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.*

Problem Set 1 Sets and Relations

A *relation* R between sets A and B is a subset $R \subseteq A \times B$. If $A = B$ then R is a *relation on* A. The *composition* $R \circ S$ of a relation $R \subseteq A \times B$ and a relation $S \subseteq B \times C$ is the relation $R \circ S \subseteq A \times C$:

$$R \circ S = \{(a, c) : \exists b \in B, (a, b) \in R, (b, c) \in S\}.$$

1. Let $A = \{1, 2, 3, 4\}$,$B = \{a, b, c, d\}$, $C = \{v, w, x, y, z\}$

$R = \{(1, a), (1, b), (2, c), (3, d), (4, d)\}$, $S = \{(a, w), (a, x), (b, x), (d, y)\}$.

Calculate $R \circ S$.

A relation R on a set A is *reflexive* if $(a, a) \in R \forall a \in A$; R is *symmetric* if $(a, b) \in R \rightarrow (b, a) \in R$, and *transitive* if $(a, b), (b, c) \in R \rightarrow (a, c) \in R$. If R possesses all three properties then R is an *equivalance relation* and the equivalance classes of R partition A into disjoint blocks. We say R is *anti-symmetric* if $(a, b) \in R$ and (b, a) in R implies that $a = b$. We say R is a *partial order* on A if R is reflexive, transitive and anti-symmetric; we say R is *total* if for all $a, b \in A$, $(a, b) \in R$ or $(b, a) \in R$. Decide which of the preceding properties are possessed by each of the following relations.

2. Let $A = \mathbb{Z}$ and aRb means that $ab > 0$.
3. Let $A = \mathbb{Z}^+$ and aRb means that $a|b$ (a is a factor of b).
4. Let $A = \mathbb{Z}^+$ with $a \equiv b \pmod{n}$.
5. Show that if R is a symmetric and transitive relation on a set A and if for all $a \in A$, it is the case that$\{(a, b) : a \in A\} \neq \emptyset$, then R is an equivalence relation on A.
6. Show that a relation R on A is both symmetric and anti-symmetric if and only if $R \subseteq \iota$, where ι is the equality relalation.
7. Let $A = \{1, 2, \cdots, 9\}$ and define a relation $\sim$ on $A \times A$ by $(a, b) \sim (c, d)$ if $a + d = b + c$. Show that $\sim$ is an equivalence and find the equivalence class

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

Although relations are generally composed from left to right, however for function (Questions 8-10) composition $g \circ f$ will mean first f then g, in the tradition of calculus.

8. Show that the composition of two *injective* (one-to-one) functions is injective.
9. Repeat Question 8 for *surjective* (onto) functions and deduce that the composition of two bijections is a bijection.
10. Let $f : A \rightarrow B$ be a function. Show that $f \circ f^{-1}$ is the identity function on the range of f but that $f^{-1} \circ f$ is an equivalence relation that induces a partition of A.

Problem Set 2 Semigroups, Monoids, and Groups

A *semigroup* $(S, \circ)$ is a set S with an associative binary operation $\circ$ (often not explicitly written and often known as *multiplication*) $\circ : S \times S \to S$ so that $a \circ (b \circ c) = (a \circ b) \circ c$. A semigroup S is a *monoid* if there exists an *identity element* $e \in S$ such that $ex = xe = x$ for all $x \in S$. A *homomorphism* between semigroups $\alpha : S \to T$ is a function that satisfies $\alpha(ab) = \alpha(a)\alpha(b)$ $(a, b \in S)$. A *monoid homomorphism* must also map the identity of S to that of T.

1. *Full transformation semigroup* Let X be a set. Show that

$$T_X = \{\alpha : X \to X\}$$

under the operation of function composition is a monoid and give its identity element.

2 (i) Show that the identity element of a monoid is unique.
(ii) Show that if $f : S \to T$ and $g : T \to V$ are homomorphisms then $g \circ f : S \to V$ is also a homomorphism.

3. Let S be any semigroup. Let S^1 be the same as S if S is a monoid and otherwise let 1 stand for a symbol not in S and extend the multiplication on S to S^1 by defining $1x = x1 = x$. Show that S^1 is a monoid.

4. *Free monoid* $F_X^1 = \{x_1 x_2 \cdots x_n : n \geq 0, x_i \in X\}$ under the operation of *concatention* meaning that

$$(x_1 x_2 \cdots x_n)(y_1 y_2 \cdots y_m) = x_1 x_2 \cdots x_n y_1 y_2 \cdots y_m$$

$(x_i, y_j \in X)$. Show that F_X^1 is a monoid and give its identity element.

A *group* G is a monoid (with identity element e) in which for every $a \in G$ there exist an element, denoted by a^{-1} (*the inverse of* a) such that $aa^{-1} = a^{-1}a = e$.

5. *Symmetric group* A *subsemigroup* U of a semigroup S is a subset of S that is a semigroup when the binary operation is restricted to $U \times U$. Show that the subsemigroup of all *permutations* on X (that is bijections from X to X) is a subsemigroup S_X of T_X. Show further that S_X is a group.

6. *Direct product* of two (or more) semigroups. Let S_1, S_2 be semigroups. Then show that $S_1 \times S_2$ is a semigroup if we define the *pointwise product*

$$(s_1, s_2)(t_1, t_2) = (s_1 s_2, t_1 t_2),\ s_1, t_1 \in S_1,\ s_2, t_2 \in S_2.$$

Show that if S_1 and S_2 are both monoids (resp. groups), then so is $S_1 \times S_2$.

7. An *abelian group* is a group in which the group operation is commutative.

(i) Show that $(\mathbb{Z}_n, +)$, the set of integers $\{0, 1, 2, \cdots, n-1\}$ under addition modulo n is an abelian group with identity element 0.

(ii) The *order* of an element a of a group G is the least power n (if it exists) such that $a^n = e$, the identity of G. Show that if every non-identity element of a group has order 2 then G is abelian.

8. Let S be the set of 2×2 matrices with real entries and T the subset of S of all matrices with non-zero determinant. Show that under multiplication S is a monoid that is not a group and that T is a subsemigroup of S that is a group.

9. Show that a non-empty subset $H \subseteq G$ of a group G is a subgroup of G if and only if H satisfies the condition that $a, b \in H \rightarrow ab^{-1} \in H$.

10. Show that a semigroup S is a group if and only if the equations $ax = b$ and $ya = b$ $(a, b \in S)$ are always solvable in S. Show that in a group the solutions to these equations are unique.

Problem Set 3 Rings and Fields

A *ring* $(R, +, \cdot)$ is a non-empty set R such that $(R, +)$ is an abelian group (with identity element denoted by 0), $(R, \cdot)$ is a semigroup and these operations are linked by the *Distributive law* of addition over multiplication: $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$ $(a, b, c \in R)$.

If a ring has a *multiplicative identity* e then R is a *unital ring*. If the operation $(\cdot)$ is also commutative, then R is a *commutative ring*. An *integral domain* is a commutative ring with *no zero divisors*, meaning that whenever $ab = 0$ $(a, b \in R)$ then at least one of a, b is 0. A unital ring R is a *divison ring* if $(R \setminus \{0\}, \cdot)$ is a group; R is a *field* if $(R \setminus \{0\}, \cdot)$ is an abelian group. The idea of *subring* is defined as the obvious analogue to that of subgroup, subsemigroup, subspace (for vector spaces) etc.

1. Show that the collection R of all $n \times n$ matrices with real entries is a unital ring under matrix addition and multiplication but is not a commutative ring.

2. Show that the collection S of all non-singular members of R (of Question 1) is not a subring of R.

3. Show that $(\mathbb{Z}, +, \cdot)$ is an integral domain that is not a field.

4. Show that in any ring R and $r, s \in R$ we have:
(i) $r0 = 0r = 0$;
(ii) $(-r)s = r(-s) = -(rs)$;
(iii) $(-r)(-s) = rs$

5. Prove that a commutative unital ring R is an integral domain if and only if R is *cancellative* meaning that if $ab = ac$ and $a \neq 0$ then $b = c$.

6. Construct a finite field with four elements.

7. Let $\mathbb{R}[x]$ be the collection of all polynomials with coefficients from the field $\mathbb{R}$. Show that $\mathbb{R}[x]$ together with the operations of polynomial addition and multiplication is an integral domain but is not a field.

8. Clearly $(\mathbb{Z}_n, +, \cdot)$ is a commutative unital ring but for what values of n is it an integral domain?

9. Show that every field is an integral domain and that every finite integral domain is a field.

10. Show that $R = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ is an integral domain.

Problem Set 4 Further ideas for semigroups, groups, and rings

Throughout let S denote a semigroup, G denote a group, and R a ring.

1. A semigroup S is *left cancellative (right cancellative)* if whenever $ab = ac$ (resp. $ca = ba$) then $b = c$. Show that any group G is *cancellative* (both left and right cancellative). Find a semigroup that is niether left nor right cancellative and a semigroup that cancels on one side but not the other.

2. Show that a finite semigroup S is a group if and only if S is cancellative. Deduce that a finite subsemigroup of a group is a group.

3. The collection of *quaternion units* $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ forms a non-abelian group (the *Quaternion group*), under multiplication. Given that $(-1)x = x(-1)$ and so can be written as $-x$ for all $x \in Q$, display the multiplication table for Q given that $i^2 = j^2 = k^2 = ijk = -1$.

4. Let A be a non-empty subset of S. Let $\langle A \rangle$ be the intersection of all subsemigroups of S that contain A. Show that $\langle A \rangle$ is a subsemigroup of S, that it is the smallest in the sense it is contained in all subsemigroups of S that contain A and that

$$\langle A \rangle = \{a_1 a_2 \cdots a_n, a_i \in A, n \geq 1\}.$$

5. Repeat Question 4 for a group G and any subset $A \subseteq G$ and show that

$$\langle A \rangle = \{b_1 b_2 \cdots b_n, b_i \in A \cup A^{-1}, n \geq 0\},$$

where the empty product ($n = 0$ case) is taken to mean the identity element e and $A^{-1} = \{a^{-1} : a \in A\}$.

6. A group is called G is called *cyclic* if $G = \langle a \rangle$ for some $a \in G$ and a is called a *generator* of G. The *order* of a set (resp. a generator a) is the cardinal of that set (resp. of $\langle a \rangle$). Describe the set of generators of the cyclic group $(\mathbb{Z}_n, +)$. What is the order of this set?

A subring I of a ring R is called an *ideal* if it satisfies the condition that $aI \subseteq I$ and $Ia \subseteq I$ for all $a \in R$ and we write $I \lhd R$ to denote this.

7. Show that the only ideals of a field F are the *improper* ideals of $\{0\}$ and F itself.

8. In the case of R an integral domain, we call an ideal $I = aR$ the *principal ideal generated by* a. Show that aR is indeed an ideal in this case.

9. Show that every ideal of $(\mathbb{Z}, +, \cdot)$ is principal. (We call such an integral domain a *principal ideal domain*).

10. An ideal I of a ring R is called *maximal* if the only ideal of R that properly contains I is R itself. Find all the maximal ideals of the ring of integers.

Problem Set 5 Cosets and Lagrange's theorem

Let $H \leq G$ (meaning H is a subgroup of G) and let $a \in G$. Then aH is a *left coset* of H in G.

1. Show that the mapping $h \mapsto ah$ is a bijection from H onto aH, so that all cosets are equicardinal with H.

2. Show that either $aH = bH$ or these two cosets are disjoint.

3. Show that the (left) cosets of H partition G into subsets of equal cardinality.

4. Prove that $aH = bH$ if and only if $a^{-1}b \in H$.

5. The *dihedral group* D_4 is the group of symmetries of a square $S = ABCD$. Let R_k ($k \in \{0, 1, 2, 3\}$) represent a rotation of S about its centre O through k right angles anticlockwise and let S_k represent the reflection of S in the line through O making an angle of $\frac{\pi k}{4}$ with the horizontal line through O. Draw up the group table of D_4 and find the left and right cosets of $H = \langle S_0 \rangle$ in D_4.

6. *Lagrange's theorem* Let $H \leq G$, where G is a finite group. Define the *index* of H in G, denoted by $[G : H]$ be the number of (left) cosets of H in G. Show that

$$|G| = [G : H]|H|;$$

in particular show that the *order* (i.e. the cardinal) of the subgroup H is a divisor of the order of the containing group G.

7. Show that any group of prime order is cyclic.

8. Find all groups of order less than 6 and find a group of order 6 that is not abelian.

9. A subgroup $H \leq G$ is called *normal* if $aH = Ha$ for all $a \in G$. In particular all subgroups of an abelian group are normal.

(i) Show that H is normal in G if and only if $aHa^{-1} \subseteq H$ for all $a \in G$.

(ii) Show that if for all $a \in G$ there exists $b \in G$ such that $aH = Hb$, then H is normal in G.

(iii) Find an example of a group G with an abelian subgroup H such that H is not normal in G.

(iv) Let H be a subgroup of G of index 2. Prove that H is normal in G.

10. In Set 3 we used the fact that any intersection of subgroups of a group is a subgroup. In contrast:

(i) Show that the union of two subgroups $H \cup K$ of a group G is not a subgroup of G unless one of H, K is contained in the other.

(ii) Find an example of a group G that is a union of *three* of its subgroups, with none of the three contained in any of the others.

Problem Set 6 Homomorphisms of semigroups and of groups

A function $f : S \to T$ between two semigroups is a *homomorphism* if

$$f(ab) = f(a)f(b).$$

If f is also one-to-one then f is a *monomorphism*, if f is surjective then f is an *epimorphism*, and if f is a bijection then f is an *isomorphism*; an *automorphism* if $S = T$. In the case of isomorphism we write $S \approx T$. An *endomorphism* is any homomorphism from a semigroup to itself.

2. (i) Show that for any group homomorphism $\phi : G \to H$, $\phi(e_G) = e_H$.
(ii) Show that the composition of any two semigroup homomorphism is itself a homomorphism.

2 (i) Let $G = \langle i \rangle$, the subsemigroup of the complex numbers under multiplication. Show that $G \approx (\mathbb{Z}_4, +)$.

(ii) Show that $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$ are not isomorphic to each other.

3. Show that the image $f(S)$ of a semigroup S under a homomorphism $f : S \to T$ is a subsemigroup of T. Show that if S (but not necessarily T) is a group, then so is $f(S)$.

4. Continuing with Question 3, show that, if not empty, the inverse image $U = f^{-1}(V)$ of a subsemigroup V of T is a subsemigroup of S.

5. Show that if $f : G \to T$ is a homomophism from a group into a group, then $f(a^{-1}) = (f(a))^{-1}$. Show also that if V is a subgroup of T, then $U = f^{-1}(V)$ is a subgroup of G.

6. Suppose that T is a *homomorphic image* of a group G, meaning that there exists an epimorphism $\phi : G \to T$.
(i) Show that if G is finite, or is abelian, the same is true of T;

(ii) Show that if A is a generating set for G then $\phi(A)$ generates T;

(iii) Show that if $V \lhd T$ then $U = \phi^{-1}(V) \lhd G$.

7. Let $S = \mathbb{C}\backslash\{0\}$ with the operation $(\circ)$ defined by $a \circ b = |a|b$ $(a, b \in \mathbb{C}\backslash\{0\})$.

(i) Show that S is a left cancellative semigroup satisfying $aS = S$ for all $a \in S$.

(ii) Express the semigroup S as a direct product $G \times E$ where G is a group and E is a *right zero semigroup* (meaning that $ef = f$ for all $e, f \in E$).

8. Define the *kernel* of a group homomorphism $\phi : G \to H$ as

$$\ker\phi = \{g \in G : \phi(g) = e_H\}.$$

(i) Show that the kernel of a homomorphism is a normal subgroup of G.

(ii) Show that a homomorphism is one-to-one if and only if the kernel of ϕ is *trivial*, meaning that $\ker(\phi) = \{e_G\}$.

9 (i) For any $g \in G$ show that the mapping $\phi_g : G \to G$, where $\phi_g(a) = gag^{-1}$ $(g \in G)$ is an automorphism of G, known as an *inner automorphism* of G.

(ii) Show that $\mathrm{Inn}(G)$, the set of all inner automorphisms of G is a group under function composition. Indeed $\mathrm{Inn}(G) \lhd \mathrm{Aut}(G)$, the group of all automorphisms of G.

A *commutator* in a group G is defined to be an element $[a, b]$ of the form $a^{-1}b^{-1}ab$ $(a, b \in G)$ and the *commutator subgroup* G_1 of G is that generated by the commutators.

(iii) Prove that for any homomorphism $\phi : G \to G$ we have

$$\phi([a, b]) = [\phi(a), \phi(b)].$$

10. We say that g *is conjugate to* h $(g, h \in G)$ if $g = xhx^{-1}$ for some $x \in G$, in which case we write $g \sim h$. Show that conjugacy defines an equivalence relation on G. (The $\sim$-classes are known as the *conjugacy classes* of G.)

Problem Set 7 Homomorphic images for groups and for rings

A subgroup N of a group G (we write $N \leq G$) is called *normal* if $aNa^{-1} = N$ for all $a \in G$ (we write $N \lhd G$). Equivalently $aN = Na$ for all $a \in G$. (Recall Questions 9 and 10 of Set 5.) Throughout this problem set N will denote a normal subgroup.

1. Show that if $N \lhd G$ then $(aN)(bN) = abN$ for all $a, b \in N$.

2. Let G/N denote the collection of cosets of a normal subgroup. Show that G/N is itself a group, (with identity element N), under multiplication as defined in Question 1.

3. *First isomorphism theorem* Let $\phi : G \to T$ be a group homomorphism. Put $N = \ker(\phi)$ and $U = \phi(G)$. Show that the mapping $\Phi : G/N \to U$ whereby $aN \mapsto \phi(a)$ is an isomorphism. Conversely for any normal subgroup of G, the group G/N is itself a homomorphic image of G under the natural mapping $\eta : G \to G/N$ whereby $\eta(a) = aN$ and $\ker(\eta) = N$.

4. Let $H \leq G$ (meaning that H is a subgroup of G) and $N \lhd G$. Then $HN = NH$ and $HN \leq G$. Also $N \lhd HN$.

5. Prove that $H \cap N \lhd H$.

6. *Second isomorphism theorem* For $H \leq G$ and $N \lhd G$

$$(HN)/N \approx H/H \cap N.$$

7. *Third isomorphism theorem* Let $N \leq M$ with $N, M \lhd G$. Show that $N \lhd M$ and that

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

Define a *ring homomorphism* $f : R \to S$ to be a mapping between rings R and S such that $f(a+b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$ for all $a, b \in R$. The *kernel* of f is then $\ker(f) = \{a \in R : f(a) = 0\}$.

8. Show that the kernel of a ring homomorphism is an ideal of R and that f is one-to-one if and only if $\ker(f) = \{0\}$.

9. Given an ideal I of a ring R show that the set of cosets R/I form a ring under the operations $(I + a) + (I + b) = I + (a + b)$ and $(I + a)(I + b) = I + ab$ $(a, b \in R)$.

10. Prove the *First isomorphism theorem for rings:* for an epimorphism of rings $f : R \to S$ show that $R/\ker f \approx S$ under the homomorphism $\phi : R/ker(f) \to S$ whereby $I + a \mapsto f(a)$, where I stands for the ideal $\ker(f)$ and conversely, for $I \lhd R$ the natural homomorphism $\eta : R \to R/I$ where $a\eta = aI$ is an epimorphism with $\ker(\eta) = I$.

Problem Set 8 Commutativity and Abelian groups

Any *finitely generated* abelian group G (so that $G = \langle A \rangle$ for some finite subset A of G) is isomorphic to a direct product of a number of cyclic groups $(\mathbb{Z}_n, +)$ and infinite cyclic groups, $(\mathbb{Z}, +)$, each of which is isomorphic to the integers under addition. The group G can be displayed uniquely in two different ways: the *invariant factor decomposition*:

$$G \approx (\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}) \times (\mathbb{Z} \times \cdots \times \mathbb{Z})$$

where $n_1 | n_2 | \cdots | n_k$, or alternatively the *prime power factor decomposition*:

$$G \approx (\mathbb{Z}_{p_1^{k_1}} \times \mathbb{Z}_{p_2^{k_2}} \times \cdots \times \mathbb{Z}_{p_m^{k_m}}) \times (\mathbb{Z} \times \cdots \times \mathbb{Z})$$

where $p_1 \leq p_2 \leq \cdots \leq p_k$ are primes and $k_i \geq 1$.

1. Use the *Chinese Remainder Theorem* (see Comment to solution of Question 6, Set 1 of MA202) to show that $\mathbb{Z}_m \times \mathbb{Z}_n \approx \mathbb{Z}_{mn}$ if and only if m and n have no common factor other than 1.

2. Find (up to isomorphism) all abelian groups G of the following orders, writing each in both forms provided by the theorem above:

(i) 12; (ii) 72; (iii) 1176.

(iv) Group the following abelian groups by isomorphism:

$\mathbb{Z}_{24}$, $\mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_8 \times \mathbb{Z}_3$, $\mathbb{Z}_6 \times \mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_{12}$, $\mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_2$.

3. *Converse of Lagrange's theorem for abelian groups* Show that if G is a finite abelian and n is a factor of $|G|$ then there exists a subgroup H of G of order n.

4. The *centre of a group* G is defined as

$$Z(G) = \{a \in G : ax = xa \, \forall x \in G\}.$$

Show that $Z(G)$ is a normal abelian subgroup of G and that $G/Z(G) \approx \mathrm{Inn}(G)$, the group of all inner automorphisms of G.

5. Show that for the quaternion group Q and the dihedral group D that $Z(Q) \approx Z(D)$ and that $Q/Z(Q) \approx D/Z(D)$, yet Q and D are not isomorphic.

6. Recall the commutator group $G_1 \leq G$ (Question 9 Set 6). Prove that $G_1 \lhd G$ and that G/G_1 is abelian.

7. Define the *centralizer* $C(a)$ of $a \in G$ as $C(a) = \{g \in G : ag = ga\}$. Show that $C(a) \leq G$.

8 (i) Show that the index $[G : C(a)]$ is equal to the number of elements in the conjugacy class $Cl(a)$ of a.

(ii) Hence deduce *the Class equation*:

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

where the sum is taken over representatives a for the set of all conjugacy classes of G.

9. Use the class equation to show that a group of prime power order p^n $(n \geq 1)$ has a non-trivial centre.

10 (i) Use Question 9 to show that every group of order p^2, where p is a prime, is abelian.

(ii) Hence find all groups of order 9.

Problem Set 9 Cayley theorems and the symmetric group

In this set mappings are composed from left to right. Let S be a semigroup and consider $T = T_{S^1}$, the full transformation semigroup on S^1. Let $\rho_x \in T$ be the *right translation mapping* whereby $a \mapsto ax$ $(a \in S, x \in S^1)$. Define the mapping $\Phi : S^1 \to T_{S^1}$ by $x\Phi = \rho_x$.

1. Show that Φ is a monomorphism and deduce *Cayley's theorem for semigroups*, any semigroup S is *embeddable* in a full transformation semigroup. (Meaning is isomorphic to some subsemigroup of ...)

Cayley's theorem for groups

2. Let $\Phi : G \to S_G$ be the mapping by which $x\Phi = \rho_x$. Show that Φ embeds the group G into the group of permutations S_G.

3. What is the order of T_X and of S_X when $|X| = n \geq 1$?

Any permutation on $X_n = \{1, 2, \cdots, n\}$ can be written as a disjoint product of cycles $(i_1\, i_2\, \cdots\, i_k)$ where $i_1 \mapsto i_2 \mapsto \cdots \mapsto i_k \mapsto i_1$. Products of cycles are composed from left to right so, for example $(1\,2)(2\,3) = (1\,3\,2)$. The *inverse* of a permutation α is the permutation α^{-1} such that $\alpha\alpha^{-1} = \alpha^{-1}\alpha = e$, where e is the identity permutation that fixes each base point. The collection of all permutations on X_n under function composition forms the *symmetric group* S_n.

4. Express as a product of disjoint cycles in S_8 the product of the cycles $(1\,4\,2)(2\,1\,8)(7\,8)(6\,3\,5\,1)$.

5. Repeat Question 4 for the product $(1\,2\,3)(4\,1\,2)^{-1}(2\,1)$.

6. Write $(1\,2\,\cdots\,n)$ as a product of *transpositions* (2-cycles). Deduce that the symmetric group is generated by its set of transpositions.

7. For $\alpha = (3\,2\,4)(1\,6\,4)$ and $\sigma = (4\,6\,8\,1)(2\,3)$ on X_8 calculate the *conjugate* $\sigma^{-1}\alpha\sigma$.

8. Verify that the conjugate of Question 7 is equal to

$$((\sigma(3)\,\sigma(2)\,\sigma(4))(\sigma(1)\,\sigma(6)\,\sigma(4)).$$

9. Use the general fact that

$$\sigma^{-1}(i_1\, i_2\, \cdots\, i_k)\sigma = (\sigma(i_1)\,\sigma(i_2)\,\cdots\,\sigma(i_k)),$$

to solve $\sigma^{-1}(1\,3\,4)(2\,5)\sigma = (4\,3\,2)(1\,5)$ for $\sigma \in S_5$.

10 (i) Show that

$$(1\,2\,\cdots\,n)^{-k}(1\,2)(1\,2\,\cdots\,n)^k = (k+1\,k+2)$$

(addition modulo n).

(ii) Deduce from Question 6 and (i) that any permutation on X_n can be generated as a product of the two cycles $(1\,2\,\cdots\,n)$ and $(1\,2)$.

Problem Set 10 Even and odd permutations; the Alternating group

1. Let A_n be the subset of S_n of all permutations that may be written as a product of an even number of transpositions. Show that $A_n \lhd S_n$.

2. Show that any cycle $\pi \in S_n$ of odd length is a member of A_n.

We know that any member of S_n can be written as a product of transpositions. The following exercises show that although a particular member of S_n may be factorized as a product of transpositons in many ways, the number of transpositions used is either always even or always odd. Consider the polynomial

$$P = P(x_1, x_2, \cdots, x_n) = \Pi_{i<j}(x_i - x_j).$$

3. Write out P explicitly for the case of $n = 4$.

For $\sigma \in S_n$ define the *signature of* σ to be

$$\text{sgn}(\sigma) = \frac{P(x_{\sigma(1)}, x_{\sigma(2)}, \cdots, x_{\sigma(n)})}{P(x_1, x_2, \cdots, x_n)}.$$

4. Work out sgn $(\sigma)$for

$$\sigma = (1\,2\,4)(4\,5) \in S_5.$$

.

5. Explain why in general it is always the case that $\text{sgn}(\sigma) = \pm 1$.

6. Show that sgn is a homomorphism of S_n onto the two-element group $\{\pm 1\}$ under multiplication.

7. Deduce from this that σ cannot equal to products of transpositions of different *parities*, which is to say one product of even length and the other of odd length.

8. What is the kernel of the homomorphism σ?

9. Show that A_n is generated by the set of 3-cycles of S_n.

10. Prove that the converse of Lagrange's theorem fails for the group A_4.

Hints for Problems

Problem Set 1

Work directly with the definitions throughout.

7. Don't lose sight of the fact that the relation is between pairs of integers, and not between the integers themselves.

Problem Set 2

10. For any a there exists x such that $ax = a$. Work to show that x is a right identity element. Then show there is a left identity element and that it must equal x, and continue from there.

Problem Set 3

1. Associativity of matrix multiplication can be taken as granted, (although it is worth going through the verification of that at least once) as can the left and right distributive laws.

3. Again take all the ordinary laws of algebra as they apply to the integers for granted.

6. It can be shown that any field with 2^n members has *characterstic* 2, meaning that $a + a = 0$ is always true. You must have elements $0, 1$ and a say. Also $1 + a$ cannot equal any of the other three members.

9. To show we have a field take any $a \in R \setminus \{0\}$ and study the mapping on $R \setminus \{0\}$ where $x \mapsto ax$.

Problem Set 4

2. Apply the argument of Question 9 Set 3 to allow the conclusion from Question 10 of Set 2.

6. Express the property of being a generator in terms of existence of solutions of linear congruences modulo n.

9. Any ideal I consists of all multiples of its least positive member, n; to get

a contradiction to I not contained in $n\mathbb{Z}$ use the Euclidean algorithm in reverse *(Bezout Lemma)* to find a smaller positive member of I.

10. Show that the principal ideals generated by primes are maximal, again getting a contradiction to that claim by using the Euclidean algorithm in reverse.

Problem Set 5

2. Prove that if $aH \cap bH \neq \emptyset$ then $aH \subseteq bH$.

6, 7, 8. Apply Lagrange's theorem

8. Apply the result of Question 7.

9 (iii) Use Question 6.

10 (i) Look at the product of members that are in one subgroup and not the other. Where can it lie?

(ii) There is a counterexample of order 4.

Problem Set 6

1(i) First show that the identity of a group is the group's one and only idempotent.

2 (i) Write down a specific isomorphism between the two groups and check that it is a function, that it is one-to-one and onto, and that it is a homomorphism.

(ii) What feature does $\mathbb{Z}_4$ have that $\mathbb{Z}_2 \times \mathbb{Z}_2$ does not?

3. Any isomorphism must preserve the order of each member.

5. To show that $f(a^{-1}) = (f(a))^{-1}$ you just need to show that $f(a^{-1})f(a) = f(a)f(a^{-1}) = e_T$.

7 (i) First we need to check that $\mathbb{C}\setminus\{0\}$ is closed under this binary operation, and that operation is associative. Then check that S is left cancellative and that the equation $a \circ x = b$ can be solved in S.

(ii) Show that $S \approx G \times E$ where $G = \mathbb{R}^+$ under multiplication and E is the set of complex numbers of modulus 1.

9 (ii) To show closure under conjugacy just check that for any automorphism α we get $\alpha\phi_g\alpha^{-1} = \phi_{\alpha(g)}$.

Problem Set 7

3. You need first to check that the mapping is well-defined: if $aN = bN$ is

it true that $\phi(a) = \phi(b)$?

6. Show that the mapping from H to HN/N where $h \mapsto hN$ is an epimorphism with kernel $H \cap N$ and the apply the 1st Isomorphism theorem.

7. Show that the mapping from G/N to G/M where $aN \mapsto aM$ is an epimorphism and again apply the 1st isomorphism theorem.

Problem Set 8

1. Consider the kernel of the map from $\mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ where $a\phi = (a, a)$.

2. Write each group in invariant factor form and compare to identify isomorphism classes.

3. Solve the problem for the cyclic group $\mathbb{Z}_{p^k}$ for prime power p^k and then use the prime power decomposition form to get the general result.

4. What is the kernel of the homomorphism where $g \mapsto \phi_g$? Then apply the 1st isomorphism theorem.

9. Use Lagrange's theorem to show all the terms in the sum are p powers; noting that $|Z(G)|$ is one of these terms!

10. Factoring out the centre in these circmustances gives a quotient group which is cyclic.

Problem Set 9

1. You need to check that $\rho_{xy} = \rho_x \rho_y$. For injectivity you will need the presence of the identity 1.

2. This time you need to check that ρ_x is a permutation, and not just a function.

4. Remember to work with the cycles from left to right.

5. To get the inverse of a cycle, just reverse it.

9. Equate the given expression for each cycle, $\sigma^{-1} C \sigma$ with a cycle of the same length in the intended product.

10 (i) Again, make use of the conjugation rule for cycles.

10 (ii) Show that *any* transposition can now be written as a product of the two given cycles.

Problem Set 10

6. Write down $\operatorname{sgn}(\sigma\tau)$ and then multiply top and bottom by $P(x_{\tau(1)}, \cdots, x_{\tau(n)})$.

10. Use the fact that that any putative subgroup H of order 6 is normal in A_4(why?) to show that H contains all eight 3-cycles of A_4.

Answers to the Problems

Problem Set 1

1. $\{(1,w),(1,x),(3,y),(4,y)\}$. 2. Symmetric, transitive. 3.partial but not a total order. 4. equivalence relation. 7. $\{(1,4),(2,5),(3,6),(4,7),(5,8),(6,9)\}$.

Problem Set 2

See solutions

Problem Set 3

See solutions

Problem Set 4

6. $\{a \in \mathbb{Z}_n : \gcd(a,n) = 1\}$, the order of this set is $\phi(n)$, where ϕ is the Euler function.

10. I is maximal if and only if $I = p\mathbb{Z}$ for some prime p.

Problem Set 5

5. The left cosets are:$H = \{R_0, S_0\}$, $R_1H = \{R_1, S_1\}$, $R_2H = \{R_2, S_2\}$, $R_3H = \{R_3, S_3\}$, while the right cosets are: $H = \{R_0, S_0\}$, $HR_1 = \{R_1, S_3\}$, $HR_2 = \{R_2, S_2\}$, $HR_3 = \{R_3, S_1\}$.

8. $\mathbb{Z}_1$, $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_5$, $\mathbb{Z}_6$; S_3 is a non-abelian group of order 6.

9 (iii) Look to the dihedral group.

10. $\mathbb{Z}_2 \times \mathbb{Z}_2$ is the union of the three subgroups $\{(0,0),(0,1)\} \cup \{(0,0),(1,0)\} \cup \{(0,0),(1,1)\}$.

Problem Set 6

See solutions

Problem Set 7

See solutions

Problem Set 8

2 (i)

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

in invariant factor form these two groups have respective representations:

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

(ii)

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

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

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

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

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

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

(iii)

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

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

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

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

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

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

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

5. $Z(Q) = \{\pm 1)$ $(ZD) = \{R_0, R_2\}$ $Z(Q) \approx \mathbb{Z}_2 \approx Z(D)$ $Q/Z(Q) \approx \mathbb{Z}_2 \times \mathbb{Z}_2 \approx D/(ZD)$. $Q \approx D$, but the set of self-inverse elements of D numbers six: $\{R_0, R_2, S_0, S_1, S_2, S_3\}$ while there for Q, the self-inverse elements are just ± 1; $\therefore Q \not\approx D$. 10 (ii) $\mathbb{Z}_3 \times \mathbb{Z}_3$ and $\mathbb{Z}_9$.

Problem Set 9

4. $(1\,4\,6\,3\,5)(2\,8)$. 5. $(1\,2\,3\,4)$. 6. $(1\,2)(1\,3)\cdots(1\,n)$. 7 & 8. $(2\,3\,4\,8\,6)$.
8. $(1\,4\,2)$.
4. $(1\,4\,6\,3\,5)(2\,8)$. 5. $(1\,2\,3\,4)$. 6. $(1\,2\cdots n) = (1\,2)(1\,3)\cdots(1\,n)$. 7. $(2\,3\,4\,8\,6)$. 9. $\sigma = (1\,4\,2)$.

Problem Set 10

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