ALGEBRA QUESTION SHEET

Harder questions are normally marked (*).

1 Prove that the following sets form infinite groups with respect to ordinary multiplication:

(a) $\{2^k\}$ where $k \in \mathbb{Z}$.

(b) $\{\frac{1+2m}{1+2n}\}$ where $m,\ n \in \mathbb{Z}$.

(c) $\{\cos\theta + i\sin\theta\}$ where θ runs over all rational numbers.

2 Think of the integers $\mathbb{Z}$ as points equally spaced along the real line. Define two kinds of transformations on $\mathbb{Z}$:
(1) Translations of the form T_a (where a is an integer) which have the effect of translating $\mathbb{Z}$ a places to the right (if $a \geq 0$; or $-a$ places to the left if $a < 0$) using the formula $n \mapsto n + a$.
(2) Reflections of the form R_c (where c is an integer) which have the effect of reflecting $\mathbb{Z}$ in the point $\frac{c}{2}$ using the formula $n \mapsto c - n$.
Work out the effect of composing the following pairs of transformations: (a) T_bT_a, (b) R_dT_a, (c) T_bR_c, (d) R_dR_c. [In each case, because these are *functions* the compositions have to be evaluated from right to left; e.g., T_bT_a means first do T_a and then do T_b.]
Now let A be the set of all such T_a and R_c. Show that A is a group and that we can find examples of elements $g,\ h \in A$ such that $gh \neq hg$, $g^2 = h^2 = e$ and $\forall s > 0,\ (gh)^s \neq e$.
[Note: A is called the group of *affine transformations* on $\mathbb{Z}$. There are more general groups of affine transformations on $\mathbb{R},\ \mathbb{R}^2,\ \mathbb{R}^3$ etc.]

3 Define a composition $*$ on the integers $\mathbb{Z}$ by

$$n * m = n + m + nm$$

Show that under this composition, $\mathbb{Z}$ is closed, associative and has an identity element. Does it have inverses?

4

(a) Let $G = \{e, a, b\}$ be a group with identity element e. Show that there is only one possible multiplication table for G [so that groups of order 3 have to have the same underlying structure].

(b) (*) Let $G = \{e, a, b, c\}$ be a group with identity element e. Show that this time there are essentially just two possible multiplication tables for G so that groups of order 4 have to have one of two distinct underlying structures. (Here "essentially" means that we may have to rename a, b and c in order to get one of the two tables.)

5

(a) Let G be the set of all 2×2 matrices of the form $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ where $a,\ b,\ d \in \mathbb{R}$, and $ad \neq 0$. Show that G is a group under matrix multiplication.

(b) With G as in part (a), define $Z(G) = \{g \in G \,|\, \text{such that}, \forall h \in G,\ gh = hg\}$. Identify the elements of $Z(G)$ and show that it is also a group. [$Z(G)$ is called the *centre* of G.]

6 Give a formal proof that every integer can be written either as $2k$ or as $2k + 1$ for some $k \in \mathbb{Z}$. [This means prove Theorem 2.1 in this case – you cannot simply assume it. If you need to, look into Whitehead's book.]

7 Let $a,\ b,\ d \in \mathbb{Z}$ and suppose $d|a$ and $d|b$. Prove that $\forall m,\ n \in \mathbb{Z}$, $d|(ma + nb)$.

8

(a) Consider the integers $n = 0, 1, \ldots, 11$. For each *either* find the smallest positive integer q such that the product nq has remainder 1 when divided by 12 *or* say why no such q can exist.
(b) Repeat the exercise in (a) with 12 replaced by 30.
(c) What general observations can one make about the outcomes of the above calculations?

9 Let $d > 0$ be an integer. Show that any consecutive ascending sequence of d integers $(n,\ n+1, \ldots, n+d-1)$ contains just one number divisible by d.

10 A **prime pair** is a pair of consecutive odd numbers that are primes (e.g., 11 and 13, or 17 and 19); a **prime triple** consists of three consecutive odd numbers that are primes. There are many prime pairs (indeed there is a famous unproved conjecture that states there are infinitely many). Prove that there is only one prime triple and find it.

11

(a) There is a simple test for whether a number is divisible by 9, which involves a calculation on the decimal digits of the number. Find out what it is. Prove that it works.
(b) Do the same for divisibility by 11.

12 **Eratosthenes Sieve** Write down the integers $2, 3, \ldots, 30$ in ascending order. Call the first element of this list (i.e., 2) p_1.
Now cross out all the multiples of $p_1 = 2$. Call the first element of what remains p_2; what is it?
Next, cross out all the multiples of p_2 in what is left. Call the first element of what remains p_3; what is it?
Next, cross out all the multiples of p_3 in what is left. Call the first element of what remains p_4; what is it?
What is the common property of $p_1,\ p_2,\ p_3,\ p_4$? Why is that property shared with *all* the remaining numbers in the list. [If you cannot spot this, look up 'Eratosthenes Sieve' on the web using Google.]
Finally, we started with the number 30 and did just 4 iterations to get the final result. How many iterations are required if we started with (a) 100, (b) 1,000, (c) 10,000, (d) 10^n? [A general statement is required in (d), not the actual number – in general it is somewhat difficult to find.]

13 Let n be a positive integer. Show that none of the integers $n! + k$, $2 \leq k \leq n$ are prime (i.e., they are all composite). Find a sequence of 10 consecutive positive composite integers. CHALLENGE: Find the lowest such sequence.

14 For a long time, people have been looking for a 'nice' formula to construct all the primes. While there are some very un-nice ones, there are some interesting equations. E.g., x^2+x+41 is prime for a certain sequence of 80 consecutive integers.
Find a value of x for which $x^2 + x + 41$ is not prime.

15 (*) Given a positive integer n, let $\sigma(n)$ be the sum of all the divisors of n less than n. (So $\sigma(4) = 1+2 = 3,\ \sigma(10) = 1+2+5 = 8,\ \sigma(15) = 1+3+5 = 9.$) A number where $\sigma(n) = n$ is called **perfect**. So $6 = 1+2+3$ and $28 = 1+2+4+7+14$ are perfect.
Let p be prime and $n = 2^k p$. Write down all the divisors of n less than n, and compute $\sigma(n)$ in this case. Deduce that, if $p = 2^{k+1}-1$, then n is perfect. Find two more perfect numbers.
[*It is conjectured that all perfect numbers are even. In fact all the even ones have the form stated above. If you start looking for odd ones, they have at least 8 different primes as factors and must be very, very large.*]

16

(a) **Mersenne Primes** Show that if $a,\ b$ are positive integers such that $a|b$, then $(x^a - 1)|(x^b - 1)$ as polynomials in x. [Hint: consider what happens when you add up the geometric series that starts at 1, has ratio x^a and has $\frac{b}{a}$ terms]. Deduce that if $2^n - 1$ is prime, then n is prime.
(b) Find the lowest prime p such that $2^p - 1$ is *not* prime [Maple will help here].
(c) **Fermat Primes** Show that if $a,\ b$ are positive integers such that $a|b$ *and* $\frac{b}{a}$ is odd, then $(x^a + 1)|(x^b + 1)$ regarded as polynomials in x [there is a similar hint]. Deduce that if $2^n + 1$ is prime, then n is a power of 2.
(d) Find the lowest n such that $2^{2^n} + 1$ is *not* prime [Maple will again help here].

17 A linear combination of integers $a,\ b$ is an expression of the form $ax + by$ where $x,\ y$ are also integers.
Show that any integer n can be written as a linear combination of (a) 2 and 3, (b) 5 and 7, (c) 8 and 13. [Here you should 'spot' the answers rather than use the Euclidean Algorithm.]

18 In each of the following use Euclid's algorithm to work out the greatest common divisor of the two given integers and express it as a linear combination of the two numbers: (a) 26, 44, (b) 1169, 3493, (c) 182, 589, (d) 1573, 2860, (e) 22103, 33580, (f) 1229, 22861.

19 Find integers $x,\ y$ such that $45x + 63y = 90$. Can we find integers $s,\ t$ such that $45s + 63t = 80$? Either find them or prove they cannot exist

20 Let $a,\ b,\ d$ be non-zero integers such that $\gcd(a, d) = 1$ and $d|ab$. Show that $d|b$. [Theorem 2.5 must not be used here: this statement is used to prove the uniqueness part of that theorem!]

21 Find the rational roots of the following polynomials: (a) $2x^3 + 3x^2 - 1$, (b) $x^3 - x^2 - 7x + 3$, (c) $4x^3 - x^2 - 11x - 6$, (d) $4x^3 + 8x^2 - x - 2$ (e) $x^4 - 2x^3 - 5x^2 + 2$ (f) $4x^4 - 27x^2 + 7x + 30$.

22 Write down the addition and multiplication tables for arithmetic modulo n when (a) $n = 4$, (b) $n = 6$, (c) $n = 7$. In each case identify those elements $\bar{x}$ for which there exists $\bar{y}$ with $\bar{x} \cdot \bar{y} = \bar{1}$.

23 In $\mathbb{Z}_n$, denote $\bar{a} \cdot \bar{a}$ by $\bar{a}^2$. Tabulate the values $\bar{a}^2$ for the non-zero elements in each of $\mathbb{Z}_7,\ \mathbb{Z}_8,\ \mathbb{Z}_{11}$. Why is there the apparent symmetry in the respective tables?

24 In each of the following, use Euclid's algorithm to find the multiplicative inverse of $\bar{a}$ in $\mathbb{Z}_n^*$ and find $\bar{x}$ such that $\bar{a}\bar{x} = \bar{b}$ in $\mathbb{Z}_n$: (a) $n = 25$, $a = 11$, $b = 19$; (b) $n = 18$, $a = 11$, $b = 4$; (c) $n = 255$, $a = 16$, $b = 5$. If you are good at mental arithmetic there is a very quick way to do the third of these. What is it?

25 (a) Compare $\mathbb{Z}_3 \times \mathbb{Z}_3$ with $\mathbb{Z}_9$ and show that they cannot be isomorphic [Hint: what happens to $\bar{1}$ in $\mathbb{Z}_9$ when you add it to itself several times. How long before you get back to $\bar{0}$?]
(b) Show that when $n \geq 2$ $\mathbb{Z}_n \times \mathbb{Z}_n$ cannot be isomorphic to $\mathbb{Z}_{n^2}$.

26 (a) Show that $\mathbb{Z}_{30}$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$.
(b) Using a similar approach, how finely can you decompose $\mathbb{Z}_{120}$? $\mathbb{Z}_{99}$? $\mathbb{Z}_{4004}$?

27 In each of the following, solve the simultaneous congruences to find the smallest positive number x that satisfies both:

(a) $x \equiv 5 \pmod{13}$ and $x \equiv 7 \pmod{19}$;
(b) $x \equiv 11 \pmod{17}$ and $x \equiv 15 \pmod{23}$;
(c) $x \equiv 4 \pmod{11}$ and $x \equiv 14 \pmod{27}$;
(d) $x \equiv 5 \pmod{12}$ and $x \equiv 14 \pmod{25}$ and $x \equiv 15 \pmod{49}$.

28

(a) Let p be a prime number. Recall that the binomial coefficient $\binom{p}{k} = \frac{p!}{k!(p-k)!}$. Show that if $1 \leq k \leq p-1$, then $\binom{p}{k} \equiv 0 \pmod{p}$. Deduce that, for every pair of integers $a,\ b$, $(a+b)^p \equiv a^p + b^p \pmod{p}$.
(b) Use part (a) to deduce that if p is prime, then for every integer a, $a^p \equiv a \pmod{p}$.
(c) From the above, when p is prime, for what values a is it true that $a^{p-1} \equiv 1 \pmod{p}$?

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) Work out $\varphi(p)$ when p is prime.
(b) For p prime and $r > 1$, write down all the integers among $1, 2, \ldots, p^r - 1$ with a common divisor greater than 1 with p^r, and find $\varphi(p^r)$.
(c) Let $p,\ q$ be distinct primes. Work out $\varphi(pq),\ \varphi(pq^2),\ \varphi(p^2q^2),\ \varphi(p^rq^s)$. These are algebraic formulae in terms of p and q. In each case show that they can be expressed as a product of an expression involving only p and one involving only q.
(d) (*) Show that if $\gcd(m, n) = 1$, then $\varphi(mn) = \varphi(m)\varphi(n)$. [Hint: use Theorem 3.23 and Remark 3.11.]
(e) From the previous part, deduce a general formula for $\varphi(n)$ in terms of the prime factorisation of n.

30 In each of the following, list all the positive integers r less than n that are coprime to n and for each find the smallest positive integer k such that $r^k \equiv 1 \pmod{n}$. In each case verify that k is a divisor of $\varphi(n)$.
(a) $n = 10$ (b) $n = 12$ (c) $n = 9$ (d) $n = 11$ (e) $n = 15$ (f) $n = 16$.

31 For the following pairs of permutations σ, τ, compute $\sigma\tau$:

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

(b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 7 & 9 & 2 & 4 & 3 & 5 & 8 & 6 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 5 & 6 & 4 & 7 & 3 & 9 & 2 & 8 \end{pmatrix}$

32 Express each of the four permutations displayed in the previous question as a product of disjoint cycles.

33 Express the results of the following products of permutations cycles as disjoint cycles and as a product of transpositions.
(a) (1 3 4 6)(2 5)(3 1 5)
(b) (1 2)(6 4 2 3 5)(1 2)
(c) (5 4 3 2 1)(2 4 6 1 3)(1 2 3 4 5)(5 3 1)
(d) (1 2 4 8)(3 2 4 7)(6 5 4 3)(8 7 5 1)

34 [RSA cryptography] Alice sends Bob a number M that is obtained by encrypting a number T according to the RSA algorithm: raise T to the power d and reduced modulo N to give the residu M in the range $0, 1, \ldots, N-1$. In each of the following cases, find the original number T when:

(a) $M = 45$, $d = 13$, $N = 667$.
(b) $M = 4063$, $d = 59$, $N = 7979$.
(c) $M = 14756$, $d = 5$, $N = 16781$.

In each case, the answers are "recognisable" numbers. You will find it useful to use Maple, and in particular the *irem* and *ifactor* functions. irem(a,b) gives the remainder when the integer a is divided by the integer b; so it gives the residue of a modulo b. ifactor(n) factorises the integer n.

35 (*) Let $n \geq 2$. For a permutation σ in S_n we define

$$\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j}\,.$$

(a) Show that $\varepsilon(\sigma) = \pm 1$.
(b) Writing $\frac{\sigma(\tau(i))-\sigma(\tau(j))}{i-j} = \frac{\sigma(\tau(i))-\sigma(\tau(j))}{\tau(i)-\tau(j)} \frac{\tau(i)-\tau(j)}{i-j}$, show that $\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau)$ for any σ, τ in S_n.
(c) Compute $\varepsilon((12))$ and, more generally, $\varepsilon((ab))$ for any transposition (ab).
(d) Show that if σ is written as a product of t transpositions, then $\varepsilon(\sigma) = (-1)^t$.
(e) Finally, verify that $\varepsilon(\sigma) = 1$ if σ is even and -1 if σ is odd.

36 (*) Let $\sigma = (a_1\ a_2\ \ldots\ a_k)$ be a k-cycle, and τ a permutation in S_n. Show that $\tau\sigma\tau^{-1} = (\tau(a_1)\ \tau(a_2)\ \cdots\ \tau(a_k))$ and so is also a k-cycle. Deduce that for any two permutations $\rho,\ \tau \in S_n$, $\tau\rho\tau^{-1}$ has the same cycle type as ρ. [Hint: write ρ as a product of disjoint cycles, insert the identity permutation e between each cycle and use the fact that $\tau^{-1}\tau = e$.]

37 Let G be a group such that for every element $g \in G$, $g^2 = e$. Show that G is Abelian.

38 Prove that, if $g,\ h$ are elements of the group G then gh and hg have the same order.

39 Prove that a group of even order has an odd number of elements of order 2. [Hint: group together g and g^{-1}. When are they the same?]

40 Let G be a finite group and let X be a non-empty *subset* of G. Show that X is a subgroup of G if and only if for every $x,\ x' \in X$, $xx' \in X$. Give an example to show that this is no longer true if G is not required to be finite.

41 Let X be a sub*set* of a group G. For fixed elements $g,\ g' \in G$, define $gXg' = \{gxg' | x \in X\}$. Show that

(a) $x \in X$ if and only if $gxg' \in gXg'$. [This is *not* absolutely trivial.]
(b) if $g \in G$ is fixed, then X is a sub*group* of G if and only if gXg^{-1} is a subgroup of G.

42 Let G be a group. Define the *centre* of G to be $Z(G) = \{g \in G |$ for all $h \in G,\ gh = hg\}$ (i.e., the set of elements that commute with *everything* in G). Show that $Z(G)$ is a subgroup of G and that for every $g \in G,\ gZ(G)g^{-1} = Z(G)$.

43 Recall that a function $\varphi : G \to H$ between two groups is a *homomorphism* if, $\forall g_1,\ g_2 \in G$, $\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2)$. The *kernel* of φ is the set $\ker(\varphi) = \{g \in G | \varphi(g) = e_H\}$. The *image* of φ is the set $\mathrm{im}(\varphi) = \{\varphi(g) | g \in G\} \subseteq H$

(a) Show that $\ker(\varphi)$ is a subgroup of G.
(b) Show that $\mathrm{im}(\varphi)$ is a subgroup of H.

44 Let $\varphi : G \to G$ be the function $\varphi(g) = g^2$. Show that if φ is also a homomorphism, then G is an Abelian group.

45 Show that a homomorphism $\varphi : G \to H$ is injective if and only if $\ker(\varphi) = \{e_G\}$.

46 [Cayley's Theorem] Show that if G is a finite group of order n, then G is isomorphic to a subgroup of S_n. [Hint: number the elements of G and think what happens to the list when you multiply all of them all simultaneously on the left by the same element of G.]

47 Let p be a prime number and G a group of order p^r for some $r > 0$. Show that G contains a subgroup of order p. [Hint: think about the subgroup generated by a non-identity element of G.]

48 Define $T(a, b)$ to be the set of transformations of the real line given by $x \mapsto ax + b$ where $a,\ b$ are real with $a \neq 0$.
Show that the set G of all the $T(a, b)$ forms a group under composition of functions. Let $H \subset G$ be all the transformations where $a = 1$. Show that H is a subgroup of G and describe the left and right cosets of H in G.

49 Let $\sigma = \gamma_1\gamma_2 \cdots \gamma_r$ be a permutation in S_n expressed as a product of disjoint cycles, where γ_i is a cycle of length k_i. Prove that the order of σ is $\mathrm{lcm}(k_1, k_2, \ldots, k_r)$.

50 Let p be a prime number and let $G = \mathbb{Z}_p^*$. Use Lagrange's theorem on G to prove that for every integer a, $a^p \equiv a \pmod{p}$ [Fermat's little theorem]. [Hint: consider the order of $\bar{a}$ in G. Don't forget other values of a.]

51 Let A_n be the set of all *even* permutations in S_n. Show that (a) A_n is a subgroup of S_n, and that $|A_n| = n!/2$ when $n \geq 2$. [A_n is called the *alternating group* on $\{1, \ldots, n\}$.] [Hint: how do the parities of permutations work when you multiply them? Use the answer to this to work out how many cosets A_n has in S_n.]

52 List all the abelian groups (up to isomorphism) as far as order 12.

53 This question considers the structure of $\mathbb{Z}_n^*$. It is a fact that $\mathbb{Z}_n^*$ for $n \geq 3$ is isomorphic to a cartesian product of the form $\mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2} \times \cdots \times \mathbb{Z}_{r_t}$ for some $t \geq 1$, and integers $r_1, r_2, \ldots, r_t$ with all $r_i \geq 2$ and each one dividing the next (so $r_1 | r_2$, $r_2 | r_3$, etc.). For each of the following values of n, determine the corresponding structure of $\mathbb{Z}_n^*$: (a) 3 (b) 5 (c) 6 (d) 7 (e) 8 (f) 9 (g) 12 (h) 15 (i) 21 (j) 24. [Hint: in each case work out the order of each element and use the list to determine which group structure must be present, using that $r_1 r_2 \cdots r_t = \varphi(n)$.]

54 List all the subgroups of (a) S_3, (b) D_4, (c) D_5, (d) D_6, (e) D_8.