ALGEBRA SOLUTION SHEET

1 Associativity of the multiplication in the real or complex numbers implies associativity in each case.

(a) $2^k 2^l = 2^{k+l}$ implies closure. The identity is $1 = 2^0$ and the inverse of 2^k is 2^{-k}.

(b) Closure follows from the observation that the product of two odd numbers is odd. The identity has $m = n = 0$. The inverse swaps the role of m and n.

(c) We are dealing with complex numbers of the form $e^{i\theta}$ where θ is rational. The multiplication then just adds the relevant θ values. That the sum of two rationals is rational gives closure. The identity has $\theta = 0$ and the inverse for θ requires the value $-\theta$ which is also rational.

2 (a) The effect of $T_b T_a$ is $n \mapsto n + a \mapsto n + a + b$, so $T_b T_a = T_{a+b}$.
(b) The effect of $R_d T_a$ is $n \mapsto n + a \mapsto d - (n + a) = (d - a) - n$, so $R_d T_a = R_{d-a}$.
(c) $n \mapsto c - n \mapsto b + c - n$, so $T_b R_c = R_{b+c}$.
(d) $n \mapsto c - n \mapsto d - (c - n) = (d - c) + n$, so $R_d R_c = T_{d-c}$.
The above calculations show we have closure. The group law is composition of functions so associativity holds. The identity is T_0. The inverse of T_a is T_{-a} and that of R_c is R_c.
For the final bit, just take two different reflections. E.g., $g = R_1$ and $h = R_0$. Then $g^2 = h^2 = e$, $gh = T_1$, $hg = T_{-1}$, and $(gh)^k = T_k \neq e$.

3 Closure is obvious. For associativity we calculate

$$m*(n*p) = m+(n*p)+m(n*p) = m+n+p+np+m(n+p+np) = m+n+p+np+mn+mp+mnp$$

Similarly

$$(m*n)*p = (m*n)+p+(m*n)p = m+n+mn+p+(m+n+mn)p = m+n+p+mn+mp+np+mnp$$

0 is an identity, since $m * 0 = m + 0 + m0 = m$, $0 * m = 0 + m + 0m = m$. For an inverse to m we need to be able to solve $m + n + mn = 0$ which requires $n = -m/(m + 1)$. This is not in general soluble in integers, but we need a specific example to show inverses fail and $m = -1$ is the most spectacular since $(-1) * n = -1 + n + (-1)n = -1$, so there is no possible inverse to -1.

4 (a) Let's determine if $a^2 = e$, a or b. If $a^2 = a$ then multiplyin on the left (or right) by a^{-1} leads to $a = e$, so that's impossible. Assume $a^2 = e$, so $a^{-1} = a$. Then $ab = e$, a or b. The first leads to $b = a^{-1} = a$, the second to $b = e$ (multiply on the left by a^{-1}), and the third to $a = e$ (multiply on the right by b^{-1}). None of those are possible, so $a^2 \neq e$. That only leaves $a^2 = b$.
Ruling out $ab = a$ or b never used any assumptions, so $ab = e$. Similarly $ba = e$. Then the only product that is not clear is b^2. If $b^2 = b$ we get $b = e$, if $b^2 = e = ab$ we get $a = b$, leaving only $b^2 = a$.
[This becomes a lot easier if we observe that $gh_1 = gh_2$ implies $h_1 = h_2$ (multiply on the left by g^{-1}). This means that in every row of the group table every element occurs at most once. It also must occur exactly once (if we want to get k in the row starting with g we have to take the column with $g^{-1}k$ at the top). Similarly $h_1 g = h_2 g$ implies $h_1 = h_2$ (multiply on the right by g^{-1}), and every element of the group occurs exactly once in every column of the group table. Now check that knowing that $a^2 = b$ allows you to fill in the group table without any further calculations.]
(b) In this case we use the rule that in every row or column of the group table every element occurs exactly once.

For a^2 there are three possibilities: $a^2 = e$, $a^2 = b$ or $a^2 = c$, but the last two coincide if we rename b and c. When filling in the table for $a^2 = e$ we have to make a choice: $b^2 = e$ or a. But the second case is like $a^2 = b$ but with a and b renamed, so we ignore it here. Then the table can be filled out in only one way.
For $a^2 = b$ the table can be filled out in only one way. (Note that $ab = e$ or c but $ab = e$ would lead to $ac = c$.)

5

(a) Since $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)\left(\begin{smallmatrix} e & f \\ 0 & h \end{smallmatrix}\right) = \left(\begin{smallmatrix} ae & af+bh \\ 0 & dh \end{smallmatrix}\right)$, all entries are real and $aedh \neq 0$ since $ad, eh \neq 0$, we have closure. Associativity comes from the fact that matrix multiplication is associative (this is a case where you should *not* multiply out three example matrices two ways!). I_2 is in G and is the identity. Finally, the inverse of $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$ is $\left(\begin{smallmatrix} a^{-1} & -a^{-1}bd^{-1} \\ 0 & d^{-1} \end{smallmatrix}\right)$.

(b) Suppose $\left(\begin{smallmatrix} A & B \\ 0 & D \end{smallmatrix}\right)$ is in $Z(G)$, so $\left(\begin{smallmatrix} Aa & Ab+Bd \\ 0 & Dd \end{smallmatrix}\right) = \left(\begin{smallmatrix} A & B \\ 0 & D \end{smallmatrix}\right)\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)\left(\begin{smallmatrix} A & B \\ 0 & D \end{smallmatrix}\right) = \left(\begin{smallmatrix} aA & aB+bD \\ 0 & dD \end{smallmatrix}\right)$ whenever $ad \neq 0$, or equivalently, $Ab + Bd = aB + bD$ whenever $ad \neq 0$. Taking $a = 2$, $d = 1$ and $b = 0$ shows $B = 0$; then taking $b = 1$ shows $A = D$. If $B = 0$ and $A = D$ the equation is satisfied, so $Z(G) = \{\left(\begin{smallmatrix} A & 0 \\ 0 & A \end{smallmatrix}\right)$ with $A \neq 0\}$. To see $Z(G)$ is a group we note that closure follows from $\left(\begin{smallmatrix} A & 0 \\ 0 & A \end{smallmatrix}\right)\left(\begin{smallmatrix} A' & 0 \\ 0 & A' \end{smallmatrix}\right) = \left(\begin{smallmatrix} AA' & 0 \\ 0 & AA' \end{smallmatrix}\right)$, matrix multiplation is associative, we get the identity for $A = 1$, and $\left(\begin{smallmatrix} A & 0 \\ 0 & A \end{smallmatrix}\right)$ has inverse $\left(\begin{smallmatrix} A^{-1} & 0 \\ 0 & A^{-1} \end{smallmatrix}\right)$.

6 Let n be the integer and consider the set of numbers: $\{n - 2k | k \in \mathbb{Z}\}$. Let r be the least non-negative value that occurs. If $r \geq 2$ and $r = n - 2k$ then $r' = n - 2(k + 1)$ satisfies $0 \leq r' < r$, so r was not the least non-negative. Hence $r = 0, 1$ are the only possibilities, and $n = 2k$ or $n = 2k + 1$ for some k in $\mathbb{Z}$.

7 By assumption there exist x, y in $\mathbb{Z}$ with $a = xd$ and $b = yd$. Then $ma + nb = (mx + ny)d$, so $d|(ma + nb)$.

8 Any linear expression where every term is divisible by k is also divisible by k. So the only integers of interest for (a) are those which have no prime factor common with 12, and similarly for (b) with 12 replaced by 30.

(a) $1 \cdot 1 = 1$, $5 \cdot 5 = 24 = 2 \cdot 12 \cdot +1$, $7 \cdot 7 = 49 = 4 \cdot 12 + 1$, $11 \cdot 11 = 121 = 10 \cdot 12 + 1$.

(b) $1 \cdot 1 = 1$, $7 \cdot 13 = 13 \cdot 7 = 91 = 3 \cdot 30 + 1$, $11 \cdot 11 = 121 = 4 \cdot 30 + 1$, $17 \cdot 23 = 23 \cdot 17 = 391 = 13 \cdot 30 + 1$, $19 \cdot 19 = 361 = 12 \cdot 30 + 1$, $29 \cdot 29 = 841 = 28 \cdot 30 + 1$

(c) The situation is symmetric in the sense that if a leads to b then $0 < b < 12$ (resp. $0 < b < 30$) and b leads to a (with $a = b$ a distinct possibility).

9 Suppose that $d|a$ and $d|b$. Then $d|a - b$ and $d||a - b| = \pm 1$. If a, b are among the integers $n, n + 1, \ldots, n + d - 1$ then $|a - b| < d - 1$ so this can only be divisible by d if it is 0, i.e., $a = b$. This shows that at most one of $n, n + 1, \ldots, n + d - 1$ is divisible by d.
To see that at least one of those integers is divisible by d we apply Theorem 2.1 to n, so $n = qd + r$ for $0 \leq r < d$. Note that $n - r = qd$ is divisible by d, but it might be too small, so we might have to consider $n - r + d$. This leads to two cases: if $r = 0$ then $d|n$ and we are done; if $1 \leq r < d$ then $n - r + d$ is divisible by d and satisfies $n < n - r + d \leq n + d - 1$, so is among the integers under consideration.

10 Consider 3 integers $n,\ n + 2,\ n + 4$. Divide n by 3 to get $n = 3k + r$ with $0 \leq r < 3$. If $r = 0$ then r is a multiple of 3. If $r = 1$ then $n + 2 = 3k + 3$ is a multiple of 3. If $r = 2$, then $n + 4 = 3k + 6$ is a multiple of 3. Thus any such triple contains a multiple of 3.
But any multiple of 3 greater than 3 is not prime. So the only prime triple must involve the integer 3 explicitly. By inspection this is the triple 3, 5, 7.

11

(a) The test is to add the decimal digits and see whether this sum is divisible by 9. If it is then so was the original number. To prove this let $n = d_k d_{k-1} \dots d_1 d_0 = \sum_{i=0}^{k} d_i 10^i$. Then the sum of the digits is $s = \sum_{i=0}^{k} d_i$ and

$$n - s = \sum_{i=0}^{k} d_i (10^i - 1)$$

But $10^i - 1$ is a multiple of 9 (it is a string of i consecutive nines). So $n - s$ is divisible by 9 whence n is divisible by 9 if and only if s is also.

(b) Here we take the *alternating* sum of the decimal digits. So with the same notation we have $s = \sum_{i=0}^{k} (-1)^i d_i$ and

$$n - s = \sum_{i=0}^{k} d_i (10^i - (-1)^i)$$

Examine the values $10^i - (-1)^i$ and we find that each of them is necessarily a multiple of 11. So essentially the same argument works.

12 Eratosthenes Sieve The p_i are just the primes in ascending order. By the time we have done 4 iterations, we have eliminated all multiples of 2, 3, 5 and 7. But $7^2 > 30$ and so what remains cannot have a divisor less than its square root so that what remains are also prime.
(a) Applying the same argument in fact all the numbers left up to 100 are prime, since any such non-prime integer would have a prime factor less than $\sqrt{100} = 10$.
(b) $31^2 = 961$, $37^2 > 1,000$, so we need to do enough iterations to get to deal with the number 31. I.e. 11 in all.
(c) $100^2 = 10,000$ so the number of iterations is the number of primes up to 100. There are 26 such.
(d) We need the number of primes up to $\sqrt{10^n}$.

13 Since $n!$ is a multiple of k, $n! + k$ is a multiple of k and is greater than k. Hence it is not prime.
The above formula says look at the 10 numbers starting at $11! + 2 = 39,916,802$.
On the other hand there is a sequence of 13 non-primes starting at 114.

14 $x = 41$ works, as does $x = 40$.

15 The divisors of $n = 2^k p$ are $1, 2, \dots 2^k, p, 2p, \dots 2^{k-1}p$. Adding these up (using the standard formula for geometric series) gives a total $2^{k+1} - 1 + p(2^k - 1)$.
For this to be equal to $2^k p$ we must have $p = 2^{k+1} - 1$ as required.
The perfect number 6 corresponds to the case $p = 3,\ k = 1$.
$k = 2$ gives $p = 2^3 - 1 = 7$ and $n = 28$.
$k = 4$ gives $p = 2^5 - 1 = 31$ and $n = 496$.

16

(a) **Mersenne Primes**

Let $a = bc$, then $1 + x^b + x^{2b} + \dots + x^{(c-1)b} = \frac{(x^{cb}-1)}{(x^b-1)}$. So

$$x^a - 1 = (x^b - 1)(1 + x^b + x^{2b} + \dots + x^{(c-1)b}) .$$

Now simply put $x = 2$ to get a factorisation of $2^a - 1$ with $2^b - 1$ as a factor. So the only way $2^n - 1$ can be prime is if $2^b - 1 = 2^1 - 1 = 1$ and $b = 1$ is the only factor of n less than n. I.e., n must be prime.

(b) $2^{11} - 1 = 23 \cdot 89$

(c) **Fermat Primes** Let $a = bc$ where c is odd. Now do the sum of the geometric series

$$\sum_{k=0}^{c-1}(-1)^k x^{kb} = \frac{((-x^b)^c - 1)}{(-x^b - 1)} = \frac{(x^a + 1)}{(x^b + 1)}$$

Thus

$$x^a + 1 = (x^b + 1)(\sum_{k=0}^{c-1}(-1)^k x^{kb})$$

Now put $x = 2$ and we have a factorisation of $2^a + 1$ involving $2^b + 1$ as a factor.

The only way this can fail to give a proper factor is if $a = b$ and $c = 1$. But as soon as a has an odd factor greater than 1, then we can choose this as c and get a factorisation. Similarly, if a is odd, we can choose $b = 1,\ c = 1$ and get a factorisation.

So the only possibility of $2^a + 1$ being prime is when $a = 2^n$ and $n > 0$.

(d) If we let the n-th Fermat number be $F_n = 2^{2^n} + 1$, then F_n is prime for $n = 1,\ 2\ , 3\ , 4$.

$F_5 = 4,294,967,297 = 641.6,700,417$. It is known that all the Fermat numbers up to F_{23} are composite (i.e. non-prime). Nothing more is known above that.

17 (a) $n = n(3-2) = n \cdot 3 - n \cdot 2$
(b) $1 = 3 \cdot 5 - 2 \cdot 7$, so $n = 3n \cdot 5 - 2n \cdot 7$
(c) $1 = 5 \cdot 13 - 8 \cdot 8$ so $n = 5n \cdot 13 - 8n \cdot 8$

18 (a) $-5 \cdot 26 + 3 \cdot 44 = 2$
(b) $-248 \cdot 1169 + 83 \cdot 3493 = 7$
(c) $178 \cdot 182 - 55 \cdot 589 = 1$
(d) $-9 \cdot 1573 + 5 \cdot 2860 = 143$
(e) $-79 \cdot 22103 + 52 \cdot 33580 = 23$
(f) $2846 \cdot 1229 - 153 \cdot 22861 = 1$

19 A bit easier than I had wanted: $x = 2,\ y = 0$ works for the first bit.
For the second it is impossible as 9 divides the LHS but not the RHS.

20 We know that we can find $ax + dy = 1$. So $abx + dby = b$. Since $d|ab$ we know that $d|LHS$ hence $d|b$.

21 (a) $(2\,x - 1)\,(x + 1)^2$: $\frac{1}{2},\ -1,\ -1$.
(b) $(x - 3)\,(x^2 + 2\,x - 1)$: Only 3, the quadratic does not factor.
(c) $(x - 2)\,(4\,x + 3)\,(x + 1)$: $2,\ -\frac{3}{4},\ -1$.
(d) $(2\,x + 1)\,(2\,x - 1)\,(x + 2)$: $-\frac{1}{2},\ \frac{1}{2},\ -2$.
(e) $(x^2 - 4\,x + 2)\,(x + 1)^2$: -1 twice; the quadratic does not factor.
(f) $(x - 2)\,(2\,x + 5)\,(2\,x - 3)\,(x + 1)$: $2,\ -\frac{5}{2},\ \frac{3}{2},\ -1$.

22 This is straightforward. The numbers we want are those coprime to the arithmetic base.

23 In each case we list them in order from 1^2 up to $(n-1)^2$.
$\mathbb{Z}_7$: 1, 4, 2, 2, 4, 1
$\mathbb{Z}_8$: 1, 4, 1, 0, 1, 4, 1
$\mathbb{Z}_{11}$: 1, 4, 9, 5, 3, 3, 5, 9, 4, 1
There is symmetry about the middle because $(n-k)^2 \equiv k^2 \pmod{n}$.

24 (a) $\gcd(11, 25) = 1 = -9 \cdot 11 + 4 \cdot 25$. So $\overline{11} \cdot \overline{-9} = \overline{1}$. Therefore $\overline{x} = \overline{19} \cdot \overline{-9} = \overline{4}$.
(b) $\gcd(11, 18) = 1 = 5 \cdot 11 - 3 \cdot 18$ and $\overline{x} = \overline{4} \cdot \overline{5} = \overline{2}$.
(c) $\gcd(16, 255) = 1 = 16 \cdot 16 - 1 \cdot 255$ (the trick was knowing that $16^2 = 256$). Now $\overline{x} = \overline{5} \cdot \overline{16} = \overline{80}$.

25

(a) $\overline{1}$ in $\mathbb{Z}_9$ has order 9. On the other hand, in $\mathbb{Z}_3 \times \mathbb{Z}_3$, every multiple of 3 gets you to $(\overline{0}, \overline{0})$.

(b) This is the same with n replacing 3 and n^2 replacing 9.

26

(a) By the standard theorem $\mathbb{Z}_{30} \cong \mathbb{Z}_2 \times \mathbb{Z}_{15}$ and $\mathbb{Z}_{15} \cong \mathbb{Z}_3 \times \mathbb{Z}_5$. Put these together and the result follows.

(b) $120 = 2^3 \cdot 3 \cdot 5$, so $\mathbb{Z}_{120} \cong \mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_5$.
$99 = 3^2 \cdot 11$, so $\mathbb{Z}_{99} \cong \mathbb{Z}_9 \times \mathbb{Z}_{11}$.
$4004 = 2^2 \cdot 7 \cdot 11 \cdot 13$, so $\mathbb{Z}_{4004} \cong \mathbb{Z}_4 \times \mathbb{Z}_7 \times \mathbb{Z}_{11} \times \mathbb{Z}_{13}$.

27 If $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$, where $m,\ n$ are coprime, then find s, t such that $sm + tn = 1$ and let $x = bsm + atn$. You may have to adjust this by adding multiples on mn to get this minimal and positive (e.g., if $x < 0$), but so long as you have the least positive residue you will have the answer.
In the given cases, the numbers required are: (a) 83 (b) 130 (c) 257 (d) 1289.

28

(a) If $1 \leq k \leq p-1$ and p is prime then both $k!$ and $(p-k)!$ contain no factor p. On the other hand $p!$ does. Thus the numerator of $\binom{p}{k}$ contains a factor p and it cannot be cancelled by anything in the denominator. The equality modulo p then follows from the binomial theorem since all other terms have a factor p.

(b) Write $a = 1 + 1 + \cdots + 1$ (a times) $= ((a-1) \cdot 1 + 1)$. Thus $a^p \equiv (a-1)^p + 1^p \equiv (a-1)^p + 1 \pmod{p}$. Similarly $(a-1)^p \equiv (a-2)^p + 1 \pmod{p}$. Thus we may strip of a contribution of 1 in each of a stages to get $a^p \equiv a \pmod{p}$ as required. [Or you can do a formal induction.] A similar argument works for negative a, and for $a = 0$ the result is obvious.

(c) Clearly if $p|a$, then $a^{p-1} \equiv 0 \pmod{p}$. And if a is not divisible by p then $\gcd(a^p, p) = 1$ so $\overline{a^p} = \bar{a}$ in $\mathbb{Z}_p^*$ by what we just proved. We can then use that $\overline{a^p} = \bar{a}^p$ in $\mathbb{Z}_p^*$ and multiply by $\bar{a}^{-1}$ in the *group* $\mathbb{Z}_p^*$. This gives $\bar{a}^{p-1} = \bar{1}$, so $a^{p-1} \equiv 1 \pmod{p}$.

29 Recall that Euler's totient function $\varphi(n)$ is the number of integers k, $1 \leq k < n$ for which $\gcd(k, n) = 1$.

(a) When p is prime, every positive integer less than p is coprime to p. Hence $\varphi(p) = p-1$.

(b) The non-coprime numbers among $1, 2, \ldots, p^r - 1$ (note we're including p^r here) are those numbers divisible by p: the gcd must be a power of p. Those are kp with $k = 1, \ldots, p^{r-1} - 1$, so $\varphi(p^r) = p^r - p^{r-1}$.

(c) The easiest approach with these is to work out what the multiples of p and/or q are among $1, 2, \ldots, pq-1$ since the gcd will have to be 1, p or q. This gives $q-1$ multiples of p together with $p-1$ multiples of q. There is no double counting here because p and q are coprime. So $\varphi(pq) = pq-1-(q-1)-(p-1) = pq-p-q+1 = (p-1)(q-1)$. Similar arguments show that $\varphi(pq^2) = (p-1)(q^2-q)$, $\varphi(p^2q^2) = (p^2-p)(q^2-q)$, and $\varphi(p^rq^s) = (p^r - p^{r-1})(q^s - q^{s-1})$. [The point with all of these is that one has to consider $1, 2, \ldots, p^rq^s$ (note we're including p^rq^s so we must make sure to exclude it as well) and that $\gcd(a, p^rq^s) \neq 1$ if and only if $p|a$ or $q|a$. This way we count the multiples of pq twice and have to correct for this; and we certainly exclude p^rq^s.]

(d) We claim that $\mathbb{Z}_{mn}^* \subseteq \mathbb{Z}_{mn}$ is mapped surjectively to $\mathbb{Z}_m^* \times \mathbb{Z}_n^* \subseteq \mathbb{Z}_m \times \mathbb{Z}_n$ in Theorem 3.23. That shows immediately that $\varphi(mn) = \varphi(m)\varphi(n)$. To see the claim note that $\gcd(r, mn) = 1$ implies $\gcd(r, m) = \gcd(r, n) = 1$ (this does not use that $\gcd(m, n) = 1$), so that $\mathbb{Z}_{mn}^*$ is mapped to $\mathbb{Z}_m^* \times \mathbb{Z}_n^*$ by Remark 3.11. To see that it is surjective, take $(\bar{a}, \bar{b})$ in $\mathbb{Z}_m^* \times \mathbb{Z}_n^* \subseteq \mathbb{Z}_m \times \mathbb{Z}_n$, and consider $\bar{c}$ in $\mathbb{Z}_m \times \mathbb{Z}_n$ mapping to

it. Then $\gcd(c, mn) = 1$: any common prime factor must come from either m or n, and since $c \equiv a \pmod m$ we have $\gcd(c, m) = \gcd(a, m) = 1$; similarly for $\gcd(c, n)$.

(e) If $n = \prod_{i=1}^{k} p_i^{r_i}$ is the factorisation of n as a product of primes, then the previous parts imply that $\varphi(n) = \prod_{i=1}^{k} \varphi(p_i^{r_i}) = \prod_{i=1}^{k} (p_i^{r_i} - p_i^{r_i - 1})$

30 In each case we form a list of things of the form $k(r)$ where k is an element and r is its least required power.
(a) 1(1), 3(4), 7(4), 9(2). $\varphi(10) = 4$.
(b) 1(1), 5(2), 7(2), 11(2). $\varphi(12) = 4$.
(c) 1(1), 2(6), 4(3), 5(6), 7(3), 8(2). $\varphi(9) = 6$.
(d) 1(1), 2(10), 3(5), 4(5), 5(5), 6(10), 7(10), 8(10), 9(5), 10(2). $\varphi(11) = 10$.
(e) 1(1), 2(4), 4(2), 7(4), 8(4), 11(2), 13(4), 14(2). $\varphi(15) = 8$.
(f) 1(1), 3(4), 5(4), 7(2), 9(2), 11(4), 13(4), 15(2). $\varphi(16) = 8$.

31 (a) $\begin{Bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 7 & 2 & 9 & 3 & 6 & 10 & 8 & 4 & 1 \end{Bmatrix}$ (b) $\begin{Bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 4 & 3 & 2 & 5 & 9 & 6 & 7 & 8 \end{Bmatrix}$

32 (a) (1 6)(2)(3 4 8)(5 7)(9 10) and (1 7 9 3 2 5 8 4 10 6).
(b) (1)(2 7 5 4)(3 9 6)(8) and (1)(2 5 7 9 8)(3 6)(4).

33 Express the results of the following products of cycles as disjoint cycles and as a product of transpositions.
(a) (1 2 5 4 6) = (1 6)(1 4)(1 5)(1 2)
(b) (1 3 5 6 4) = (1 4)(1 6)(1 5)(1 3)
(c) (1 2)(5 6)
(d) (2 8 3 6 5) = (2 5)(2 6)(2 3)(2 8)

34 The notation here matches the course summary, not the problem as originally handed out. The algorithm works by encoding a message T as $T \equiv M^d \pmod N$. We know that $N = pq$ for two primes p, q. To do the decoding we need to find $\phi(N) = (p-1)(q-1)$ and a positive number e with $de = 1 + m(p-1)(q-1)$, and determine U among $0, 1, \ldots, pq-1$ with $U \equiv M^e$ modulo pq. The number e can be found using the extended Euclidean algorithm; if we find a negative e then we can replace e and m by $e + k(p-1)(q-1)$ and $m + dk$ for any integer k and make e positive. The solutions for the given calculations are:
(a) $e = 237$, $M = 252$. (b) $e = 7139$, $M = 2004$. (c) $e = 6605$, $M = 1234$.

35

(a) In the denominator we get the product of all the negative differences $i-j$ for pairs i, j. In the numerator we get the product of, for each pair $\sigma(i), \sigma(j)$, either the positive or the negative difference of $\sigma(i)$ and $\sigma(j)$. But all pairs $\sigma(i), \sigma(j)$ $(\sigma(i) \neq \sigma(j))$ correspond to all pairs i, j $(i \neq j)$ since σ permutes $1, \ldots, n$, so apart from the sign the numerator and denominator are equal.

(b) Using the given formula we find $\varepsilon(\sigma\tau) = \varepsilon(\tau) \prod_{i<j} \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{\tau(i) - \tau(j)}$. Because τ is a permutation, all pairs $\tau(i), \tau(j)$ $(i \neq j)$ are all pairs i, j $(i \neq j)$, but we do not know if $\tau(i) < \tau(j)$ or $\tau(i) > \tau(j)$. However, since $\frac{\sigma(\tau(i)) - \sigma(\tau(j))}{\tau(i) - \tau(j)} = \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)}$ we always get the right contribution to $\varepsilon(\sigma)$ anyway, and $\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau)$.

(c) Let $\sigma = (12)$ and consider all pairs i, j with $i < j$. If $\{i, j\} \cap \{1, 2\} = \emptyset$ then $\frac{\sigma(i) - \sigma(j)}{i - j} = 1$ since $\sigma(i) = i$ and $\sigma(j) = j$. If $i = 1$ and $j = 2$ then this gives -1. The remaining pairs are of the form $1, j$ with $j > 2$ and $2, j$ with $j > 2$. But their contribution is

$$\left(\prod_{j>2} \frac{\sigma(1) - \sigma(j)}{1 - j} \right) \left(\prod_{j>2} \frac{\sigma(2) - \sigma(j)}{2 - j} \right) = \left(\prod_{j>2} \frac{2 - j}{1 - j} \right) \left(\prod_{j>2} \frac{1 - j}{2 - j} \right) = 1 \,.$$

The general case for $\sigma = (ab)$ is similar but notationally more awkward. We may assume $a < b$ (why?). Then $\frac{\sigma(i)-\sigma(j)}{i-j} = 1$ for any pair $i < j$ with $\{i, j\} \cap \{a, b\} = \emptyset$ since $\sigma(i) = i$ and $\sigma(j) = j$. For the pair a, b we get -1. The remaining pairs are the i, a with $i < a$; the a, j with $a < j < b$ or $b < j$; the i, b with $i < a$ or $a < i < b$; and the b, j with $j > b$. Their contribution is

$$\left(\prod_{i<a} \frac{\sigma(i)-\sigma(a)}{i-a}\right)\left(\prod_{a<j<b} \frac{\sigma(a)-\sigma(j)}{a-j}\right)\left(\prod_{j>b} \frac{\sigma(a)-\sigma(j)}{a-j}\right)$$
$$\left(\prod_{i<a} \frac{\sigma(i)-\sigma(b)}{i-b}\right)\left(\prod_{a<i<b} \frac{\sigma(i)-\sigma(b)}{i-b}\right)\left(\prod_{j>b} \frac{\sigma(b)-\sigma(j)}{b-j}\right)$$
$$= \left(\prod_{i<a} \frac{i-b}{i-a}\right)\left(\prod_{a<j<b} \frac{b-j}{a-j}\right)\left(\prod_{j>b} \frac{b-j}{a-j}\right)\left(\prod_{i<a} \frac{i-a}{i-b}\right)\left(\prod_{a<i<b} \frac{i-a}{i-b}\right)\left(\prod_{j>b} \frac{a-j}{b-j}\right)$$

and everything cancels because $\frac{i-a}{i-b} = \frac{a-i}{b-i}$.

(d) From (b) and (c) we know that if we write $\sigma = \tau_1 \cdots \tau_t$ with all τ_i transpositions, then $\varepsilon(\sigma) = \varepsilon(\tau_1\tau_2 \cdots \tau_t) = \varepsilon(\tau_1)\varepsilon(\tau_2 \cdots \tau_t) = \cdots = \varepsilon(\tau_1)\varepsilon(\tau_2) \cdots \varepsilon(\tau_t) = (-1)^t$. So t is always even when $\varepsilon(\sigma) = 1$ and t is always odd when $\varepsilon(\sigma) = -1$.

(e) If $\sigma = \gamma_1 \cdots \gamma_r$ is a product of disjoint cycles, with γ_i of length k_i, then each γ_i can be written as a product of $k_i - 1$ transpositions. So σ can be written as a product of $t = (k_1 - 1) + \cdots + (k_r - 1) = k_1 + \cdots + k_r - r$ transpositions, and $\varepsilon(\sigma) = (-1)^t$. This is 1 if t is even (i.e., if σ is even), and -1 if t is odd (i.e., if σ is odd).

36 Consider the element $\tau(a_i)$. Then the effect of $\tau\sigma\tau^{-1}$ on it is

$$\tau(a_i) \to a_i \to a_{i+1} \to \tau(a_{i+1})$$

(where the subscripts are taken cyclically so that $a_{k+1} = a_1$).
On the other hand, if b is an element not of the form $\tau(a_i)$, then $\tau^{-1}(b)$ is not an a_i and so σ leaves it unmoved. Thus the effect of $\tau\sigma\tau^{-1}$ on b is to leave it fixed. This proves the result. Now consider a general permutation ρ. Write $\rho = \sigma_1 \cdots \sigma_r$ as a product of disjoint cycles. Then

$$\begin{aligned}\tau\rho\tau^{-1} &= \tau\sigma_1 \cdots \sigma_r\tau^{-1} \\ &= \tau\sigma_1\tau^{-1}\tau\sigma_2\tau^{-1}\tau\sigma_3 \cdots \tau^{-1}\tau\sigma_r\tau^{-1} \\ &= \prod_{i=1}^{r} \tau\sigma_i\tau^{-1}\end{aligned}$$

In addition, since τ is a permutation, the fact that the σ_i are disjoint cycles implies that the $\tau\sigma_i\tau^{-1}$ are also disjoint cycles. By the first part they have the same lengths, so the cycle types of ρ and $\tau\rho\tau^{-1}$ are the same.

37 Let g, h be any two elements in G. Then $(gh)^2 = e$ gives $ghgh = e$. Multiply this on the left by g and on the right by h to find $g^2hgh^2 = geh$, and since $g^2 = h^2 = e$ this simplifies to $hg = gh$, so the group is Abelian.

38 Let $r > 0$. Then $(gh)^r = e$ if and only if $h(gh)^r h^{-1} = heh^{-1}$, which simplifies to $(hg)^r = e$ (use the definition of $(gh)^r$). So gh has finite order if and only if hg has finite order, and if that is the case the order (the smallest positive r such that equality holds) must be the same for gh and hg.

39 Group together g and g^{-1} whenever $g \neq g^{-1}$. (Since $(g^{-1})^{-1} = g$ we really get pairs here.) This uses an even number of elements in the group, so since the group has an even number of elements, we are left with an even number of elements. But those elements are

those g where $g = g^{-1}$, i.e., $g^2 = e$. So those are exactly the elements of order 1 or 2. Since there is exactly one element of order 1, the number of elements of order 2 must be odd.

40 One way round is trivial: a subset that is a subgroup must be closed. We need to prove the converse is true for a non-empty subset in a finite group.
So let X be such a non-empty set. By Lemma 5.3(2) it suffices to show that X is closed under taking inverses since it is closed under taking products. Take $x \in X$. Since X is closed under multiplication, $x,\ x^2,\ x^3, \dots$ are also in X. As G is finite, we must have $x^i = x^j$ for some $0 < i < j$. Then $x^{-1} = x^{j-i-1}$. If $j - i > 1$ then x^{j-i-1} is in X. If $j - i - 1 = 0$ then $x^{-1} = e$ so $x^{-1} = e = x$ is in X as well. [Alternatively, $x^{-1} = x^{2(j-i)-1}$ is always in X.]
The statement is always false if G has an element of infinite order. For example, if $G = \mathbb{Z}$ then the non-empty subset $X = \{1, 2, 3, \dots, \}$ is closed under addition but is not a subgroup.

41

(a) If $x \in X$ then $gxg' \in gXg'$ is a trivial consequence. Suppose conversely, that $gxg' \in gXg'$, then this means that we can find $x' \in X$ with $gxg' = gx'g'$ [this is the non-trivial observation]. But this means that $x = g^{-1}gxg'g'^{-1} = g^{-1}gx'g'g'^{-1} = x'$ and so $x = x' \in X$ as required.

(b) Suppose that X is a subgroup of G. Then consider ab^{-1} for two elements $a = gxg^{-1}$ and $b = gyg^{-1}$ both in gXg^{-1}:

$$ab^{-1} = gxg^{-1}(gyg^{-1})^{-1} = gxg^{-1}(g^{-1})^{-1}y^{-1}g^{-1} = gxg^{-1}gy^{-1}g^{-1} = gxy^{-1}g^{-1}$$

But since X is a subgroup, $xy^{-1} \in X$ and so $ab^{-1} \in gXg^{-1}$. This is enough to demonstrate that gXg^{-1} is a subgroup also.

Conversely, if gXg^{-1} is a subgroup, then applying the above argument, so is $g^{-1}(gXg^{-1})(g^{-1})^{-1} = X$.

42 $Z(G)$ is the set of all elements that commute with every element of G. Since $eg = ge = e$ for every $g \in G$, the identity $e \in Z(G)$. If $z \in Z(G)$ then for any $g \in G$, z must commute with g^{-1}, i.e. $zg^{-1} = g^{-1}z$ Taking inverses of both sides, this gives $gz^{-1} = z^{-1}g$ for every $g \in G$. So $Z(G)$ contains inverses.
Finally, it is also closed under multiplication, since if $y,\ z \in Z(G)$ and $g \in G$, $gyz = ygz = yzg$. so $yz \in Z(G)$.
Finally, note that if $z \in Z(G)$, then $gzg^{-1} = gg^{-1}z = z$ which proves the final part.

43 We use Lemma 3.9.

(a) First of all, $\varphi(e_G) = e_H$ so $\ker(\varphi)$ is non-empty. Let $g_1,\ g_2 \in \ker(\varphi)$, so $\varphi(g_1) = \varphi(g_2) = e_H$. Then $\varphi(g_1g_2^{-1}) = \varphi(g_1)\varphi(g_2^{-1}) = e_H\varphi(g_2)^{-1} = e_H^{-1} = e_H$ and so $g_1g_2^{-1} \in \ker(\varphi)$. Therefore $\ker(\varphi)$ is subgroup of G.

(b) Let $h_1,\ h_2 \in \mathrm{im}(\varphi)$, then we can find $g_i \in G$ with $\varphi(g_i) = h_i$ $(i = 1,\ 2)$. Ten $\varphi(g_1g_2^{-1}) = \varphi(g_1)\varphi(g_2^{-1}) = h_1h_2^{-1}$ and so $h_1h_2^{-1} \in \Im(\varphi)$ and $\mathrm{im}(\varphi)$ is also a subgroup.

44 Let $g,\ h \in G$. Then $\varphi(gh) = \varphi(g)\varphi(h)$ gives $ghgh = g^2h^2$. Cancel g on the left and h on the right and we get $hg = gh$.

45 If φ is injective then $\varphi(g) = e_H = \varphi(e_G)$ implies that $g = e_G$ and so $\ker(\varphi) = \{e_G\}$.
Conversely, if $\ker(\varphi) = \{e_G\}$, then $\varphi(g_1) = \varphi(g_2)$ gives $\varphi(g_1g_2^{-1}) = \varphi(g_1)\varphi(g_2)^{-1} = e_H$ and so $g_1g_2^{-1} = e_G$, hence $g_1 = g_2$.

46 Let $G = \{g_1, \dots, g_n\}$. Let $g \in G$, then the ordered sequence

$$gg_1, gg_2, \dots, gg_n$$

is a permutation of the original ordered sequence $g_1, \dots, g_n$. In other words we can write $gg_i = g_{\sigma_g(i)}$ for a permutation we call $\sigma_g \in S_n$.
The association $g \to \sigma_g$ then allows us to define a function $\varphi : G \to S_n$, by $\varphi(g) = \sigma_g$.

It is then an easy calculation that for $g,\ h \in G$, $\sigma_{gh} = \sigma_g\sigma_h$. Therefore $\varphi(gh) = \varphi(g)\varphi(h)$ and φ is a homomorphism.
Finally, suppose that σ_g is the identity permutation. This means that for all g_i, $gg_i = g_i$. But the only element of G for which this is true is e_G. Thus $\ker(\varphi) = \{e_G\}$, so φ is injective. It is surjective onto its image $\mathrm{im}(\varphi)$, which is a subgroup of S_n because φ is a homomorphism. G is therefore isomorphic to $\mathrm{im}(\varphi)$.

47 $|G| > 1$ and so there exists an element $g \in G$ with $g \neq e$. Since $|g|$ divides $|G|$, g has order p^s for some $s \leq r$. Now just choose $h = g^{p^{s-1}}$ and h clearly has order p.

48 $T(a,b)T(c,d) = T(ac, ad+b)$, so we have closure. Associativity is trivial as we are dealing with functions. $e = T(1,0)$ and $T(a,b)^{-1} = T(\frac{1}{a}, -\frac{b}{a})$ (which is where $a \neq 0$ is required).
H is clearly a subgroup: it is non-empty ($T(1,0)$ is in it); if g, h are in H then gh^{-1} is in H since $1\frac{1}{1} = 1$.
Multiplying on the right or left by $T(1,c)$ changes $T(a,b)$ into something of the form $T(a,*)$ for some number $*$. So any left or right coset must have elements of the form $T(a,b)$ where a is constant. On the other hand, $T(a,b) = T(a,c)T(1,\frac{b-c}{a}) = T(1,b-c)T(a,c)$ and so two such objects are always in the same left and right cosets. Thus a left or right coset is all transformations where the value a is fixed. [Note that in this case left and right cosets always coincide, even though the group is not commutative.]

49 Disjoint cycles commute, so $\sigma^m = \gamma_1^m\gamma_2^m\cdots\gamma_r^m$. This can equal e if and only if $\gamma_i^m = e$ for all i, so each k_i divides m.

50 For $a = 1, \ldots, p-1$ we have $\bar{a}^{p-1} = \bar{1}$ in $\mathbb{Z}_p^* \subset \mathbb{Z}_p$ by Theorem 3.27. (We use that p is prime to see that $\bar{a}$ is in $\mathbb{Z}_p^*$ for those values of a.) Multiplying by $\bar{a}$ gives that $\bar{a}^p = \bar{a}$ for $\bar{a} = \bar{1}, \bar{2}, \ldots, \overline{p-1}$, and for $\bar{a} = \bar{0}$ it clearly holds. So $a^p \equiv a$ modulo p for any integer a.

51

(a) Clearly e is in A_n so A_n is non-empty. The inverse of an even permutation is even (why?), and the product of two even permutations is even, so A_n is a subgroup. [Alternatively, $A_n = \ker(\varepsilon)$ where $\varepsilon : S_n \to \{\pm 1\}$ is as in Question 35; it is a homomorphism by part (b) of that question.]

(b) We claim that there are two left cosets of A_n in S_n when $n \geq 2$: A_n and $(12)A_n$. For this we only have to check that $(12)A_n$ is the set of odd permutations in S_n. But if σ is an odd permutation, then $(12)\sigma$ is even so lies in A_n, hence $(12)(12)\sigma = \sigma$ lies in $(12)A_n$. Conversely, any element in $(12)A_n$ is odd. So $|S_n : A_n| = 2$, and therefore $|S_n| = 2|A_n|$ gives the result.

52 Finite Abelian groups are always products of finite cyclic groups. For each order n we have $\mathbb{Z}_n$ which finishes the list for any prime order. Also we know that $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ if $\gcd(m,n) = 1$, which means that this also deals with $n = 6,\ 10$. So we only have $n = 4,\ 8,\ 9,\ 12$ left.
Then we can start with any $\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_t}$ with $d_1 d_2 \cdots d_t = n$ and rearrange things as on page 23 of the course summary to find that in these cases, we have, apart from $\mathbb{Z}_n$:
$n = 4:\ \mathbb{Z}_2 \times \mathbb{Z}_2$.
$n = 8:\ \mathbb{Z}_2 \times \mathbb{Z}_4,\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.
$n = 9:\ \mathbb{Z}_3 \times \mathbb{Z}_3$.
$n = 12:\ \mathbb{Z}_2 \times \mathbb{Z}_6$ (since $\mathbb{Z}_3 \times \mathbb{Z}_4 \cong \mathbb{Z}_{12}$).

53 We get a start from the fact that $|\mathbb{Z}_n^*| = \varphi(n)$ (Euler's totient function).
(a) $\varphi(3) = 2$ and so we must have $\mathbb{Z}_2$.
(b) $\varphi(5) = 4$ and $\bar{2}$ has order 4, so we get $\mathbb{Z}_4$.
(c) $\varphi(6) = 2$ and so we must have $\mathbb{Z}_2$.

(d) $\varphi(7) = 6$ and $\bar{3}$ has order 6, so we get $\mathbb{Z}_6$.
(e) $\varphi(8) = 4$ and every element has order 1 or 2, so we get $\mathbb{Z}_2 \times \mathbb{Z}_2$.
(f) $\varphi(9) = 6$ and $\bar{2}$ has order 6, so we get $\mathbb{Z}_6$.
(g) $\varphi(12) = 4$ and and every element has order 1 or 2, so we get $\mathbb{Z}_2 \times \mathbb{Z}_2$.
(h) $\varphi(15) = 8$ and we have elements of order 4 but none of order 8, so we must have $\mathbb{Z}_2 \times \mathbb{Z}_4$.
(i) $\varphi(21) = 12$ and we have elements of order 6 but none of order 12, so we must have $\mathbb{Z}_2 \times \mathbb{Z}_6$.
(j) $\varphi(24) = 8$ and every element has order 1 or 2, so we must have $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

54 This can be quite a long and tedious question. **In each case we do not list the trivial subgroup, the whole group, and cyclic subgroups.** The cyclic subgroups can be easily calculated by taking all elements in the group and computing which subgroup they generate (but several elements may lead to the same cyclic subgroup).
In order to find the **other** subgroups, the general starting point is to think about the order of the group and any consequences of Lagrange's theorem.

(a) There are no other subgroups as $S_3 = 6$ and the only proper divisors of 6 are primes.
(b) $D_4 = 8$ and the only proper non-prime divisor of it is 4, so a non-cyclic proper subgroup would have 4 elements, 3 which have order 2. Since the only rotation of order 2 is r^2 there must be two reflections. Since the product of two distinct reflections is a rotation (and not the identity symmetry), and the only rotation of order 2 is r^2, this shows $\{e, r^2\}$ is part of such a subgroup. If we then add in a reflection and see what this implies for the fourth element we get the solutions: $\{e, r^2, h, r^2h\}$, $\{e, r^2, rh, r^3h\}$. Note that it requires *checking* that those are indeed subgroups.
(c) The only proper divisors of $|D_5| = 10$ are primes so there are no other subgroups.
(d) $|D_6| = 12$ which has proper non-prime divisors 4 and 6. The same reasoning and checking as in (b) leads to the 3 subgroups $\{e, r^3, r^ih, r^{i+3}h\}$ $(i = 0, 1, 2)$ of order 4.

Non-cyclic groups of order 6 are isomorphic to S_3, so must contain 2 elements of order 3 and 3 elements of order 2. The only elements of order 3 are r^2 and r^4, the only elements of order 2 are r^3 and the reflections. A subgroup containing r^2 and r^3 contains $\langle r \rangle$, which has six elements but is cyclic, so we ignore it. So the elements of order 2 must all be reflections. Adding a reflection then gives only the candidate subgroups $\{e, r^2, r^4, r^ih, r^{i+2}h, r^{i+4}h\}$ for $i = 0, 1$. Checking that those are subgroups can be done by a brute force calculation. But we can also inscribe two equilateral triangles inside a regular hexagon (with vertices on vertices), and the elements in D_6 preserving one of those triangles (i.e., preserving even more symmetry) must form a non-cyclic subgroup with 6 elements. So there *must* be 2 non-cyclic subgroups with 6 elements, and the subsets we found must be subgroups.
(e) $|D_8| = 16$, which has non prime divisors 4 and 8. The same argument as in (b) and (d) leads to 4 non-cyclic groups all of the form $\{e, r^4, r^ih, r^{i+4}h\}$, $i = 1,\ 2,\ 3,\ 4$.

If we look for a group of order 8, then if all the elements had order 1 or 2, we would need at least 6 reflections. But combining a fixed reflection with five other reflections gives five different rotations, so their orders get too big. Hence such a subgroup has an element of order 4, which must be r^2 or r^6. Either way, it contains $\{e, r^2, r^4, r^6\}$. Adding a reflection we see that only $\{e, r^2, r^4, r^6, h, r^2h, r^4h, r^6h\}$ and $\{e, r^2, r^4, r^6, rh, r^3h, r^5h, r^7h\}$ are candidate subgroups. These are indeed subgroups, the subgroups preserving one of the two squares that can be inscribed in a regular hexagon.