Mathematics 205 Abstract Algebra

Professor Peter M. Higgins

March 10, 2018

The purpose of modern abstract algebra is to study important aspects of algebra in their own right without binding it to particular mathematical ideas or applications. This pursuit set much of mathematics free as the underlying structure of the subject was revealed. To decide on which aspects are important, standard examples are used as motivation and so in this module we will never be far away from familiar objects such as the integers or matrices. However the feel is decidely pure mathematical with much more emphasis on proof that on calculations.

The first problem set recounts basic ideas of functions and relations. Set 2 introduces algebras with a single operation, they being *semigroups, monoids* and *groups*. The emphasis will be on group theory throughout. However Set 3 introduces algebras with two operations linked by distributivity, these being *rings* and *fields*. Set 4 introduces more fundamental ideas such as generating sets and subalgebras as they apply to groups and rings.

In Set 5 we begin classical group theory and here we meet *Lagrange's theorem* based on counting *cosets* of subgroups. In Sets 5 and 6 we meet the idea of *normal subgroup* and its relationship to *homomorphisms* and *quotient groups*. In Set 7 we run through the three basic *isomorphism theorem*s for groups and the *1st isomorphism theorem* as it applies to rings. Set 8 is about commutativity within groups and here we meet the *Fundamental structure theorems for abelian groups* and other asepcts of group commutativity including *centralizers*, the *centre of a group*, and the *class equation.*

The final two problem sets investigate the *Symmetric group* and we work through the proof of *Cayley's theorem.* Finally we meet the *Alternating group* and the notion of *even* and *odd permutations.*

Solutions and Comments for the Problems

Problem Set 1

1. Directly from the definition we get $R \circ S = \{(1, w), (1, x), (3, y), (4, y)\}$.

Comment We can, by imposing a total ordering on A and B, represent relations as binary $|A| \times |B|$ matrices with a 1 at (i, j) if the corresponding pair is in R. The product of the corresponding matrices $M_R M_S = M_{R \circ S}$ if we use the addition $1 + 1 = 1$. (An entry in the product is n if there are n pairs of the form $(i, j) \in R$ and $(j, k) \in S$; we are however only interested if $n \geq 1$ or if $n = 0$.)

2. R is not reflexive as $(0, 0) \notin R$; R is symmetric as $(a, b) \in R \Rightarrow ab > 0 \Rightarrow ba > 0 \Rightarrow (b, a) \in R$; R is transitive as if $(a, b), (b, c) \in R$ then $ab > 0$ and $bc > 0$ so that $ab^2c > 0$, whence $ac > 0$ (as $b^2 > 0$), so that $(b, c) \in R$; R is not anti-symmetric as, for example, $(1, 2), (2, 1) \in R$ but $1 \neq 2$. Hence R is not an equivalence relation, nor a partial order. Nor is R total as, for example, $(-1, 2), (2, -1) \notin R$.

3. Since $a \in \mathbb{Z}^+$ we have $\frac{a}{a} = 1 \in \mathbb{Z}$ so that $a|a$ and R is reflexive; R is anti-symmetric as if $a|b$ and $b|a$ then $b = ak$ and $a = lb$ for some $k, l \in \mathbb{Z}^+$. But then $a = (lk)a$ so that $lk = 1$, which implies that $k = l = 1$ and $a = b$; R is not symmetric as, for example $2|4$ but 4 is not a factor of 2; R is transitive for suppose that $a|b$ so that $b = ka$ say and $b|c$ so that $c = lb$ say for some $k, l \in \mathbb{Z}^+$. Then $c = (kl)a$ and since $kl \in \mathbb{Z}^+$ it follows that $a|c$. Overall, R is not an equivalence relation (not symmetric) but is a partial order but not a *total order* as, for example, neither $(2, 3)$ not $(3, 2)$ are members of R.

4. $\equiv$ is and equivalence relation; reflexivity: $\frac{a-a}{n} = 0 \in \mathbb{Z}$ so that $a \equiv a \pmod{n}$; symmetry: suppose that $a \equiv b \pmod{n}$ so that $\frac{b-a}{n} = k \in \mathbb{Z}$, then $\frac{a-b}{n} = -k \in \mathbb{Z}$ so that $b \equiv a \pmod{n}$; transitivity: suppose that $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ so that $\frac{b-a}{n} = k$ and $\frac{c-b}{n} = l$ say. Then

$$\frac{c-a}{n} = \frac{(c-b)+(b-a)}{n} = \frac{c-b}{n} + \frac{b-a}{n} = l + k \in \mathbb{Z},$$

so that $a \equiv c \pmod{n}$. However, $\equiv$ is not anti-symmetric as, for example $(0, n)$ and $(n, 0)$ are both in R but $0 \neq n$. Also R is not total for $n \geq 2$ as, for example, $(0, 1), (1, 0) \notin R$ but $0 \neq 1$.

5. We just need to show that R is reflexive. To this end let $a \in A$. By hypothesis there exist $b \in A$ such that $(a, b) \in R$. By symmetry we have $(b, a) \in R$. Now we have $(a, b), (b, a) \in R$ so by transitivity, $(a, a) \in R$, as required.

Comment Note that the example of Question 2 is a relation that is both symmetric and transitive but not (quite) reflexive.

6. Suppose that R is both symmetric and anti-symmetric and let $(a, b) \in R$. Then by symmetry we have $(b, a) \in R$, whence by anti-symmetry we get that

$a = b$ and so $R \subseteq \iota$. Conversely if $R \subseteq \iota$ then R only contains pairs of the form (a, a) in which case R is clearly both symmetric and anti-symmetric.

7. $\sim$ is reflexive as $(a, b) \sim (a, b)$ is to say that $a + b = b + a$, which is true. Now suppose that $(a, b) \sim (c, d)$ so that $a + d = b + c \Rightarrow c + b = a + d$, which is to say that $(c, d) \sim (a, b)$. Finally for transitivity suppose that $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$ so that $a + d = b + c$ and $c + f = d + e$. Then adding these two equations gives:

$$a + d + c + f = b + c + d + e \Rightarrow a + f = b + e$$

$$\Rightarrow (a, b) \sim (e, f),$$

and so $\sim$ is an equivalence relation on the set $A = \{1, 2, \cdots, 9\}$.

$[(2, 5)] = \{(a, b) \in A \times A : (a, b) \sim (2, 5)\}$

$$\Rightarrow a + 5 = b + 2 \Rightarrow b = a + 3,$$

hence

$$[(2, 5)] = \{(1, 4), (2, 5), (3, 6), (4, 7), (5, 8), (6, 9)\}.$$

8. Suppose that $f : A \to B$ and $g : B \to C$ are injective function and consider the function $g \circ f : A \to C$. Suppose that for some $x, y \in A$ we have $(g \circ f)(x) = (g \circ f)(x)$ so that

$$g(f(x)) = g(f(y)) \Rightarrow f(x) = f(y)$$

as g is injective, and then since f is injective we conclude that $x = y$. This shows that the composite $g \circ f$ is also injective.

9. Suppose now that f and g are both surjective. Let $c \in C$. Since g is surjective, there exists $b \in B$ such that $g(b) = c$. Since f is surjective, there exists $a \in A$ such that $f(a) = b$. Then we have

$$(g \circ f)(a) = g(f(a)) = g(b) = c,$$

and since $c \in C$ was arbitrary, it follows that $g \circ f$ is also surjective.

The results of Questions 7 and 8 together tell us that if both f and g are injective and surjective, then so is $g \circ f$, which is to say that $g \circ f$ is a bijection from A onto C.

10. For any $b \in \text{ran} f$ we have

$$(b, a) \in f \circ f^{-1} \Leftrightarrow \exists c \in A : (c, a) \in f \wedge (b, c) \in f^{-1}$$

$$\Leftrightarrow ((c, a) \in f) \wedge ((c, b) \in f)$$

$$\Leftrightarrow (f(c) = a) \wedge (f(c) = b)$$

$$\Rightarrow a = b \,\text{as}\, f \,\text{is a function;}$$

hence $f \circ f^{-1}$ is the identity function on $\text{ran} f$. On the other hand for any $a \in A$ we have

$$(a, b) \in f^{-1} \circ f \Leftrightarrow (\exists c \in B : (a, c) \in f) \wedge ((c, b) \in f^{-1})$$

$$\Leftrightarrow ((a,c) \in f) \wedge ((b,c) \in f)$$
$$\Leftrightarrow f(a) = f(b) = c;$$

hence we have the relation, $\ker f$ by which $(a,b) \in \ker f$ if and only if $f(a) = f(b)$. It follows by the definition of equality that $\ker f$ is reflexive, symmetric, and transitive and therefore $\ker f$ defines an equivalence relation on A in which two elements of A are in the same class of the corresponding partition if they have the same image under f. Note that $\ker f$ is itself the equality relation if and only if f is one-to-one.

Comment The equivalence relation $\sim$ is called the *kernel* of the function f so that $(a,b) \in \ker f$ if and only if $f(a) = f(b)$.

Problem Set 2

1. If $\alpha, \beta \in T_X$ then $\alpha\beta : X \to X$ also so T_X is closed under function composition, so that $\circ$ is indeed a binary operation on T_X. What is more it follows from the definition of function composition that $\circ$ is associative for if $\alpha, \beta, \gamma \in T_X$ we find (supressing the $\circ$ symbol) that for all $x \in X$

$$((\alpha\beta)\gamma)(x) = (\alpha\beta)(\gamma(x)) = \alpha(\beta(\gamma(x)))$$
$$= \alpha((\beta\gamma)(x)) = (\alpha(\beta\gamma))(x)$$
$$\Rightarrow (\alpha\beta)\gamma = \alpha(\beta\gamma),$$

so that $\circ$ is associative and $(T_X, \circ)$ is a semigroup. Moreover the identity mapping $\varepsilon : X \to X$ where $\varepsilon(x) = x$ is the identity of T_X as for all $x \in X$ we have:

$$(\alpha\varepsilon)(x) = \alpha(\varepsilon(x)) = \alpha(x) = \varepsilon(\alpha(x)) = (\varepsilon\alpha)(x)$$

so that $\alpha\varepsilon = \varepsilon\alpha = \alpha$ for all $\alpha \in T_X$. Therefore T_X is a monoid with identity element ε.

2. Let M be a monoid with e and f identity elements of M. Then since f is an identity we have $ef = e$ but since e is an identity we also have $ef = f$ so that $e = ef = f$ and therefore $e = f$ and therefore the identity element of a monoid is unique.

Comment It is worth noting that this argument shows that if a semigroup S has a *left identity element* e and a *right identity element* f then $e = f$ and S is a monoid. A similar argument shows that if S has a *left zero element* e meaning that $ea = e$ for all $a \in S$, and also a *right zero element* f then $e = f$ is the unique zero element of S.

A semigroup can however have any number of left identity elements and right zero elements: let S be a set and define a multiplication by $ab = b$ for all $a, b \in S$. Then every element of S is a left identity element and a right zero element. We call S a *right zero semigroup*.

3. By definition, if S is a monoid then $S^1 = S$ is the same monoid. Otherwise, again by definition $1a = a1 = a$ for all $a \in S^1$ so that 1 acts as identity element of S^1. It does remain to check that S^1 is still associative: typical cases $1(ab) = ab = (1a)b$, $a(1b) = ab = (a1)b$ etc.

Comment In the same way we may adjoin a zero element 0 to a semigroup S that does not otherwise have a zero and the resulting semigroup S^0 is a semigroup with 0 with S embedded in S^0.

4. For any three strings $x_1 \cdots x_n$, $y_1 \cdots y_m$, and $z_1 \cdots z_k$ $(x_i, y_j, z_t \in A, 0 \leq n, m, k)$ we have

$$((x_1 \cdots x_n)(y_1 \cdots y_m))z_1 \cdots z_k = (x_1 \cdots x_n y_1 \cdots y_m)(z_1 \cdots z_k)$$

$$= x_1 \cdots x_n y_1 \cdots y_m z_1 \cdots z_k = (x_1 \cdots x_n)(y_1 \cdots y_m z_1 \cdots z_k)$$

$$= ((x_1 \cdots x_n)((y_1 \cdots y_m)(z_1 \cdots z_k)),$$

as required to show associativity of string concatenation. For any string $x = x_1 \cdots x_n$ and the *empty string* $1 = (\cdot)$ we have

$$1x = x = x1$$

so that the *identity* 1 in this case is the same as the empty string in that both act the same way on F_X. Hence F_X^1 is indeed a monoid.

Comment F_X, which is the same as F_X^1 without inclusion of the empty string, is known as the *free semigroup* on X. The term *free* has a specfic meaning in algebra - in particular any semigroup is the homomorphic image of a free semigroup.

5. Since the composition of two bijections is a bijection (Question 9, Set 1) it follows that when the domain and range are both equal, we conclude that the composition of two permutations of X is another permutation of X. (Quite generally, a non-empty subset U of a semigroup S will be a subsemigroup of S if U is closed under the semigroup operation as the property of associativity will be inherited from S). Moreover, since the identity mapping ε is itself a permutation, it follows that S_X is a monoid. Finally, for any $\alpha \in S_X$ the inverse relation α^{-1} is an inverse function: the domain ofα^{-1} is X as α is surjective and α^{-1} is a function (and not just a relation) as α is one-to-one. Finally $(\alpha^{-1})^{-1} = \alpha$ so that it follows that α^{-1} is also a permutation of X. Since $\alpha\alpha^{-1} = \alpha^{-1}\alpha = \varepsilon$ we conclude that S_X is indeed a group with identity element ε.

6. Take any trio $(s_1, s_2), (t_1, t_2), (u_1, u_2) \in S_1 \times S_2$. Then

$$((s_1, s_2)(t_1, t_2))(u_1, u_2) = (s_1 t_1, s_2 t_2)(u_1, u_2)$$

$$= (s_1 t_1, s_2 t_2)(u_1, u_2) = ((s_1 t_1)u_1, (s_2 t_2)u_2)$$

whence by associativity in each component we may re-bracket and continue as follows:

$$= (s_1(t_1 u_1), s_2(t_2 u_2)) = (s_1, s_2)(t_1 u_1, t_2 u_2)$$

$$= ((s_1, s_2)((t_1, t_2)(u_1, u_2))$$

as required to demonstrate associativity in $S_1 \times S_2$. Next let e_1, e_2 be the respective identity elements of S_1 and S_2 and let $(s_1, s_2) \in S_1 \times S_2$. Then

$$(e_1, e_2)(s_1, s_2) = (e_1 s_1, e_2 s_2) = (s_1, s_2)$$

$$= (s_1 e_1, s_2 e_2) = (s_1, s_2)(e_1, e_2),$$

showing that $S_1 \times S_2$ is a monoid with identity element (e_1, e_2).

Finally let us suppose that both $S_1$and S_2 are groups. Then by above $S_1 \times S_2$ is a monoid with identity (e_1, e_2). Let $(a, b) \in S_1 \times S_2$ and let a^{-1} and b^{-1} be the respective inverses of a and of b in S_1 and S_2. Then

$$(a, b)(a^{-1}, b^{-1}) = (aa^{-1}, bb^{-1}) = (e_1, e_2)$$

and in the same way, $(a^{-1}, b^{-1})(a, b) = (e_1, e_2)$ also, and so it follows that $S_1 \times S_2$ is itself a group.

Comment We should be aware that the multiplication operations in the first and second components of the direct product are that of S_1 and S_2 and so are otherwise unrelated: for example S_1 may be a semigroup of matrices under multiplication while S_2 could be a semigroup of functions under composition.

7 (i) We shall denote the addition operation in $(\mathbb{Z}_n, +)$ by $\bigoplus$ in this question in order to distinguish it from ordinary addition (this symbol is often used in texts for this purpose). The set N_n is closed under the operation $\bigoplus$ but we need to check that this binary operation is associative. To this end let $a, b, c \in N_n = \{0, 1, \cdots, n\}$. Now

$$a \bigoplus (b \bigoplus c) = a \bigoplus (b + c (\mathrm{mod}\ n)) = a + (b + c\,(\mathrm{mod}\ n))\,(\mathrm{mod}\, n) \qquad (1)$$

$$(a \bigoplus b) \bigoplus c = (a + b \bmod n) \bigoplus c = ((a + b \bmod n) + c)\,(\mathrm{mod}\ n) \qquad (2)$$

Quite generally, $x \bigoplus y$ $(x, y \in N_n)$ is equal to either $x + y$ or to $x + y - n$. It follows that each of (1) and (2) is equal to one of $a + b + c, a + b + c - n, a + b + c - 2n$. However, since (1) and (2) also lie in N_n and only one of these three numbers lies in N_n, it follows that (1) and (2) agree and so that the operation $\bigoplus$ is associative. Clearly 0 is the identity element so that $(\mathbb{Z}_n, \bigoplus)$ is a monoid (indeed, clearly a commutative monoid also). Moreover for each $a \in N_n$ we have $n - a \in N_n$ and $a \bigoplus (n - a) = 0$ as $a + (n - a) = n \equiv 0 \pmod{n}$ and so each member of N_n has an inverse with respect to 0. Therefore $(\mathbb{Z}, \bigoplus)$ is a group, and indeed is an *abelian* (i.e. a commutative) group.

(ii) Let $a, b \in G$. Then $a^2 b^2 = e^2 = e$, and bearing in mind that every member of G is equal to its own inverse we obtain

$$ab = (a^{-1}a^2)(b^2 b^{-1}) = a^{-1}(a^2 b^2)b^{-1} = a^{-1}eb^{-1} = a^{-1}b^{-1} = (ba)^{-1} = ba$$

$$\Rightarrow ab = ba\ \forall a, b \in G,$$

which is to say that G is abelian.

8. Taking matrix multiplication as associative (verified in linear algebra texts) it is clear that S is a semigroup and indeed a monoid as I, the 2×2 identity matrix, is the identity of S. However, S is not a group as, for example the zero matrix Z is in S but there is no solution A to $AZ = I$. (Indeed no member of S with zero determinant can be inverted in this way.) On the other hand, since for any square matrices A and B we have $|AB| = |A| \cdot |B|$ it follows that the subset T of S of all matrices with non-zero determinant is closed under matrix product and so forms a subsemigroup and indeed a submonoid of S. What is more, for any such A, the matrix A^{-1} exists and $|A^{-1}| = |A|^{-1} \neq 0$ and so $A^{-1} \in T$. Hence T is a subsemigroup of S that is a subgroup, meaning that T is a group under the same operation (in this instance, matrix multiplication).

Comment For a monoid M with identity element e we say that a subsemigroup N of M is a submonoid of M if $e \in N$. That is to say a subsemigroup of M that is a monoid with a different identity is a monoid but not a submonoid of M. For example, an idempotent $f \in M$ forms a subsemigroup $\{f\}$, which is not a submonoid of M if $f \neq e$.

9. Let $a, b \in H$. If $H \leq G$ (meaning that$H$ is a subgroup of G) then $b^{-1} \in H$, as H is closed under the taking of inverses, whence $ab^{-1} \in H$ as H is closed under product. Conversely, suppose that H satisfies the given condition. Since $H \neq \emptyset$ we may take $a \in H$. By putting $b = a$ in the given condition we get that $aa^{-1} = e$, the identity of G, belongs to H. Put $a = e$ in the condition and take any member $b \in H$. Then $eb^{-1} = b^{-1} \in H$ so that H is closed under the taking of inverses. Finally let $a, b \in H$. By what we have just proved, $b^{-1} \in H$, and so by the given condition so is $a(b^{-1})^{-1} = ab \in H$. Therefore H is closed under the group operation, (which we already know is associative), $e \in H$, so H has the identity element and is closed under the taking of inverses. Therefore H is a group in its own right under the same group operation as G, which is to say that $H \leq G$.

10. Take any $a \in S$. From $aS = S$ it follows that there exist $x \in S$ such that $ax = a$. Now let $b \in S$. From $Sb = S$ it follows that there exist $y \in S$ such that $ya = b$. But they $bx = y(ax) = ya = b$ so that x is a right identity element for the semigroup S. By the symmetric argument, there exist a left identity element $z \in S$. But then $z = zx = x$, with the first equality because x is a right identity and the second as z is a left identity element. Hence $z = x$ and x is the unique identity element of S, which is therefore a monoid. Now for any $a \in S$ there exist $a_1, a_2 \in S$ such that $a_1 a = x = a a_2$. But then

$$a_1 = a_1 x = a_1 a a_2 = x a_2 = a_2$$

and so $a_1 = a_2$ is the (unique) inverse of a with respect to the identity element x. In particular, S is a group.

Moreover we observe that in these circumstances the solutions to the equations $xa = b$ and $ay = b$ are unique, they being $x = ba^{-1}$ and $y = a^{-1}b$ as

$$xa = b \Rightarrow (xa)a^{-1} = ba^{-1} \Rightarrow x(aa^{-1}) = ba^{-1}$$

$$\Rightarrow xe = ba^{-1} \Rightarrow x = ba^{-1}$$

and conversely $(ba^{-1})a = b(a^{-1}a) = be = b$, verifying that $x = ba^{-1}$ does solve $xa = b$. A similar argument applies to the equation $ay = b$.

Problem Set 3

1. The set R is certainly closed under addition and it is trivial to check that matrix addition is associative and commutative. Moreover the zero matrix Z acts as the identity element under addition and for each $A \in R$, $-A$ also belongs to R and $A + (-A) = Z$. Hence R is an abelian group under matrix addition. Next, the product of two $n \times n$ matrices, M and N is another $n \times n$ matrix and since matrix multiplication is associative, it follows that R is a semigroup. Moreover the presence of the $n \times n$ identity matrix I_n assures us that R is a unital ring.

In general matrix multiplication is not commutative. For example let $M_{i,j}$ denote the $n \times n$ matrix with a 1 at position (i, j) and zeros elsewhere. Then $M_{1n}M_{n,1} = M_{1,1}$ but $M_{n,1}M_{1,n} = M_{n,n}$ and for $n \geq 2$ these products are different. Finally, the distributive law of addition over multiplication follows from that for the real numbers, and so R is a non-commutative ring.

2. Let R_1 now denote the set of all non-singular $n \times n$ matrices over $\mathbb{R}$. It is true that for $A, B \in R$ we have $|AB| = |A| \cdot |B|$ and since both $|A|$ and $|B|$ are non-zero, so is $|AB|$. Hence R_1 is closed under matrix multiplication. But not addition, for if $A \in R_1$ then so is $-A$ (as $|-A| = (-1)^n|A| \neq 0$) but $A + (-A) = Z$, the zero matrix and $Z \notin R_1$ as $|Z| = 0$.

3. The axioms of a commutative unital ring are more or less taken from the integers under addition and multiplication. The multiplicative identity is 1 and of course the product of non-zero integers is not zero. However $(\mathbb{Z}, +, \cdot)$ is not a field as no integers, apart from ± 1, have a multiplicative inverse.

Comment Of course the integers can be embedded in a field, the smallest one being the field $(\mathbb{Q}, +, \cdot)$ of all rational numbers. Indeed any integral domain can be embedded in its *field of fractions* in a similar way.

4. (i) We have

$$r0 = r(0 + 0) = r0 + r0,$$

and so subtracting $r0$ from both sides (in the abelian group $(R, +)$) we get $0 = r0$, as required.

(ii) $(-r)s + rs = (-r + r)s = 0s = 0$ (by (i)). Hence, by uniqueness of inverses in a group (see Question 10 Set 2), it follows that $(-r)s = -(rs)$. Similarly $r(-s) + rs = r(-s + s) = r0 = 0$ so that $r(-s) = -(rs)$.

(iii) Using (ii) we have

$$(-r)(-s) + (-(rs)) = (-r)(-s) + (-r)s = (-r)(-s + s) = (-r)0 = 0;$$

hence, again by uniqueness of inverses it follows that $(-r)(-s) == -(-(rs)) = rs$.

5. Let R be an integral domain and suppose that $ab = ac$ with $a \neq 0$. Then $ab - ac = a(b - c) = 0$. Since R is an integral domain and $a \neq 0$ it follows that $b - c = 0$ so that $b = c$ and R is indeed cancellative.

Conversely, suppose that R is a cancellative unital commutative ring and that $ab = 0$. Then by Question 4(i) we have $ab = a0$. Hence either $a = 0$ or, if not, we may cancel a to recover $b = 0$. In either case we see therefore that R has no zero divisors and so is an integral domain.

6. Any field must contain the elements 0 and 1. It can in fact be shown that, up to isomorphism, there is a unique field of order p^n where p is prime and $n \geq 1$ and there are no other finite fields. (By convention, $0 \neq 1$; of course if we put $0 = 1$ the field collapses to the one element group as both operations become identical.) Each such field F has *characteristic* p, which means that for any $x \in F$, $px = x + x + \cdots + x$ (p times) $= 0$. It follows that a four-element field has characteristic 2 and we have $x + x = 0$. Let a be another element. Then $1 + a = 0$ would give that $0 = 1 + 1 = 1 + a$ so that $a = 1$; if $1 + a = 1$ then $a = 0$ and if $1 + a = a$ then $1 = 0$; since none of these possibillities is allowed as a was chosen distinct from 0 and 1 it follows that the four distinct elements of our field F are $\{0, 1, a, 1 + a\}$. There is now only one way to complete the addition and the multiplication tables for F:

$+$	0	1	a	$1+a$
0	0	1	a	$1+a$
1	1	0	$1+a$	a
a	a	$1+a$	0	1
$1+a$	$1+a$	a	1	0

$\times$	0	1	a	$1+a$
0	0	0	0	0
1	0	1	a	$1+a$
a	0	a	$1+a$	1
$1+a$	0	$1+a$	1	a

In the case of multiplication, consider the value of a^2. If $a^2 = 0$ we get $a = 0$ (integral domain rule); if $a^2 = 1$ then $a(1 + a) = a + a^2 = 1 + a$ and cancelling in the group $F \setminus \{0\}$ would give $a = 1$; if $a^2 = a$ this gives $a = 1$ also, and so $a^2 = 1 + a$ is the only possiblility. Then $a(1 + a) = a + a^2 = a + (1 + a) = 1$ as $a + a = 0$. Therefore the tables are the only ones possible for a finite field of order 4 (up to the naming of elements).

This still does not prove that the tables define a finite field as we need to verify all the field axioms. In particular we must check that the operations are both associative (although commutativity of both operations is clear). However the addition table is just that of $\mathbb{Z}_2 \times \mathbb{Z}_2$: this group is sometimes known as the *Klein 4-group*: it consists of an identity element 0 and the sum of any two of the other elements equals the third. As for multiplication, $\{1, a, 1+a\}$ is a three member cyclic group (a copy of $\mathbb{Z}_3$) generated by a (and also generated by $1+a$), and all products involving 0 are equal to 0, so this table is also associative.

Comment It can be show than in the finite field of order p^n the multiplicative group is cyclic (with $p^n - 1$ elements).

Distributivity also needs to be checked: $x(y + z) = xy + xz$. This is clear if $x = 0$ or $x = 1$. We just check one other representative example here with

$x = 1 + a$, $y = 1 + a$, $z = 1$

$$x(y + z) = (1 + a)((1 + a) + 1) = (1 + a)a = a + a^2 = a + 1 + a = 1;$$

$$xy + xz = (1 + a)(1 + a) + (1 + a)1 = a + 1 + a = 1,$$

so both sides match, and the other cases are similar.

7. Taking the corresponding properties for real numbers for granted, it is plain that $R[x]$ is an abelian group under polynomial addition: the additive inverse of $p(x)$ must be $-p(x)$ and similary $R[x]$ under multiplication is a commutative monoid, with identity the constant polynomial 1. Again distributivity is a consequence of distibutivity of real numbers so that $\mathbb{R}[x]$ is a commutative unital ring.

We do need to check for zero divisors, so let $p(x), q(x) \in \mathbb{R}[x] \setminus \{0\}$ with respective leading terms $a_n x^n$ and $b_m x^m$ with $a_n, b_m \neq 0$ and $m, n \geq 0$. Then the leading term of $p(x)q(x)$ is $a_n b_m x^{n+m}$ and since $\mathbb{R}$ has no zero divisors it follows that $a_n b_m \neq 0$ and so $p(x)q(x) \neq 0$. Hence $\mathbb{R}[x]$ is an integral domain.

But $\mathbb{R}[x]$ is not a field as, for example if we take $p(x) = x$ then for any $q(x)$ we have the degree of $xq(x)$ is either at least 1 or, if $q(x) = 0$, so is $xq(x)$. In any event, $xq(x) \neq 1$ so that x has no multiplicative inverse.

8. If n is composite so that $n = ab$ say with $2 \leq a, b < n$ then in $\mathbb{Z}_n$ we have $a, b \neq 0$ but $ab = n \equiv 0 \pmod{n}$ so that $\mathbb{Z}_n$ is not an integral domain if n is composite. However for prime n no such factorization is possible and so we conclude that $\mathbb{Z}_n$ is an integral domain if and only if n is prime. (In which case $\mathbb{Z}_n$ is a field, as follows from the next question).

9. Let F be a field and suppose that $a, b \in F$ with $ab = 0$. Then either $a = 0$ or, if not we get $a^{-1}(ab) = a^{-1}0$ so that $(a^{-1}a)b = 0$ and $1b = b = 0$. This shows that any field is an integral domain.

Conversely we know that not every integral domain is a field (eg. $(\mathbb{Z}, +, \cdot)$ but suppose that R is a finite integral domain and let $a \in R \setminus \{0\}$. Then the rule $x \mapsto ax$ defines a mapping from $R \setminus \{0\}$ to itself as the product on the right cannot be zero. Moreover, this mapping is one-to-one for suppose that $ax = ay$ for some $x, y \in R \setminus \{0\}$. Then we may cancel to obtain $x = y$ showing that multiplcation by a does indeed define an injective mapping. Finally, since R is finite, it follows that our mapping is also surjective. In particular there exists $x \in R \setminus \{0\}$ such that $ax = 1$, showing that each member $a \in R \setminus \{0\}$ does have a multiplicative inverse with respect to the multiplcative identity element. Therefore every finite integral domain is a (finite) field.

10. We check that R is closed under addition and multiplication:

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = ((a + c) + (b + d)\sqrt{2} \in R \text{ as } a + c, b + d \in \mathbb{Z}$$

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2} \in R \text{ as } ac + 2bd, ad + bc \in \mathbb{Z}.$$

The laws of commutativity, associativity, and distributivity are inherited from the larger ring of all real numbers. What is more, $(R, +)$ is clearly an abelian group as $0 \in R$ and for $r = a + b\sqrt{2}$ we have that $-r = -a - b\sqrt{2} \in R$ as $-a, -b \in \mathbb{Z}$. As for multiplication, the identity element $1 \in R$ as is seen by

putting $a = 1, b = 0$, so that R is a commutative unital ring. It remains to check for zero divisors but that follows at once as the property is inherited from the real numbers.

Problem Set 4

1. Let us suppose that $ab = ac$ hold in the group G with identity element e. Then

$$a^{-1}(ab) = a^{-1}(ac)$$
$$\Rightarrow (a^{-1}a)b = (a^{-1}a)c \Rightarrow eb = ec$$
$$\therefore b = c$$

and so G is left cancellative. Similarly given that $ba = ca$, multiplying on the right by a^{-1} yields $b = c$. Therefore any group G is cancellative.

Consider the semigroup (the *two-element semilattice*) $L = \{0, 1\}$ under multiplication. This is commutative but not cancellative as $0 \cdot 1 = 0 \cdot 0$ but we cannot cancel the 0 to conclude that $0 = 1$. For a semigroup that is left but not right cancellative let E be the *right zero semigroup* on the non-empty set E, the operation being defined by $ef = f$ for all $e, f \in E$. This is easily seen to be a semigroup but as long as $|E| \geq 2$, then E is not right cancellative for if we take $e, f \in E$ with $e \neq f$ then $ef = ff = f$ but we cannot cancel the common factor of f on the right and conclude that $e = f$. However E is left cancellative as if $ef = eg$ then by definition of the product in E we have $f = g$ immediately.

Comment $S = (\mathbb{Z}^+, +)$, the positive integers under addition is an example of a cancellative semigroup that is not a group. However, S is clearly embeddable in the the group of all integers under addition. In general it can be shown that any commuative cancellative semigroup is embeddable in an abelian group but it is not true that every cancellative semigroup is group embeddable. However any *finite* cancellative semigroup is a group as is shown in the next question.

Let L and R be respectively a left zero semigroup and a right zero semigroup, each with at least 2 members. Then the semigroup $L \times R$ is neither left nor right cancellative. By symmetry it is enough to show the failure of left cancellativity so to this end take $e, f \in L$ with $e \neq f$ and let $t \in R$. Then $(e, t)(e, t) = (e^2, t^2) = (e, t)$ while $(e, t)(f, t) = (ef, t^2) = (e, t)$. Hence we have

$$(e, t)(e, t) = (e, t)(f, t)$$

but if we cancel on the left here we get the statement $(e, t) = (f, t)$, which is false as $e \neq f$.

Comment A semigroup S in which all members are idempotents (i.e. satisfy $x = x^2$) is known as a *band*. (Note that the identity element of a group is its only idempotent.) The example $L \times R$ given here is known as a *rectangular*

band. It can be shown that a semigroup S has the form $L \times R$ above if and only if for any members $x, y \in S$ it is always the case that $x = xyx$.

2. Certainly any group is cancellative by Question 1 but it remains to show that a finite cancellative semigroup S is a group. We argue as in Question 9 Set 3 and take any $a \in S$ and consider the mapping on S in which $x \mapsto ax$. By left cancellativity it follows that this mapping is one-to-one, which is to say that $aS = S$. By right cancellativity we similarly get that $Sa = S$. The result now follows by Set 2 Question 10. Finally let S be a finite subsemigroup of a group. Then since G is cancellative, then so is S and therefore S is a subgroup of G.

3.

$\times$	1	-1	i	j	k	$-i$	$-j$	$-k$
1	1	-1	i	j	k	$-i$	$-j$	$-k$
-1	-1	1	$-i$	$-j$	$-k$	i	j	k
i	i	$-i$	-1	k	$-j$	1	$-k$	j
j	j	$-j$	$-k$	-1	i	k	1	$-i$
k	k	$-k$	j	$-i$	-1	$-j$	i	1
$-i$	$-i$	i	1	$-k$	j	-1	k	$-j$
$-j$	$-j$	j	k	1	$-i$	$-k$	-1	i
$-k$	$-k$	k	$-j$	i	1	j	$-i$	-1

Now $ijk = -1$ gives $ijk^2 = -k$ so that $-ij = -k$ and so $ij = k$; similarly we have $i^2jk = -i$ so that $-jk = -i$ so that $jk = i$. And also

$$(ijk = -1) \Rightarrow (i^2jki = -i^2 = 1) \Rightarrow (-jki = 1) \Rightarrow (-j^2ki = j) \Rightarrow (ki = j).$$

Next we note that $ji = j(jk) = j^2k = -k$ and similarly we get the other two revesed products $kj = -i$ and $ik = -j$. This is enough to complete all entries of the group table as above.

The *centre* of Q is the subgroup of $\{1, -1\}$.

Comment Observe that cancellativity in groups ensures that a group table (or *Cayley table* as it is often called) as above has the *Latin square property* that each member of the group appears exactly once in each row and each column of the table. The *Quaternion number system* consists of all expressions of the form $a + bi + cj + dk$ $(a, b, c, d \in \mathbb{R})$ and was introduced by the Irish mathematician William Rowan Hamilton as a 4-dimensional analogue to the complex numbers $a+bi$. However quaternions are not multiplicatively commutative as, for instance $ij = -ji$. There is no 3-dimensional analogue of the complex numbers that satisfies all the main laws of algebra. Quaternions are often used in describing motion in 3-dimensional space.

4. Let $\langle A \rangle = \cap S_i$ where the intersection is taken over all subsemigroups of S that contain A. Since S is a member of this intersection, the collection of the S_i is not the empty collection. Moreover, since each of the S_i contains the non-empty set A, it follows that $A \subseteq \langle A \rangle$. Since $\langle A \rangle$ is, by definition, contained in every susbsemigroup of S that contains A, it follows that to show that $\langle A \rangle$ is the smallest subsemigroup of S that contains A it remains only to check that

$\langle A\rangle$ is a subsemigroup of S. To do that we need only check that $\langle A\rangle$ is closed under product so let $a, b \in \langle A\rangle$. Let S_j be any one of the sets in our intersection. Then since $a, b \in \cap S_i$, it follows that $ab \in S_j$ for all j and so $ab \in \cap S_i = \langle A\rangle$. Therefore $\langle A\rangle$ is the smallest subsemigroup of S that contains A; we call $\langle A\rangle$ the *subsemigroup generated by A*.

For any $a_1, a_2, \cdots, a_n \in A$ it follows by a simple induction on n that the product $a_1a_2\cdots a_n$ is a member of any subsemigroup of S that contains A; in particular $a_1a_2\cdots a_n \in \langle A\rangle$. Since $\langle A\rangle$ is the smallest subsemigroup of S that contains A it follows that in order to show that the set P of these products is equal to $\langle A\rangle$, it is enough to show P is a semigroup that contains A. However each $a_1 \in A$ is a member of P, as here we are in the $n = 1$ case. Moreover for two members of P, $a = a_1a_2\cdots a_n$ and $b = b_1b_2\cdots b_m$ say, then $ab = a_1a_2\cdots a_nb_1b_2\cdots b_m \in P$ as P is the set of all such products.

5. Let $\langle A\rangle = \cap G_i$ where the intersection is taken over all subgroups of G that contain A. Since the identity element $e \in G$ is a member of each G_i, it follows that the intersection contains $A \cup \{e\}$ and is therefore not empty.

Comment The intersection of two subsemigroups of a semigroup S may be empty: for example any two non-empty disjoint subsets of a right zero semigroup S are each subsemigroups of S.

Since $\langle A\rangle$ is, by definition, contained in every subgroup of G that contains A, it follows that to show that $\langle A\rangle$ is the smallest subgroup of G that contains A it remains only to check that $\langle A\rangle$ is a subgroup of G. As in the semigroup case, $\langle A\rangle$ is closed under product. In the same way, since each G_i is closd under the taking of inverses, so is their intersection $\langle A\rangle$, and so $\langle A\rangle$ is the smallest subsgroup of G that contains A; we call $\langle A\rangle$ the *subgroup generated by A*.

Next let $a_1, \cdots, a_n \in A \cup A^{-1}$ $(n \geq 0)$. Since $\langle A\rangle$ is a group it follows that the product $p = a_1 \cdots a_n \in \langle A\rangle$. (If $n = 0$, then p is the empty product, taken to be the identity element e and, as we have already noted, $e \in \langle A\rangle$.) Hence this set of products P is a subset of $\langle A\rangle$. To show the reverse inclusion we only need check that P is a subgoup of G and that $A \subseteq P$. As in the semigroup case, it is clear that $A \subseteq P$ and that P is a subsemigroup of G. Finally, P is closed under the taking of inverses for if $p = a_1 \cdots a_n \in P$ then

$$p^{-1} = (a_1 \cdots a_n)^{-1} = a_n^{-1} \cdots a_1^{-1}$$

and since each $a_i^{-1} \in A \cup A^{-1}$, it follows that $p^{-1} \in P$, as required to complete the proof.

Comment Do note that the inverse of a product is the product of the inverses in the reverse order, a phenomenon that the student will have seen in the case of matrices which represent a fundamental algebraic system in which multiplication is not commutative and so order matters.

6. A member $a \in (\mathbb{Z}_n, +)$ will be cyclic if and only if for all $b \in \mathbb{Z}_n$ there exists an $x \in \mathbb{Z}$ such that $ax \equiv b \pmod{n}$ and from Set 1 of MA202 we know this can only happen if the $\gcd(a, n)$ divides b. In particular there must be a solution to $ax \equiv 1 \pmod{n}$ and that can only occur if a and n are relatively prime. Conversely, if a and n are relatively prime, each of the preceding congruences has a solution.

In conclusion, a is a generator of $(\mathbb{Z}_n, +)$ if and only if a and n have no common factor apart from 1. The number of such generators is therefore $\phi(n)$, where ϕ is the Euler ϕ-function. (See Set 3 of MA202.)

7. Clearly $\{0\}$ and F are ideals of F. Let I be a non-zero ideal of F so we may take $a \in F \setminus \{0\}$. Then since $aF \subseteq I$ it follows that in particular $aa^{-1} = 1 \in I$. But then, for any $b \in F$ we have $1b = b \in I$ and since b was arbitrary we conclude that $F \subseteq I$ and so $I = F$.

8. $I = aR$ is closed under addition because $ab + ac = a(b + c) \in I$. Clearly $0 = a0 \in I$ and if $ar \in I$ then $-(ar) = a(-r) \in I$ also so that I is an abelian group under addition. Moreover I is closed under multiplication as $(ar)(as) = a(ras) \in aR = I$ and the other properties of a subring are inherited from R. Finally I is an ideal as for any $ar \in I$ and any $s \in R$ we have $(ar)s = a(rs) \in aR = I$. And of course $aR = Ra$ by commutativity.

9. The principal ideals of the integral domain $\mathbb{Z}$ are by definition the subrings of the form $n\mathbb{Z}(n \in \mathbb{Z})$. The claim is that *any* ideal I of $\mathbb{Z}$ has this form. If $I = \{0\}$ (which is certainly an ideal) then take $n = 0$ in our claim. Otherwise I contains non-zero integers and since I is an additive subgroup of $\mathbb{Z}$ it follows that I contains positive integers. Let n be the least positive integer in I. Certainly we have $n\mathbb{Z} \subseteq I$; we need to prove the reverse inclusion to complete the proof.

Take any positive number $m \in I$ so we have $n \leq m$. Let d be the gcd of m and n. Then by the Euclidean algorithm we know that there exist integers a and b such that $am + bn = d$. However since $m, n \in I$ then so are am, bn (as I is closed under addition and under the taking of negatives, a point that is important as a and b may be negative) and so $d = am + bn \in I$ also. However since d is positive and $d \leq n$ it follows by choice of n that $d = n$ and so $m \in n\mathbb{Z}$. Finally if $m \in I$ and $m < 0$ then $-m \in I$ and $-m > 0$ and by what we have just proved $-m$, and therefore also m, is a member of the principal ideal $n\mathbb{Z}$. Therefore $I = n\mathbb{Z}$, as claimed.

10. The maximal ideals of $\mathbb{Z}$are the principal ideals $p\mathbb{Z}$ where p is prime. To see this let I be any ideal of $\mathbb{Z}$. Then $I = n\mathbb{Z}$say. If n is composite, so that $n = ab$ say with $2 \leq a, b$ and then we have that $I \subseteq a\mathbb{Z}$ as for any $nk \in I$ we may write $nk = a(bk) \in a\mathbb{Z}$. On the other hand since $a < n$ we cannot write a in the form $a = nk$ $(k \in \mathbb{Z})$ and since $a = a \cdot 1 \in a\mathbb{Z}$, it therefore follows that if n is composite then I is not maximal. In other words, any maximal ideal of $\mathbb{Z}$ has the form $I = p\mathbb{Z}$ for some prime p.

Conversely let J be an ideal of $\mathbb{Z}$ such that $I = p\mathbb{Z}$ is strictly contained in J. Take $n \in J \setminus I$ so that p is not a factor of n. Hence p and n are relatively prime and so by the Euclidean algortithm there exist integers a and b such that $ap + bn = 1$. It then follows that $1 \in J$, whereupon it follow that $J = \mathbb{Z}$. Therefore $I = p\mathbb{Z}$ is indeed a maximal ideal of $\mathbb{Z}$.

Problem Set 5

1. Certainly $a \mapsto ah$ maps H into aH and is clearly surjective as any member of the range has the form ah ($h \in H$). The mapping is also one-to-one as if $ah = bh$ then $a = b$ as groups are cancellative. Hence the mapping is a bijection from H onto aH and so all left cosets are equicardinal.

Comment H is both a left and right coset of H as $H = eH = He$.

2. We prove this by showing that if $aH \cap bH \neq \emptyset$ then $aH = bH$. To do this it is enough to show that $aH \subseteq bH$ for the reverse containment then follows by symmetry. Let us take $c \in aH \cap bH$ so that $c = ah_1 = bh_2$ for some $h_1, h_2 \in H$. Then $a = bh_2h_1^{-1} \in bH$ as $h_2h_1^{-1} \in H$. However since $a \in bH$ we get $aH \subseteq (bH)H = b(H^2) = bH$, as required to complete the proof.

3. By Question 2 we have that the left cosets of H are pairwise disjoint. The union of all the left cosets is G as each $a \in G$ is a member of its own left coset aH as $a = ae$ and $e \in H$. Therefore the left cosets (and dually the right cosets) of G partition G into blocks, and by Question 1 these blocks are all of the same cardinal.

4. Note that

$$(aH = bH) \Leftrightarrow (a^{-1}aH = a^{-1}bH) \Leftrightarrow (eH = a^{-1}bH) \Leftrightarrow (H = a^{-1}bH) \qquad (3)$$

but then $a^{-1}b = a^{-1}be \in a^{-1}bH = H$ so that $a^{-1}b \in H$.

Comment Note in particular that $H = aH$ if and only $eH = aH$, which is to say that $e^{-1}a = ea = a \in H$. Similarly $Ha = H$ if and only if $a \in H$.

Conversely if $a^{-1}b \in H$ then since $hH = H$ for every $h \in H$ (as $h = he = eh \in hH \cap eH = H$ implies that $hH = H$ by Question 2) then $a^{-1}bH = H$ and so $aH = bH$ by (3).

5. In the table below, the entry in row X and column Y is the result of acting first X and then Y.

$\times$	R_0	R_1	R_2	R_3	S_0	S_1	S_2	S_3
R_0	R_0	R_1	R_2	R_3	S_0	S_1	S_2	S_3
R_1	R_1	R_2	R_3	R_0	S_1	S_2	S_3	S_0
R_2	R_2	R_3	R_0	R_1	S_2	S_3	S_0	S_1
R_3	R_3	R_0	R_1	R_2	S_3	S_0	S_1	S_2
S_0	S_0	S_3	S_2	S_1	R_0	R_3	R_2	R_1
S_1	S_1	S_0	S_3	S_2	R_1	R_0	R_3	R_2
S_2	S_2	S_1	S_0	S_3	R_2	R_1	R_0	R_3
S_3	S_3	S_2	S_1	S_0	R_3	R_2	R_1	R_0

Since $H = \{R_0, S_0\}$ has two members, there are $\frac{8}{2} = 4$ left cosets and 4 right cosets of H. The left cosets are as follows:

$H = \{R_0, S_0\}$, $R_1H = \{R_1R_0, R_1S_0\} = \{R_1, S_1\}$, $R_2H = \{R_2, S_2\}$, $R_3H = \{R_3, S_3\}$, while the right cosets are:

$H = \{R_0, S_0\}$, $HR_1 = \{R_0R_1, S_0R_1\} = \{R_1, S_3\}$, $HR_2 = \{R_2, S_2\}$, $HR_3 = \{R_3, S_1\}$.

6. By Question 4, the left cosets of H partition G into blocks all of equal cardinality. Since H is itself one of these cosets, the cardinality of each left coset

(and each right coset) is $|H|$. The order of G is therefore $|H|$ times the number of left cosets of H in G, which is by definition the index of H is G. Therefore we have the equation:

$$|G| = [G : H] \cdot |H|.$$

In particular, in the case of a finite semigroup G, the order of any subgroup $|H|$ must be a factor of $|G|$.

7. Let G be a group with $|G| = p$, a prime. Let a be any element of G apart from its identity element e. Then $H = \langle a \rangle$is a subgroup of G and $|H| \geq 2$ as $e, a \in H$. By Lagrange's theorem, $|H|$ is a factor of p but since p is prime it follows that $|H| = p = |G|$ and so $H = G$, which is a cyclic group of order p.

Comment Anticipating Problem Set 6, we may say G is *isomorphic* to $\mathbb{Z}_p$, an isomorphism $\phi : H \to \mathbb{Z}_p$ is defined by $a^k\phi = k$ $(k \in \{0, 1, \cdots, k-1\}$.

8. By Question 7 it follows that, up to isomorphism (the naming of elements) the only groups of orders $2, 3$ and 5 are $\mathbb{Z}_2$, $\mathbb{Z}_3$, and $\mathbb{Z}_5$ respectively and of course all groups of order 1 are trivial. A group of order 4 is either cyclic (so that G is not a copy of $\mathbb{Z}_4$) or every non-identity member $a \in G$ must have order 2 by Lagrange's theorem. Let use write $G = \{e, a, b, c\}$ say and so we have $a^2 = b^2 = c^2 = e$. Now since G is cancellative and inverses are unique it follows that $ab \in \{e, a, b\}$ is impossible. Hence we must have $ab = c$ and by the same token a product of any two distinct members of the set $\{a, b, c\}$ must equal the third. Hence this completely determines the multiplication of G and so there can be only one other group of order 4 apart from the cyclic group $\mathbb{Z}_4$. This table does indeed represent a group as $\mathbb{Z}_2 \times \mathbb{Z}_2$ is a group of order 4 that is not a copy of $\mathbb{Z}_4$ as not every member of $\mathbb{Z}_2 \times \mathbb{Z}_2$ generates a group of order 4.

Suppose G is abelian of order 6. We show that G is cyclic and so G is a copy of $\mathbb{Z}_6$. All non-identity members of G have orders $2, 3$ or 6. Suppose that a and$b$ were two distinct members of G of order 2. Then $ab = c$ with $c \neq a, b$ and $c^2 = a^2b^2 = e$. Then $ac = a^2b = b$, $bc = b^2a = a$ and so $\{e, a, b, c\}$ is a subgroup of order 4; however 4 does not divide 6, so this contradicts Lagrange's theorem. If G were not cyclic it follows that at least 4 members of G are of order 3. If a is of order 3 then so is a^2 so there exist two subgroups of the form $H_a = \{e, a, a^2\}$ and $H_b = \{e, b, b^2\}$ with $H_a \cap H_b = \{e\}$,with the remaining member $c \in G$ then necessarily of order 2. Then $cH_a = \{c, ca, ca^2\} = G \setminus H_a = \{c, b, b^2\}$. But if $ca = b$ we have $c^2a^2 = a^2 = b^2$, a contradiction, while if $ca = b^2$ then $c^2a^2 = a^2 = b^4 = b$, again a contradiction. The only remaining alternative is that G has a member of order 6 and so G is cyclic.

However, there is one non-abelian group of order 6, which is S_3, the symmetric group on a set of order 3 (which is also D_3, the group of symmetries of the equilateral triangle). For instance the product of the two transpositions $(1\,2)$ and $(2\,3)$ is equal to the 3-cycle $(1\,3\,2)$ (if we act $(1\,2)$ first) and is equal to $(1\,2\,3)$ if acted in the reverse order.

9. (i) Suppose that $H \lhd G$ and let $a \in G$. Then

$$aH = Ha \Rightarrow aHa^{-1} = Haa^{-1} = H$$

so it is certainly the case that $aHa^{-1} \subseteq H$ for all $a \in G$.

Conversely suppose that for all $a \in G$ we have$aHa^{-1} \subseteq H$. Then $aHa^{-1}a \subseteq Ha$, and $aH \subseteq Ha$. We may obtain the reverse inclusion by replacing a by a^{-1} for then we have $a^{-1}H(a^{-1})^{-1} = a^{-1}Ha \subseteq H$ so that $aa^{-1}Ha \subseteq aH$, which is to say $Ha \subseteq aH$. Therefore the condition that $a^{-1}Ha \subseteq H$ for all $a \in G$ implies that $aH = Ha$ for all $a \in G$, which is to say that $H \lhd G$, as required.

(ii) We have that $aH = Hb$ so that $a = ae \in aH = Hb$ so that for some $h \in H$ we have $a = hb$. But then $Ha = Hhb = Hb = aH$. It follows that $H \lhd G$.

(iii) Take the dihedral group of Question 6. The subgroup H is abelian (as noted in Question 8) but is not normal in G as $R_1H \neq HR_1$ (as shown above).

(iv) We have $[G : H] = 2$. Let $a \in G$. If $a \in H$ then $aH = Ha = H$. Otherwise $a \notin H$ so $aH \neq H$ and $Ha \neq H$. However since the index of H is 2 it follows that $aH = Ha = G \setminus H$. Hence for any $a \in G$ we have $aH = Ha$ so that $H \lhd G$.

10 (i) Trivially if one subgroup is contained in the other, $H \subseteq K$ say, then $H \cup K = K \leq G$. Otherwise we may take $h \in H \setminus K$ and $k \in K \setminus H$ and consider the product hk. If $H \cup K \leq G$ then $hk \in H$ or $hk \in K$. However, if $hk = h' \in H$ then $k = h^{-1}h' \in H$, contrary to our choice of k. Similarly $hk \in K$ leads to the corresponding contradiction that $h \in K$. Therefore the assumption that $H \cup K \leq G$ is false unless $H \subseteq K$ or $K \subseteq H$.

(ii) Take $G = \mathbb{Z}_2 \times \mathbb{Z}_2$. Let $H_1 = \{(0,0),(0,1)\}, H_2 = \{(0,0),\{1,0)\}$ and $H_3 = \{(0,0),(1,1)\}$. Then evidently each $H_i \leq G$, none of these three subgroups is contained in one of the others but $H_1 \cup H_2 \cup H_3 \leq G$, indeed this union is equal to G.

Problem Set 6

1 (i) Note first that the identity e of any group K is the unique idempotent of K, for certainly $e^2 = e$ and if $a^2 = a$ then $a^2 = ae$ whence by cancellativity $a = e$. Hence we may show that $\phi(e_G) = e_H$ by veriftying that $\phi(e_G)$ is an idempotent. However, since ϕ is a homomorphism

$$\phi^2(e_G) = \phi(e_G^2) = \phi(e_G),$$

as required.

(ii) For $a, b \in S$ we have

$$(f \circ g)(ab) = f(g(ab)) = f(g(a)g(b)) = f(g(a))f(g(b)) = (f \circ g)(a)(f \circ g)(b).$$

Comment In particular, the composition of two endomorphisms is another, showing that the endomorphisms of a semigroup S form a semigroup; since the composition of two permutations is a permutation, it follows that the automorphisms of a semigroup S form a group, denoted by $\mathrm{Aut}(S)$.

2. (i) Define the mapping $\phi : \langle i \rangle \to \mathbb{Z}_4$ by $i^t \mapsto t \pmod 4$. Since $i^4 = 1$ it follows that $\phi(i^t) = \phi(i^s)$ if and only if $t \equiv s \pmod 4$ so that ϕ is a well-defined

function (because of the forward implication) and ϕ is one-to-one (because of the reverse implication). Find $\phi(i^t i^s) = \phi(i^{t+s}) = (t+s) \pmod 4 \equiv (t \pmod 4 + s \pmod 4) \pmod 4 = (\phi(i^t) + \phi(i^s)) \pmod 4$, so that$\phi$ is a bijective homomorphism and therefore the two groups are isomorphic.

(ii) The two groups are not isomorphic as one has an element of order 4 and the other does not. In detail, take any homomorphism $\phi : \mathbb{Z}_4 \to \mathbb{Z}_2 \times \mathbb{Z}_2$ and take any $k \in \mathbb{Z}_4$ so that $\phi(k) = (a, b)$ say. Then

$$\phi(2k) = \phi(k + k) = \phi(k) + \phi(k) = (a, b) + (a, b) = (2a, 2b) = (0, 0).$$

However, by Question 1(i) we know that $\phi(0) = (0, 0)$ and so if ϕ were injective this would imply that $2k = 0$ for all $k \in \mathbb{Z}_4$. Since $\mathbb{Z}_4$ has members that are not of order 1 or 2 (1 and 3 generate all of $\mathbb{Z}_4$) it follows that there is no monomorphism from $\mathbb{Z}_4$ to $\mathbb{Z}_2 \times \mathbb{Z}_2$ and in particular the two groups are not isomorphic.

Comment In general, to show that two groups (or semigroups or rings etc) are *not* isomorphic it is enough to identity one algebraic feature (a feature preserved by isomorphisms) that is different from the first group to the second. For example, cardinality, commutativity, order of elements, nature of subgroups etc. If after due consideration the two groups appear to be algebraically the same, we prove as much by finding a specific isomorphism between the two groups (as in Question 1).

3 Certainly $f(S)$ is a non-empty subset of T. Take $t_1, t_2 \in f(S)$ so we may write $t_1 = f(a_1)$ and $t_2 = f(a_2)$ say. Then

$$t_1 t_2 = f(a_1)f(a_2) = f(a_1 a_2) \in f(S),$$

thereby showing that $f(S)$ is a subsemigroup of T.

Suppose next that S is a group and consider the subsemigroup $f(S)$ of T. Let e be the identity of S. Then $g = f(e)$ is the identity element of $f(S)$ for take any $t = f(a) \in f(S)$. Then

$$tg = f(a)f(e) = f(ae) = f(a) = t,$$

and a similarly line of proof shows that g is also a left identity element of $f(S)$. Finally let t, t^{-1} be a pair of inverses in the group S. Then

$$f(t)f(t^{-1}) = f(tt^{-1}) = f(e) = g$$

so that $f(t^{-1}) = (f(t))^{-1}$ and therefore $f(S)$ is a group within the semigroup T.

Comment We cannot conclude in these circumstances that T is a group. For example, take any monoid S with identity e and suppose that S is not a group. The identity mapping on S (which is an automorphism of S) then maps the subgroup $\{e\}$ of S onto itself but the image S is not itself a group.

4. Let $u_1, u_2 \in f^{-1}(V)$ so that $f(u_1) = v_1$and $f(u_2) = v_2$. Then $f(u_1 u_2) = f(u_1)f(u_2) = v_1 v_2 \in V$ as $V \leq T$. Hence, if $f^{-1}(V) \neq \emptyset$ then $f^{-1}(V) \leq S$.

5 (i) By Question 3 we know that $f(G)$ is a subgroup of the semigroup T. Take any $v \in f(G)$, which we may write as $v = f(a)$ for some $a \in G$. Let e denote the identity element of G. By Question 2 we know that $g = f(e)$ is the identity element of the group $f(G)$. Then since G is a group, we may take the inverse $a^{-1}$of a in G and obtain:

$$f(a^{-1})f(a) = f(a^{-1}a) = f(e) = g$$

and similarly we find that $f(a)(f(a^{-1}) = g$. Since inverses in a group are unique, we conclude that $f(a^{-1}) = f(a)^{-1}$, as required.

Comment What we have shown here is that a group homomorphism preserve the identity element and preserves inverses.

Now let V be a subgroup of T. By Question 4 we have that $U = f^{-1}(V)$ is a subsemigroup of G. By Question 2, we have that $f(e_G) = e_T$, which is necessarily a member of the subgroup V as the group T has e_T as its only idempotent. This says that $e_G \in f^{-1}(V)$. Finally take any $a \in f^{-1}(V)$. Then by above we have that $f(a^{-1}) = (f(a))^{-1} \in V$ as $f(a) \in V$ and V is a subgroup of T. Therefore $a^{-1} \in f^{-1}(V)$ also and therefore $U = f^{-1}(V)$ is a subgroup of G.

Comment Note that the inverse image $f^{-1}(V)$ of a subgroup of the group T cannot be empty as $e_T \in V$ and $f(e_G) = e_T$ so that $e_G \in f^{-1}(V)$. However, in the case of a *semigroup* T that is not a group, it is possible for a subgroup V of T to have an empty intersection with the image group $f(G)$. This is because a semigroup T can contain disjoint subgroups (with different identity elements).

6 (i) If there is a mapping ϕ from a finite set S onto another set T, then T is finite: for each $t \in T$ choose a member of $\phi^{-1}(t)$. Since the sets $f^{-1}(t)$ partition S, it follows that any such choice defines a one-to-one map from T into S and in particular $|T| \leq |S|$. Hence if S is finite, so is its image T.

Suppose now that G is abelian. We know from Question 3 that the image $\phi(G) = T$ is a group. Take any $t_1, t_2 \in T$, which we may write as $t_i = \phi(a_i)$ $(i = 1, 2)$. Then

$$t_1t_2 = \phi(a_1)\phi(a_2) = \phi(a_1a_2) = \phi(a_2a_1) = \phi(a_2)\phi(a_1) = t_2t_1,$$

showing that T is also an abelian group.

(ii) We have $\langle A\rangle = G$ and $\phi G \to T$ is an epimorphism. Take any $t \in T$ so that $t = \phi(a)$ say. We may factorize a as $a = a_1a_2 \cdots a_n$ $(n \geq 0)$ where the a_i are (not necessarily distinct) members of the generating set A.

Comment Note that for $n = 0$ we mean that $a = e$, the identity of G; since e lies in every subgroup of G and in general $\langle A\rangle$ is the intersection of all subgroups of G that contain A, it follows that $e \in \langle A\rangle$ is always true.

But then we have

$$t = \phi(a) = \phi(a_1a_2 \cdots a_n) = \phi(a_1)\phi(a_2) \cdots \phi(a_n),$$

and since t was arbitrary this shows that $\phi(A)$ generates the image $\phi(G) = T$.

(iii) Suppose that $V \leq T$. Then by Question 5 we have $U = \phi^{-1}(V)$ is a subgroup of G. Suppose further that $V \lhd T$. Then for any $a \in G$ we have

$$\phi(aUa^{-1}) = \phi(a)\phi(U)\phi(a^{-1}) = \phi(a)V(\phi(a))^{-1}$$

and since $V \lhd T$ it follows that $\phi(aUa^{-1}) = V$ or what is the same, $aUa^{-1} \subseteq \phi^{-1}(V) = U$. By Question 9 of Set 5 we conclude that $U \lhd G$, as required.

7 (i) Certainly $\mathbb{C} \setminus \{0\}$ is closed under this binary operation (as $\mathbb{C}$ has no zero divisors) but associativity needs to be checked, so let $a, b, c \in \mathbb{C}$. Then

$$a \circ (b \circ c) = a \circ (|b|c) = |a||b|c = |ab|c;$$

$$(a \circ b) \circ c = (|a|b) \circ c = ||a|b|c = |ab|c$$

so we have associativity and thus a semigroup. Suppose that $a \circ b = a \circ c$ in S, which is to say that $|a|b = |a|c$ and since $|a| \neq 0$ we may cancel to get $b = c$, thereby establishing left cancellativity. However, given that $b \circ a = c \circ a$ we have only that $|b|a = |c|a$ which will be true whenever $|b| = |c|$ so there is no need for $b = c$ to hold. To show *right simplicity* of our semigroup, which is to say that $a \circ S = S$ for all $a \in S$ we need to show we can solve the equation $a \circ x = b$ for any given $a, b \in S$. Our equation is then $|a|x = b \Leftrightarrow x = \frac{b}{|a|}$, as required.

(ii) The key now is to ask ourselves when is it the case that $a \circ b = b$? This occurs when $|a|b = b \Leftrightarrow |a| = 1$. Let us put $E = \{a \in \mathbb{C} : |a| = 1\}$. By the previous observation it follows that for any $e, f \in E$ we have $e \circ f = |e|f = f$ so that E is indeed a right zero subsemigroup of S. We may write any $a \in S$ as $a = |a|\frac{a}{|a|}$, thus expressing a as a product of a positive real number and a complex number of unit modulus. To this end let $G = (\mathbb{R}^+, \cdot)$, the group of all positive real numbers under multplication and consider the semigroup $G \times E$.

We claim that $G \times E$ is isomorphic to S. We claim that the mapping is $\phi(a) = (\frac{a}{|a|}.|a|)$ is an isomorphism as we now check.

To see that ϕ is one-to-one, suppose that $\phi(a) = \phi(b)$ so that $(\frac{a}{|a|}, |a|) = (\frac{b}{|b|}, |b|)$. Then $\frac{a}{|a|} = \frac{b}{|b|} = \frac{b}{|a|}$, which implies that $a = b$, thus establishing that ϕ in injective.

Next take any member $(g, e) \in G \times E$ ($g \in \mathbb{R}^+, e \in \mathbb{C}$with $|e| = 1$) and put $a = ge$. Then $|a| = |ge| = |g||e| = g \cdot 1 = g$. Hence $\phi(a) = (\frac{a}{|a|}, |a|) = (\frac{ge}{g}, g) = (e, g)$, whence it follows that ϕ is also surjective and hence a bijection. Finally, ϕ preserves the semigroup operation as

$$\phi(ab) = (\frac{ab}{|ab|}, |ab|) = (\frac{a}{|a|} \cdot \frac{b}{|b|}, |a| \cdot |b|) = (\frac{a}{|a|}, |a|)(\frac{b}{|b|}, b) = \phi(a)\phi(b).$$

Therefore we can say that S is indeed represented by the direct product $G \times E$.

Comment It may also be proved that any left cancellative and right simple semigroup has the form $G \times E$ for a suitable group G and a right zero semigroup E (and conversely). What is more any these properties are also equivalent to S being right simple and containing at least one idempotent. However, there exist examples of (necessarily infinite) semigroups that are both right simple

and right cancellative without being left cancellative: the so-called *Baer-Levi semigroups*.

8 (i) Since $\phi(e_G) = e$ it follows that $e_G \in \ker(\phi)$ and that $\ker(\phi) \neq \emptyset$. Next take $a, b \in \ker(\phi)$. By Question 9 set 2, to show that $\ker(\phi) \leq G$ we need only check that $ab^{-1} \in \ker(\phi)$. But since homomorphisms commute with inversion we get:

$$\phi(ab^{-1}) = \phi(a)\phi(b^{-1}) = \phi(a))(\phi(b))^{-1} = e_H e_H^{-1} = e_H^2 = e_H.$$

Finally, to show normality of $\ker(\phi)$ we need only show (by Question 9(i) of Set 5) that if $n \in \ker\phi$ and $a \in G$ then $a^{-1}na \in \ker(\phi)$:

$$\begin{aligned}\phi(a^{-1}na) &= \phi(a^{-1})\phi(n)\phi(a) = (\phi(a))^{-1}e_H\phi(a)\\ &= (\phi(a))^{-1}\phi(a) = e_H,\end{aligned}$$

which completes the proof.

(ii) It is always the case that $\phi(e_G) = e_H$ so that $e_G \in \ker(\phi)$ is always true. If $a \in \ker(\phi)$ then $\phi(a) = \phi(e_G) = e_H$. Hence if ϕ is injective then $a = e_G$ so that $\ker(\phi) = \{e_G\}$. Conversely suppose that $\ker(\phi) = \{e_G\}$ and that $\phi(a) = \phi(b)$. Then

$$(\phi(a)(\phi(b))^{-1} = e_H) \Rightarrow (\phi(a)\phi(b^{-1}) = e_H) \Rightarrow \phi(ab^{-1}) = e_H$$

so that $ab^{-1} \in \ker(\phi)$. However, since $\ker(\phi) = \{e_G\}$ we have that $ab^{-1} = e_G \Leftrightarrow a = b$. This shows that if $\ker(\phi)$ is trivial in this way then ϕ is a monomorphism.

9 (i) First we show that ϕ_g is a homomorphism on G, so let us take any $a, b \in G$ and remembering that $g^{-1}g = e$, the identity of G, we obtain

$$\phi_g(ab) = g(ab)g^{-1} = (gag^{-1})(gbg^{-1}) = \phi_g(a)\phi_g(b).$$

Next we show injectivity:

$$\begin{aligned}&\phi_g(a) = \phi_g(b)\\ \Rightarrow\ &gag^{-1} = gbg^{-1},\end{aligned}$$

which implies that $a = b$ as groups are cancellative. Finally for surjectivity, take any target point $x \in G$. Then

$$\phi_g(g^{-1}xg) = gg^{-1}xgg^{-1} = x,$$

and so it follows that ϕ_g is also onto. Therefore ϕ_g is an automorphism of G.

Comment An automorphism of the type ϕ_g defined by conjugation by g is known as an *inner automorphism* of G.

(ii) Take any $\phi_g, \phi_h \in In(G)$ and $a \in G$. We have

$$(\phi_g\phi_h)(a) = \phi_g(\phi_h(a)) = g(hah^{-1})g^{-1} = (gh)a(gh)^{-1} = \phi_{gh}(a) \qquad (4)$$

and so (4) shows that $\phi_g\phi_h = \phi_{gh}$ and in particular $In(G)$ is a semigroup. Moreover $In(G)$ has an identity element in ϕ_e as by (4) we have

$$\phi_e\phi_g = \phi_{eg} = \phi_g = \phi_{ge} = \phi_g\phi_e.$$

Finally $(\phi_g)^{-1} = \phi_{g^{-1}}$ as $\phi_{g^{-1}}\phi_g = \phi_{g^{-1}g} = \phi_e$ and in the same way $\phi_g\phi_{g^{-1}} = \phi_e$. Therefore $\mathrm{Inn}(G)$ is a group.

It follows from the elementary facts that the composition of permutations is another permutation and the composition of homomorphisms is another homomorphism that $Aut(G)$ is a group, so we now know that $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$. Let us take any $\alpha \in \mathrm{Aut}(G)$ and $\phi_g \in \mathrm{Inn}(G)$. We claim that $\alpha\phi_g\alpha^{-1} = \phi_{\alpha(g)}$ from which follows our normality claim for $\mathrm{Inn}(G)$ in $\mathrm{Aut}(G)$. And so, take any $a \in G$. We obtain

$$\alpha\phi_g\alpha^{-1}(a) = \alpha(g\alpha^{-1}(a)g^{-1}) = \alpha(g)\alpha(\alpha^{-1}(a))\alpha(g^{-1})$$

$$= \alpha(g)a(\alpha^{-1}(g)) = \phi_{\alpha(g)}(a),$$

and since a was arbitrary we arrive at the required conclusion that a $\mathrm{Inn}(G)$ is closed under conjugation by automorphisms of G.

(iii)

$$\phi([a,b]) = \phi(a^{-1}b^{-1}ab) = \phi(a)^{-1}\phi(b)^{-1}\phi(a)\phi(b) = [\phi(a), \phi(b)].$$

10. If $g = xhx^{-1}$ then $h = x^{-1}gx = x^{-1}g(x^{-1})^{-1}$ showing that the relation $\sim$ is symmetric on G. Since $g = ege^{-1}$ we have that $g \sim g$ and so $\sim$ is reflexive. Finally suppose that $g \sim h$ and $h \sim k$ say so that $g = xhx^{-1}$ and $h = yky^{-1}$. Then substituting the second equation into the first yields

$$g = x(yky^{-1})x^{-1} = (xy)k(xy)^{-1},$$

thus showing that $g \sim k$ and so $\sim$ is transitive and therefore conjugacy does define an equivalence relation on $\sim$.

Problem Set 7

1. Since $N \lhd G$ we have $aN = Na$ so that

$$(aN)(bN) = (Na)(bN) = N(abN) = N^2ab = Nab = abN.$$

Comment It is worth making doubly sure that this product makes sense, or is well-defined as we say, by checking that if we take different representatives for our cosets, the product coset is still the same. We say the outcome is *independent of the coset representatives used*. That is, let us suppose that $aN = a_1N$ and $bN = b_1N$, which is equivalent to saying that $aa_1^{-1}, bb_1^{-1} \in N$ (Question 4 Set 5). Then we need to check that $abN = a_1b_1N$. Now $ab(a_1b_1)^{-1} = abb_1^{-1}a_1^{-1}$. However $bb_1^{-1} = x \in N$, and then $axa^{-1} \in N$ as $N \lhd G$.

2. For associativity take aN, bN, and cN in G/N. Using associativity of G we obtain:

$$(aNbN)cN = abNcN = (ab)cN = a(bc)N$$

$$= aN(bNcN), \text{ as required.}$$

This shows that G/N is a semigroup and indeed a monoid as the coset N is the identity element: $(aN)N = aNeN = aeN = aN$ and similarly $N(aN) = aN$. Finally the inverse of aN is the coset $a^{-1}N$ as $(aN)(a^{-1}N) = aa^{-1}N = eN = N$, and similarly $(a^{-1}N)(aN) = N$. Therefore G/N is a group.

Comment We refer to G/N as a *quotient group* of G.

3. To show that η is well-defined suppose that $aN = bN$, which gives $ab^{-1} \in N = \ker(\phi)$, which in turn gives $\phi(ab^{-1}) = e_T$, so that $\phi(a)(\phi(b))^{-1} = e_T \Leftrightarrow \phi(a) = \phi(b)$, as required to show that η is indeed a function from G/N to $U = \phi(G)$.

To see that Φ is surjective, take any $u \in U$ so that $u = \phi(a)$ say. Then $aN \in G/N$ as $aN \mapsto \phi(a) = u$, hitting the nominated target in the range. Next, Φ is injective for suppose that $(aN)\Phi = (bN)\Phi$, which is to say that $\phi(a) = \phi(b)$, whence $\phi(ab^{-1}) = e_T$ so that $ab^{-1} \in N \Leftrightarrow aN = bN$, as required to show that Φ is one-to-one. Finally Φ is a homomorphism as

$$\Phi(aNbN) = \Phi(abN) = \phi(ab) = \phi(a)\phi(b) = \Phi(aN)\Phi(bN).$$

In conclusion, the mapping $\eta : G/N \to U$ is an isomorphism of G/N onto the homomorphic image $U = \phi(G)$.

Conversely let $N \lhd G$ and let $\eta : G \to G/N$ be defined by $a\eta = aN$. Then η is clearly surjective and η is a homomorphism by Question 2 for if we take $a, b \in G$ we then have

$$\eta(ab) = abN = aNbN = \eta(a)\eta(b).$$

Finally $a \in \ker(\eta)$ if and only if $a\eta = N \Leftrightarrow aN = N \Leftrightarrow a \in N$, so that $\ker(\eta) = N$, as required.

Comment It follows that, up to isomorphism, every homomorphic image of G has the form G/N for some normal subgroup of G. In particular this shows that all homomorphic images as they are called of G can be constructed from G itself (via its normal subgroups) without reference to any 'outside' group.

4. Since $aN = Na$ for all $a \in G$ it is certainly the case that $aN = Na$ for all $a \in H$ and so it follows that $HN = NH$. To see that HN is a subgroup of G take $a, b \in HN$, which we may write as $a = h_1n_1$ and $b = h_2n_2$ ($h_i \in H, n_i \in N, i = 1, 2$). Then

$$ab^{-1} = (h_1n_1)(h_2n_2)^{-1} = h_1(n_1n_2^{-1})h_2 = h_1nh_2$$

where $n = n_1n_2^{-1} \in N$. Since $HN = NH$ we may write $nh_2 = h_2'n_2'$ for some $h_2' \in H$ and $n_2' \in N$. But then

$$ab^{-1} = h_1nh_2 = (h_1h_2')n_2' \in HN$$

thereby showing that $HN \leq G$. Clearly $N \subseteq HN$ and since $aN = Na$ for all $a \in G$ it is the case that $aN = Na$ for all $a \in HN$ so we have $N \lhd HN$.

5. Since $H, N \leq G$ it is certainly the case that $H \cap N \leq G$. Take any $a \in H$. Then $a(H \cap N)a^{-1} \subseteq H$ as $H \leq G$ and $a(H \cap N)a^{-1} \subseteq N$ as $N \lhd G$. Therefore

$a(H \cap N)a^{-1} \subseteq H \cap N$ for all $a \in H$, which shows by Question 9(i) Set 5 that $H \cap N \lhd H$.

6. Define a mapping $\phi : H \to HN/N$ by $h \mapsto hN$. (Note that N is not assumed to be a subset of H so that hN lies in HN/N and not in H/N.) Then ϕ is a homomorphism as

$$\phi(ab) = abN = (aN)(bN) = \phi(a)\phi(b).$$

Then

$$\ker(\phi) = \{h \in H : hN = N\} = \{h \in H : h \in N) = H \cap N.$$

Finally we note that ϕ is a surjection because for any $hnN \in HN/N$ we have $hnN = hN = \phi(h)$. From the 1st Isomorphism theorem we conclude that

$$\frac{H}{H \cap N} \approx \frac{HN}{N}.$$

7. We consider the mapping $\phi : (G/N) \to G/M$ whereby $aN \mapsto aM$, first showing it to be well-defined. Suppose that $aN = bN$; then $ab^{-1} \in N \leq M$ so $aM = bM$ also and so ϕ is indeed a function and, by construction, a surjective function. What is more, ϕ is a homomorphism as

$$\phi(aNbN) = \phi(abN) = abM = (aM)(bM) = \phi(aN)\phi(bN).$$

Finally we identify the kernel of ϕ:

$$\ker(\phi) = \{aN : aM = M\} = \{aN : a \in M\} = M/N.$$

Hence by the 1st Isomorphism theorem we conclude that

$$(G/N)/(M/N) \approx G/M.$$

Comment This theorem is saying that if you factor G by a normal subgroup N, and factor the image by the normal subgroup M/N where $N \leq M$, then that is effectively the same as factoring out the larger normal subgroup M of G in the first place. The notation encourages this to be thought of as a kind of cancellation in the $\frac{G}{N}/\frac{M}{N} \approx \frac{G}{M}$.

8. Since ϕ is a homomorphism of the abelian group $(R, +)$ we have that $\phi(0) = 0$ so that $0 \in \ker(\phi)$, which is therefore not empty. Suppose that $a, b \in \ker(\phi)$ and $c \in R$. Then

$$\phi(a + b) = \phi(a) + \phi(b) = 0 + 0 = 0;$$

$$\phi(ac) = \phi(a)\phi(c) = 0\phi(c) = 0$$

and similarly $\phi(ca) = 0$ so that $\ker(\phi)$ is an ideal of R.

Suppose that $a \in \ker(\phi)$ so that $\phi(a) = \phi(0) = 0$. It follows that if ϕ is one-to-one then $a = 0$ and so $\ker(\phi) = \{0\}$.

Conversely suppose that $\ker(\phi) = \{0\}$ and suppose that $\phi(a) = \phi(b)$. Since group homomorphisms respect inverses we have (in additive notation)

$$\phi(a-b) = \phi(a+(-b)) = \phi(a) + \phi(-b) = \phi(a) - \phi(b) = 0$$

and so $a - b \in \ker(\phi) = \{0\}$ so that $a - b = 0$, which gives $a = b$. Hence if $\ker(\phi)$ is trivial then ϕ is indeed a monomorphism.

9. Since $(R, +)$ is an abelian group we immediately have that R/I is also with addition $(I + a) + (I + b) = I + (a + b)$. We need to check that the formula $(I + a)(I + b) = I + ab$ is well-defined, which is to say independent of the representatives of the cosets in the product. To that end suppose that $I + a = I + a'$ and $I + b = I + b'$. Then $a = a' + i, b = b' + j$, where $i, j \in I$. Then

$$ab = a'b' + (a'j + b'i + ij);$$

now since I is an *ideal* we have that $a'j, b'i, ij \in I$ so that $ab - a'b' = a'j + b'i + ij \in I$ and so $I + ab = I + a'b'$. The associativity of the semigroup $(R, \cdot)$ now follows from that of R as does the distributivity of addition over multiplication.

Comment Note that, unlike the case of groups, we are not claiming that the multiplication of the sets $(I + a)(I + b)$ in R results in the set $I + ab$, as we are not claiming that $I^2 + aI + Ib$ contains all of I; however we have shown that this rule acts as a valid multiplication in the ring R/I.

10. Let $I = \ker(f)$. Then the rule $I + a \mapsto f(a)$ is that of a well-defined mappng ϕ as if $I+a = I+b$ then $a-b \in \ker(f)$ so that $f(a-b) = f(a)-f(b) = 0$ so that $f(a) = f(b)$. This mapping ϕ is a homomorphism:

$$\phi((I + a) + (I + b)) = \phi(I + (a + b)) = f(a + b) = f(a) + f(b)$$

$$= \phi(I + a) + \phi(I + b);$$

$$\phi((I + a)(I + b)) = \phi(I + ab) = f(ab) = f(a)f(b)$$

$$= \phi(I + a)\phi(I + b).$$

Finally the mapping is clearly onto and is also one-to-one as if $\phi(I+a) = \phi(I+b)$ then $f(a) = f(b)$, so that $f(a - b) = 0$ so that $a - b \in I$ and so $I + a = I + b$. Therefore ϕ is an isomorphism between the rings R/I and S.

Conversely, give an ideal I of R consider the mapping $\eta : R \to R/I$ where $\eta(a) = aI$. This is clearly a surjection and $\eta(ab) = (aI)(bI) = abI = \eta(a)\eta(b)$ shows we have an epimorphism. Moreover

$$\ker(\eta) = \{a \in R : \eta(a) = I\} = \{a \in R : a \in I\} = I.$$

Comment In words, if S is a homomorphic image of R then there exists an ideal I such that $S \approx R/I$ and conversely if $I \lhd R$ then there exists a homomorphic image of R of the form R/I.

Problem Set 8

1. The claim is clear in the case where either $m = 1$ or $n = 1$ so we assume that $2 \leq m, n$. Consider the mapping $\phi : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ whereby $a\phi = (a, a)$. This mapping is always a homomorphism as, working with the appropriate modulus throughout we have

$$\phi(a + b) = (a + b, a + b) = (a, a) + (b, b) = \phi(a) + \phi(b).$$

Since $|\mathbb{Z}_m \times \mathbb{Z}_n| = mn = |\mathbb{Z}_{mn}|$ it follows that ϕ is an isomorphism if and only if ϕ is one-to-one, which is equivalent to saying that $\ker(\phi)$ is trivial, so let us suppose that $a\phi = (0, 0)$, $(0 \leq a \leq mn - 1)$ which is to say that

$$(a, a) = (0, 0) \Leftrightarrow (m|a \wedge n|a).$$

Now let us suppose further that m and n are relatively prime. The Chinese remainder theorem tells us that if $(m, n) = 1$ then there is a unique $x = a$ with $0 \leq a \leq mn - 1$ such that for any integers b and c, $x \equiv b \pmod{m}$ and $x \equiv c \pmod{n}$. In particular, taking $b = c = 0$ it follows that $a = 0$ is the unique member of $\mathbb{Z}_{mn}$ such that $m|a$ and $m|b$ and so ϕ is a required isomorphism.

Conversely suppose that $\alpha : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ is any homomorphism. Then $0\alpha = (0.0)$. Now let d denote a common factor of m and n. Then $(\frac{mn}{d})\phi = (\frac{n}{d}m.\frac{m}{d}n) = (0, 0)$. However if $d \geq 2$ then $\frac{mn}{d} \not\equiv 0 \pmod{mn}$ and so ϕ is not one-to-one and so α is not an isomorphism. Therefore if $\mathbb{Z}_{mn} \approx \mathbb{Z}_m \times \mathbb{Z}_n$ then m and n have no common factor apart from 1.

Comment Some texts denote the cyclic group $\mathbb{Z}_n$ by C_n (C for cyclic) and reserve the symbol $\mathbb{Z}_n$ for the *ring* $\mathbb{Z}_n(+, \cdot)$.

2 (i) The prime decomposition of 12 is $12 = 2^2 \cdot 3$. In prime power factor form we have that the distinct (i.e. pairwise non-isomorphic) abelian groups of order 12 are:

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3, \text{ and } \mathbb{Z}_4 \times \mathbb{Z}_3;$$

in invariant factor form these two groups have respective representations:

$$\mathbb{Z}_2 \times \mathbb{Z}_6, \text{ and } \mathbb{Z}_{12}.$$

(ii) $72 = 2^3 \cdot 3^2$. Hence the six distinct abelian groups of order 72 are:

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \approx \mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_6, \ 2|6|6$$

$$\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \approx \mathbb{Z}_6 \times \mathbb{Z}_{12}, \ 6|12;$$

$$\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \approx \mathbb{Z}_3 \times \mathbb{Z}_{24}, \ 3|24;$$

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \approx \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{18}, \ 2|2|18;$$

$$\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_9 \approx \mathbb{Z}_2 \times \mathbb{Z}_{36}, \ 2|36;$$

$$\mathbb{Z}_8 \times \mathbb{Z}_9 \approx \mathbb{Z}_{72}.$$

(iii) $1176 = 2^3 \cdot 3 \cdot 7^2$:

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_7 \times \mathbb{Z}_7 \approx \mathbb{Z}_2 \times \mathbb{Z}_{14} \times \mathbb{Z}_{42}, \ 2|14|42;$$

$$\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_7 \times \mathbb{Z}_7 \approx \mathbb{Z}_2 \times \mathbb{Z}_{28} \times \mathbb{Z}_{84},\ 2|28|84;$$

$$\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_7 \times \mathbb{Z}_7 \approx \mathbb{Z}_7 \times \mathbb{Z}_{168};\ 7|168;$$

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_{49} \approx \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{294},\ 2|2|294;$$

$$\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_{49} \approx \mathbb{Z}_2 \times \mathbb{Z}_{588},\ 2|588;$$

$$\mathbb{Z}_8 \times \mathbb{Z}_{147} \approx \mathbb{Z}_{1176}.$$

(iv) Writing each group in turn in invariant factor form the list becomes:

$$\mathbb{Z}_{24}, \mathbb{Z}_2 \times \mathbb{Z}_{12}, \mathbb{Z}_{24}, \mathbb{Z}_2 \times \mathbb{Z}_{12}, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_6, \mathbb{Z}_2 \times \mathbb{Z}_{12};$$

hence the isomorphism groups are:

$$\{\mathbb{Z}_{24}, \mathbb{Z}_8 \times \mathbb{Z}_3\}, \{\mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_2, \mathbb{Z}_2 \times \mathbb{Z}_{12}, \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_2\}, \{\mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2\}.$$

3. First let us suppose that $G \approx \mathbb{Z}_{p^k}$ for some prime power $n = p^k$. The factors of n then have the form p^r for some $r \leq k$. Take $a = p^{k-r} \in \mathbb{Z}_{p^k}$. Then $ta = 0$ in G if and only if $p^k | ta$ and the least t for which this holds is $t = p^r$. Hence the order of p^{k-r} in G is p^r, which established the claim in the case of an abelian group of prime power order.

Now take an arbitrary finite abelian group with prime power factor decomposition $G \approx \mathbb{Z}_{p_1^{k_1}} \times \cdots \times \mathbb{Z}_{p_m^{k_m}}$. Then $n = |G| = p_1^{k_1} \cdots p_m^{k_m}$. Any factor $r|n$ has the form $r = p_1^{r_1} \times \cdots \times p_m^{r_m}$ for $0 \leq r_i \leq k_i$ $(1 \leq i \leq m)$. By the previous paragraph we know that for each i there exists $H_i \leq \mathbb{Z}_{p_i^{k_i}}$ such that $|H_i| = p_i^{r_i}$. Then $H = H_1 \times \cdots \times H_m \leq G$ and $|H| = p_1^{r_1} \cdots p_m^{r_m}$, as required.

Comment In general the converse of Lagrange's theorem does not hold, for the smallest counterexample see Problem 10 Set 10.

4 Certainly $e \in Z(G)$ so the centre of a group is not empty. Let $a, b \in Z(G)$ and let $x \in G$. Then

$$(ab^{-1})x = a(x^{-1}b)^{-1} = a(bx^{-1})^{-1} = axb^{-1} = x(ab^{-1}),$$

showing that $ab^{-1}Z(G)$ which is therefore a subgroup of G. Indeed $Z(G) \lhd G$ as for any $g \in G, a \in Z(G)$ we have $gag^{-1} = agg^{-1} = a$ so that, in a trivial fashion, $Z(G)$ is closed under conjugation. Moreover, since each member of $Z(G)$ commutes with all members of G, such a member certainly commutes with all members of $Z(G)$ and therefore $Z(G)$ is an abelian normal subgroup of G.

Next consider the mapping $\alpha : G \to \mathrm{Inn}(G)$ defined by $g \mapsto \phi_g$, where ϕ_g is as introduced in Question 9 Set 6. Then α is a homomorphism as the statement that $\alpha(gh) = \alpha(g)\alpha(h)$ means just that $\phi_{gh} = \phi_g \phi_h$, which we have already observed in Question 9 (ii) of Set 6. By construction, the range of α is the whole of $\mathrm{Inn}(G)$, so it remains to describe $\ker(\alpha)$. Now $g \in \ker(\alpha)$ if and only if $\phi_g = \phi_e$, which in turn is equivalent to saying that for all $a \in G$ we have

$$\phi_g(a) = \phi_e(a) \Leftrightarrow gag^{-1} = eae^{-1} = eae = a$$

$$\Leftrightarrow ga = ag \ \forall a \in G$$
$$\Leftrightarrow a \in Z(G).$$

Therefore by the 1st isomorphism theorem we conclude that $G/Z(G) \approx \mathrm{Inn}(G)$.

5. By inspection we see that $Z(Q) = \{\pm 1)$ (Set 4, Question 3)and $Z(D) = \{R_0, R_2\}$(Set 5, Question 5) (you need to identify elements in the table with identical row and column). It follows that $Z(Q) \approx \mathbb{Z}_2 \approx Z(D)$ and since the relation $\approx$ is transitive, we have that the centres of these groups are isomorphic. The order of both quotient groups $Q/Z(Q)$ and $D/Z(D)$ is $\frac{8}{2} = 4$. By inspection the order of each non-identity element in $Q/Z(Q)$ is 2, for example $((-k)\{1,-1\})^2 = (-1)\{1,-1\} = \{-1,1\} = Z(Q)$ and so it follows that $Q/Z(Q) \approx \mathbb{Z}_2 \times \mathbb{Z}_2$. Similarly all non-identity members of $D/Z(D)$ have order 2: the square of each reflection $S_i^2 = R_0$ and $R_1^2 = R_3^2 = R_2$, and so $D/Z(D) \approx \mathbb{Z}_2 \times \mathbb{Z}_2$ also. However, despite this, it is still not the case that $Q \approx D$, which can be from the fact that D the set of self-inverse elements of D numbers six: $\{R_0, R_2, S_0, S_1, S_2, S_3\}$ while there are only two self-inverse elements in Q, they being ± 1, the others all having order 4.

6. Applying the result of Question 9 (iii) Set 6 to the automorphism ϕ_g gives:

$$g[a,b]g^{-1} = [gag^{-1}, gbg^{-1}] \tag{5}$$

and so the conjugate of a commutator is a commutator. Now an arbitrary member of the G_1 has the form $x = c_1c_2\cdots c_n$ $(n \geq 0)$ where each c_i is a commutator. Then since ϕ_g is a homomorphism we have

$$\phi_g(x) = \phi_g(c_1)\phi_g(c_2)\cdots\phi_g(c_n),$$

which by (5) is a product of commutators and therefore G_1 is a normal subgroup of G.

To see that G/G_1 is abelian, let $aG_1, bG_1 \in G/G_1$. The required conclusion that $(aG_1)(bG_1) = abG_1 = baG_1 = (bG_1)(aG_1)$ is equivalent to showing $(ab)(ba)^{-1} \in G_1$. However

$$(ab)(ba)^{-1} = aba^{-1}b^{-1} = [a^{-1}, b^{-1}] \in G,$$

thus completing the proof.

7. Clearly $e \in C(a)$ so that $C(a) \neq \emptyset$. Take $x, y \in C(a)$. Then

$$(xy)a = x(ya) = x(ay) = (xa)y = (ax)y = a(xy)$$

so that $xy \in C(a)$ and hence $C(a)$ is a subsemigroup of G. Next, since $ax = xa$ we see that

$$(ax = xa) \Rightarrow (axx^{-1} = xax^{-1}) \Rightarrow (x^{-1}a = x^{-1}xax^{-1})$$
$$\Rightarrow x^{-1}a = ax^{-1}$$

so that $x \in C(a)$ implies that $x^{-1} \in C(a)$ and therefore $C(a) \leq G$.

8. (i) Observe that

$$gC(a) = hC(a) \Leftrightarrow gh^{-1} \in C(a) \Leftrightarrow gh^{-1}a = agh^{-1}$$

$$\Leftrightarrow h^{-1}ah = g^{-1}ag.$$

Hence we have a bijection from the set of left cosets of $C(a)$ onto the conjugacy class $Cl(a)$ defined by the rule $gC(a) \mapsto g^{-1}ag$.

(ii) Since G is partitioned by its conjugacy classes we may write:

$$|G| = \sum_a |Cl(a)|$$

where the sum takes one representative a from each conjugacy class of G. However, by part (i), each $|Cl(a)|$ may be replaced by the number of left cosets of $C(a)$ (the index of $C(a)$ in G) giving us the *Class equation*:

$$|G| = \sum_a [G : C(a)]$$

where once again the sum is taken over a cross-section (or *transversal*) of representatives from the conjugacy classes of G.

9. Observe that the conjugacy class of a in G is trivial if and only if $a \in Z(G)$ in which case $[G : C(a)] = 1$ as $C(a) = G$. Hence the class equation takes the form:

$$|G| = |Z(G)| + \sum_a [G : C(a)] \tag{6}$$

where the sum is over all a representing non-trivial conjugacy classes. Now suppose that $|G| = p^n$, a prime power. By Lagrange's theorem we infer that $|C(a)| = p^k$ for some $k \leq n - 1 (k \neq n$ for $a \notin Z(G))$. Hence

$$[G : C(a)] = \frac{|G|}{|C(a)|} = p^{n-k},$$

is a proper prime power ($n - k \neq 0$). Therefore p is a divisor of every term in (6) and since $|Z(G)| \geq 1$ (as $e \in Z(G)$) it follows that $|Z(G)|$ is also a non-zero power of p. In particular $Z(G)$ is not trivial.

10. (i) Let G be any group of order p^2 where p is prime. By Question 9, $|Z(G)| = p$ or p^2. We are asked to show the latter so by way of contradiction, let us suppose that $|Z(G)| = p$ and consider the quotient group $G/Z(G)$ which then consists of $\frac{p^2}{p} = p$ cosets.

Since every group of prime order is cyclic, we have that $G/Z(G) = \langle aZ(G) \rangle$ for some generator $aZ(G)$. In particular, every element of G has the form $a^t z$ for some $0 \leq t \leq p - 1$ and $z \in Z(G)$. However any two elements of that form commute with each other:

$$a^{t_1} z_1 \cdot a^{t_2} z_2 = a^{t_2} z_2 \cdot a^{t_1} z_1$$

as each z_i commutes with all elements of G and powers of a commute with one another. It follows that $Z(G) = G$ after all, which is to say that G is abelian.

(ii) In particular for the prime $p = 3$ we see that all groups of order $3^2 = 9$ are abelian and by the structure theorem for finite abelian groups we obtain exactly two distinct groups of order 9, they being $\mathbb{Z}_3 \times \mathbb{Z}_3$ and $\mathbb{Z}_9$.

Problem Set 9

1. For any $x, y \in S^1 (xy)\Phi = \rho_{xy}$ and $x\Phi y\Phi = \rho_x \rho_y$. We need to check equality of these mappings, but this follows by associativity of S^1 as for any $a \in S^1$ we have

$$a\rho_{xy} = a(xy) = (ax)y = a\rho_x \rho_y$$

and so Φ is a homomorphism from S_1 to T_{S^1}. To see it is injective, suppose that $x\Phi = y\Phi$ so that $\rho_x = \rho_y$. Then, in particular for $a = 1$ we get $1\rho_x = 1\rho_y$ so that $1x = 1y$ and so $x = y$. Therefore Φ is a monomorphism. In conclusion, the natual embedding of S into S^1 followed by Φ is then a monomorphism from S into T_{S^1}. Therefore any semigroup may be embedded in a semigroup of transformation and if S is finite, so is the semigroup of mappings into which it is embedded.

Comment The mapping Φ does define a homomorphism of S into T_S but it is not necessarily one-to-one. For example, if S is a left zero semigroup then for any $x \in S$ we have $a\rho_x = ax = a = ay = a\rho_y$ so that $\rho_x = \rho_y$ is *always* true and the range of $S\Phi$ of Φ has only one member (the identity mapping) and so is the trivial group, which does not contain a copy of S. This difficulty however does not arise with groups (see Question 3).

2. In the case where $S = G$ is a group, we need to check that $x\Phi \in S_G$, which is to say that ρ_x is a permutation (and not just a mapping) on the base set G. However this follows at once by group cancellativity for if $a\rho_x = b\rho_x$ we have $ax = bx$ and so $a = b$. Since $G = G^1$ we know by the argument of Question 1 that Φ is one-to-one and Φ is a homomorphism as before. Therefore we have *Cayley's theorem for groups*, every group G may be embedded in the symmetric group S_G. (And again, G is finite if and only if S_G is finite.)

3. An arbitrary mapping α on X is constructed by making n independent choices for $\alpha(1), \cdots, \alpha(n)$. Hence $|T_n| = n^n$.

An arbitrary permutation α is constructed by making n choices for $\alpha(1)$, then $n - 1$ for $\alpha(2)$ (as α is one-to-one) and so on, giving a total number of $n(n-1)\cdots 2 \cdot 1 = n!$, so that $|S_n| = n!$.

4.

$$(1\,4\,2)(2\,1\,8)(6\,3\,5\,1) = (1\,4\,6\,3\,5)(2\,8).$$

5.

$$(1\,2\,3)(4\,1\,2)^{-1}((2\,1) = (1\,2\,3)(2\,1\,4)(1\,2) = (1\,2\,3\,4).$$

6.

$$(1\,2\,\cdots n) = (1\,2)(1\,3)\cdots(1\,n) \tag{7}$$

Since each permutation in S_X (with X finite) can be written as a product of cycles and that (7) shows that each of those cycles can be written as a product of transpositions, it follows that the set of all transpositions acts as a generating set of S_X.

7. Now $\alpha = (3\,2\,4)(1\,6\,4) = (1\,6\,4\,3\,2)$. Hence

$$\sigma^{-1}\alpha\sigma = (2\,3)(1\,8\,6\,4)(1\,6\,4\,3\,2)(4\,6\,8\,1)(2\,3) = (2\,3\,4\,8\,6).$$

8. $(\sigma(3)\,\sigma(2)\,\sigma(4))(\sigma(1)\,\sigma(6)\,\sigma(4)) = (2\,3\,6)(4\,8\,6) = (2\,3\,4\,8\,6)$, in accord with Question 7.

9. We have $((\sigma(1)\,\sigma(3)\,\sigma(4))(\sigma(2)\,\sigma(5)) = (4\,3\,2)(1\,5)$ so that one solution for $\sigma \in S_5$ is given by setting $\sigma = \left(\begin{smallmatrix}1&3&4&2&5\\4&3&2&1&5\end{smallmatrix}\right) = (1\,4\,2)$.

Comment Note that we use that if C, D are two cycles then $\sigma^{-1}CD\sigma = \sigma^{-1}C\sigma\sigma^{-1}D\sigma$, so that we can apply the given conjugation formula, which is itself easily verified, to each cycle separately. We may check our answer:

$$\sigma^{-1}(1\,3\,4)(2\,5)\sigma = (2\,4\,1)(1\,3\,4)(2\,5)(1\,4\,2) = (1\,5)(2\,4\,3) = (4\,3\,2)(1\,5).$$

However the solution is not unique as we may write the cycles in any cyclic order before equating as we have done: in this example there will be $3 \times 2 = 6$ permutations σ satisfying the given conjugation equation.

10 (i) We have an expression of the form $\sigma^{-1}(1\,2)\sigma = (\sigma(1)\,\sigma(2))$ where $\sigma = (1\,2\,\cdots n)^k$ so that, under σ we have $i \mapsto (i+k) \pmod n$. In particular $(\sigma(1)\,\sigma(2)) = (1+k\,2+k)$ (addition mod n), as required.

(ii) Any member of S_n is a product of cycles. By Question 6, each cycle can be factored as a product of transpositions. By (i) each transposition of the form $(k\,k+1)$ can be written as a product of the two given generator cycles, $(1\,2\,\cdots n)$ and $(1\,2)$ so to complete the proof we need to check that any arbitrary transpostion $(i\,j)$ is a product of transpositions of the form $(k\,k+1)$. Without loss, take $i < j$. Then a required factorization is given by:

$$(i\,j) = (i\,i+1)(i+1\,i+2)\cdots(j-1\,j).$$

Problem Set 10

1. Let $x, y \in A_n$ so that x and y are products of $2t$ and $2s$ transpositions and let $a \in S_n$ with a the product of r transpositions. (Remember the transpositions are a generating set for S_n by Question 6 Set 9.) Then xy is a product of $2t + 2s = 2(t+s)$ transpositions, so that A_n is a subsemigroup of S_n. We may write the identity mapping ε as a product of zero transpositions, or as a product of two transpositions: $(1\,2)^2 = \varepsilon$; certainly $\varepsilon \in A_n$. Finally, by

writing the $2t$ transpositions whose product is x in reverse order, we see that x^{-1} is also a product of $2t$ transpositions, so in particular $x^{-1} \in A_n$. Therefore $A_n \leq S_n$. Finally A_n is closed under conjugation as zxz^{-1} is a product of $r + 2t + r = 2(r + t)$ transpositions (where z is a product of t transpositions), showing that $zxz^{-1} \in A_n$. We conclude that $A_n \lhd S_n$.

2. We have the factorization of the general cycle:

$$(1\,2\,\cdots n) = (1\,2)(1\,3)\cdots(1\,n)$$

showing that a cycle of length n is a product of $n-1$ transpositions. In particular any odd cycle is a member of A_n.

3.

$$P(x_1, x_2, x_3, x_4) = (x_1 - x_2)(x_1 - x_3)(x_2 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4).$$

4.

$$\mathrm{sgn}(\sigma) = \tfrac{P(x_2,x_5,x_3,x_1,x_4)}{P(x_1,,x_2,x_3,x_4,x_5)} = \tag{8}$$

$$\frac{(x_2 - x_5)(x_2 - x_3)(x_2 - x_1)(x_2 - x_4)(x_5 - x_3)(x_5 - x_1)(x_3 - x_1)(x_3 - x_4)(x_1 - x_4)}{P(x_1, x_2, x_3, x_4, x_5)}$$

$= (-1)^n$ where n is the number of changes of sign of the common factors in the quotient, which we count as $1 + 1 + 1 + 1 + 1 = 5$ so that $\mathrm{sgn}(\sigma) = -1$.

Comment We shall refer to the denominator and numerator in (8) as P and P_σ respectively.

5. As observed, the same factors appear in both polynomials except for a change of sign if $i < j$ but x_j precedes x_i. In particular the value of the quotient is either ± 1.

6. By Question 5 we have that sgn: $S_n \to \{-1, 1\}$, so it remains to check that $\mathrm{sgn}(\sigma\tau) = \mathrm{sgn}(\sigma)\mathrm{sgn}(\tau)$ for any $\sigma, \tau \in S_n$.

$$\mathrm{sgn}(\sigma\tau) = \tfrac{P(x_{\sigma(\tau(1))},\cdots,x_{\sigma(\tau(n))})}{P(x_1,\cdots,x_n)}$$

$$= \frac{P(x_{\tau(1)}, \cdots, x_{\tau(n)})}{P(x_1, \cdots, x_n)} \cdot \frac{P(x_{\sigma(\tau(1))}, \cdots, x_{\sigma(\tau(n))})}{P(x_{\tau(1)}, \cdots, x_{\tau(n)})}$$

$$= \mathrm{sgn}(\tau) \cdot \mathrm{sgn}(\sigma) = \mathrm{sgn}(\sigma) \cdot \mathrm{sgn}(\tau).$$

7. Consider the sign of a transposition $\tau = (i\,j)$ with $i < j$. The factors that change sign when passing from P to P_τ are $(x_i - x_{i+1}), (x_i - x_{i+2}), \cdots, (x_i - x_j)$ and $(x_{i+1} - x_j), (x_{i+2} - x_j) \cdots, (x_{j-1} - x_j)$, which number $(j - i) + (j - 1 - i) = 2(j - i) - 1$, which is odd so that the sign of any transposition is odd. It follows from Question 6 that if a permutation σ is written as a product of k transpositions then $\mathrm{sgn}(\sigma) = (-1)^k$. Since this number is the same for any such product, it follows that the parity of the number of transpositions in any such product is always the same for any given σ, which is to say is either always even (in which case $\sigma \in A_n$) or is always odd.

Comment Permutations may now be called *even* or *odd* depending on whether they are a product of an even or an odd number of transpositions, without any ambiguity.

8. Now $\ker(\text{sgn}) = \{\sigma \in S_n : \text{sgn}(\sigma) = 1\} = A_n$.

Comment It follows that $|A_n| = \frac{1}{2}|S_n| = \frac{n!}{2}$ and that $A_n \lhd S_n$ because $[S_n : A_n] = 2$ (Set 5, Problem 10).

9. From Question 2 we know that every cycle of odd length is an *even permutation* (i.e. lies in A_n) and in particular every 3-cycle lies in A_n. Since any member of A_n is the product of an even number of transpositions, it is enough to show that the product of any pair of transpositions is a product of 3-cycles. There are only two cases: either the transpositions in the pair are disjoint or they are not. The first case may be represented by the product

$$(1\,2)(3\,4) = (1\,2\,3)(4\,3\,1),$$

a product of two 3-cycles, while the second simply equals a3-cycle as $(1\,2)(2\,3) = (1\,3\,2)$.

10. The alternating group A_4 has order $\frac{4!}{2} = 12$ but does not have a subgroup of order6. Suppose to the contrary that $H \leq A_4$ with $|H| = 6$. Since $[A_4 : H] = \frac{12}{6} = 2$, it follows that $H \lhd A_4$. By Question 9, A_4 contains all the 3-cycles in S_4, which number $4 \times 2 = 8$ (the 4 factor counts the fixed point and there are 2 cycles possible for the three points in the cycle). The other elements are the identity element and the 3 products of disjoint transpositions. Therefore H contains at least one 3-cycle: without loss we take that to be $\alpha = (1\,2\,3)$ and $\alpha^2 = (1\,3\,2)$. However by conjugation we also have

$$(1\,2)(3\,4)(1\,2\,3)(1\,2)(3\,4) = (1\,4\,2) \in H$$

so that H also contain $(1\,4\,2)$ and its square $(1\,2\,4)$. In like manner we get

$$(1\,4)(2\,3)(1\,2\,3)(1\,4)(2\,3) = (2\,4\,3) \in H$$

and so also $(2\,4\,3)^2 = (2\,3\,4) \in H$. And similarly

$$(1\,2)(3\,4)(2\,3\,4)(1\,2)(3\,4) = (1\,4\,3) \in H$$

as is $(1\,4\,3)^2 = (1\,3\,4)$, giving the contradiction that $|H| \geq 8$. Therefore A_4 has no subgroup of order 6 so that the converse of Lagrange's theorem is in general false.