), (12), (14), (24)\}$, $\{e, (134), (143), (123), (14), (34)\}$, $\{e, (234), (243), (23), (24), (34)\}$.
To see this, consider the order of each element of S_4. A subgroup H of order 6 cannot contain a 4-cycle (Cor.20.4). Also (by our list of small groups) H must be isomorphic to either $\mathbf{Z}_6$ or S_3, but since S_4 has no elements of order 6, H cannot be cyclic. So only S_3 is possible, so H must contain 2 elements of order 3, for example (123) and (132), and 3 of order 2. If we try to put in any permutation involving 4, H being closed will produce 4-cycles, and more than 6 elements. So the only possibility is to put in (12), (13), and (23).

25. Note first two facts true in any group: (1) since $(xy)(y^{-1}x^{-1}) = e$, we know that $(xy)^{-1} = y^{-1}x^{-1}$.
(2) By the existence (group axiom 4) and uniqueness (Prop. 18.2.ii) of inverses,
the function $f(x) = x^{-1}$ is bijective.
($\Rightarrow$) Assume G is abelian. Then $f(xy) = (xy)^{-1} = y^{-1}x^{-1}$ as above, but since G is abelian, this equals $x^{-1}y^{-1} = f(x)f(y)$. So f is a homomorphism. Since (as above) f is also bijective, it is an isomorphism.
($\Leftarrow$) Assume f is an isomorphism, and so a homomorphism.
Then for any $x, y \in G$, we know $f(x^{-1}y^{-1}) = f(x^{-1})f(y^{-1}) = xy$.
But also, as above in (1), $f(x^{-1}y^{-1}) = (x^{-1}y^{-1})^{-1} = (y^{-1})^{-1}(x^{-1})^{-1} = yx$. So $xy = yx$. So G is abelian.

26. ($\Leftarrow$) Suppose G and H are both abelian.
Then for any (a, b) and $(c, d) \in G \times H$ we have $(a, b)(c, d) = (ac, bd) = (ca, db) = (c, d)(a, b)$.
($\Rightarrow$) Can easily be shown by contradiction, but instead notice that $G \times H$ has subgroups
$G \times \{e\} = \{(g, e)|g \in G\}$ and $\{e\} \times H = \{(e, h)|h \in H\}$ which are clearly isomorphic to G and H respectively.
Subgroups of an abelian group are abelian.
Thus if $G \times H$ is abelian, then so are $G \times \{e\}$ and $\{e\} \times H$, and so G and H also.
Also, subgroups of a cyclic group are cyclic, so if $G \times H$ is cyclic, then similarly G and H are too.
(A cyclic group is $\cong \mathbf{Z}_n$ for some n. Any subgroup of $\mathbf{Z}_n$ is $\cong \mathbf{Z}_m$, where $m|n$, and is generated by $\overline{n/m}$.)