MA3343: GROUP THEORY
SEMESTER 1 2019-20
PARTIAL SOLUTIONS TO PROBLEM SHEET 1

1. Determine whether each of the following sets is a group. If your answer is that the object *is* a group, it is sufficient to just say so. If not you should give a reason why not.

   (a) The examples in parts (a) and (e) *are* groups.

   (b) This is not a group, it is not closed under composition.

   (c) This is not a group, because the inverse of a 2×2 matrix with integer entries and non-zero determinant need not have integer entries. A "perfect" answer to this question would include this remark and an example, like $\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$, of an invertible 2×2 matrix with integer entries whose inverse does not have integer entries.

   (d) No - the set of symmetric matrices is not closed under matrix multiplication. For example

$$\begin{pmatrix} 1 & 2 \\ 2 & 0 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 7 & 5 \\ 2 & 1 \end{pmatrix}$$

2. Give an example of

   (a) an infinite non-abelian group: $GL(2, \mathbb{R})$, the group of all 2×2 matrices with real entries and with non-zero determinant, under matrix multiplication.

   (b) an infinite abelian group: $\mathbb{Z}$ under addition.

   (c) An abelian group with exactly 10 elements: the group of rotational symmetries of a regular decagon.

   (d) A non-abelian group with exactly 10 elements: D_{10}, the group of symmetries of a regular pentagon.

   (e) a group with four elements, in which every element is equal to its own inverse: the group of symmetries of a (non-square) rectangle.

   (f) a group with four elements, in which every element is equal to its own inverse: the group of rotational symmetries of a square.

3. Suppose that G is a finite group of even order. Show that G must contain a non-identity element a for which $a^2 = \mathrm{id}_G$.

   An element a satisfies $a^2 = \mathrm{id}_G$ if and only if a is its own inverse. Let T be the subset of G consisting of all elements that are not equal to their own inverse. Then elements of T are naturally organised into pairs (each with its inverse) so the number of them is even. Since $|G|$ is even, it follows that the number of elements of G that don't belong to T is even too. There is at least one such element, namely the identity, so there must be at least one more, which is a non-identity element that is equal to its own inverse.

4. Give an example of

   (a) a binary operation on $\mathbb{Z}$ that is both associative and commutative;
   Addition.

   (b) a binary operation on $\mathbb{Z}$ that neither associative nor commutative;
   Subtraction.

   (c) a binary operation on $\mathbb{Z}$ that is associative but not commutative;
   $\square$, defined by $x \square y = y$.

(d) a binary operation on $\mathbb{Z}$ that is commutative but not associative;
$\star$, defined by $x \star y = |x - y|$.

5. A binary operation $\star$ is defined on $\mathbb{Z}$ by $x \star y = |xy|$. Determine, with explanation, whether $\mathbb{Z}$ is a group under the operation $\star$.
See answer to part (d) in Q3 above.

6. (a) Write out the multiplication table for the group D_8 of symmetries of the square.

   (b) Show that D_8 contains a subgroup of order 4 in which not every element is its own inverse.
   The group consisting of the four rotations has this property.

   (c) Show that D_8 contains another subgroup of order 4 in which every element is its own inverse.
   The group consising of the reflections in the two diagonals, the rotation through 180° and the identity element has this property.

7. Let G be a group with subgroups H and K.

   (a) Show that $H \cap K$ is a subgroup of G.
   We need to show that the identity element of G belongs to $H \cap K$, that $H \cap K$ is closed under the operation in G, and that $H \cap K$ contains the inverse of each of its elements.

   - $id_G \in H$ and $id_G \in K$, so $id_G \in H \cap K$.
   - Suppose that x and y are elements of $H \cap K$. Then $xy \in H$ since H is closed under the operation in G, and $xy \in K$ since K is closed under the operation in G. So $xy \in H \cap K$.
   - Suppose $x \in H \cap K$. Then $x^{-1} \in H$ since $x \in H$, and $x^{-1} \in K$ since $x \in K$. So $x^{-1} \in H \cap K$.

   We conclude that $H \cap K$ is a subgroup of G.

   (b) Is it true that $H \cup K$ must be a subgroup of G? Give an example to support your answer.
   No - for example $5\mathbb{Z}$ (the subset of $\mathbb{Z}$ conisting of all multiples of 5) and $3\mathbb{Z}$ are subgroups of $\mathbb{Z}$, but their union is not - it is not closed under addition, for example it contains the elements 5 and 3 but not 8.

8. Let D_6 be the group of symmetries of an equilateral triangle. Show that D_6 can be generated by one rotation and one reflection, or by two reflections.

   - *One reflection and one rotation*: Choose a reflection (for example the reflection S_L in the vertical line L, and a rotation, for example the rotation R_{120} through 120°. The powers of R_{120} include all three rotations, and the other two reflections can be obtained by composing S_L with R_{120} in both orders. So by starting with just R_{120} and S_L we can obtain all six elements of D_6.
   - *Two reflections*: Start with two reflections in two different lines. By composing these we can get a rotation through 120° or 240°. The powers of this rotation include all three rotations, and we can obtain the missing reflection by composing a rotation with one of the reflections that we started with. So again we can generate all six elements from the two reflections that we start with.

9. Let D_8 be the group of symmetries of the square.

   (a) Show that D_8 can be generated by the rotation through 90° and any one of the four reflections.
   Let R_{90} denote the rotation through 90° and let T be one of the reflections. Then R_{90} already generates all four rotations, so the subgroup $\langle R_{90}, T\rangle$ contains at least 5 elements (the four rotations and T). It follows from Lagrange's Theorem that this subgroup must be D_8 since its order is at least 5 and is a divisor of 8.
   If you don't want to use Lagrange's Theorem, you can note that composing T with each of the four rotations gives the four reflections.

(b) Show that D_8 can be generated by two reflections.
Let T_1 be the reflection in one of the diagonals of the square, and let T_2 the reflection in one of the perpendicular bisectors of the sides. Then $T_1 \circ T_2$ is a rotation through 90° or 270°, which generates the cyclec group of all four rotations. Thus the group generated by T_1 and T_2 contains T_1 and R_{90}, hence it is the full group D_8, by part (a) above.

(c) Is it true that the group D_8 of symmetries of the square can be generated by *any* two reflections?
No: Start with the two refections in the diagonals. These generate a subgroup of D_8 of order 4.

10. Suppose that $S = \{q_1, \dots, q_r\}$ is a finite subset of $\mathbb{Q}$, and let P denote the set of prime divisors of the denominators of the q_i, when each q_i is written in a form where its numerator and denominator have no factors in common. Then every element of the subgroup $\langle S \rangle$ of $(\mathbb{Q}, +)$ generated by S can be written as a fraction whose denominators are products of elements of P. Let p be a prime that does not belong to P. Then the rational number $\frac{1}{p}$ cannot be written as a sum of fractions whose denominators are products of elements of P, so $\frac{1}{p} \neq \langle S \rangle$ and S does not generate the group $(\mathbb{Q}, +)$.
Note: Here we have used the fact that the set of prime numbers is infinite, in choosing a prime p that does not belong to P. An example of an infinite set that *does* generate the additive group of $\mathbb{Q}$ is the set of reciprocals of all prime numbers.

11. Let G be a cyclic group generated by the element x. So $G = \{x^i : i \in \mathbb{Z}\}$. Let H be a subgroup of G. If H is the trivial subgroup consisting only of the identity element x^0 of G, then H is cyclic. If H is not the trivial subgroup of G, let m be the least positive integer for which $x^m \in H$. We claim that H is the cyclic subgroup generated by x^m. Certainly $H \supseteq \langle x^m \rangle$, since H is closed under the operation of G and under taking inverses, and since $x^m \in H$. Let $y \in H$. Then $y = x^j$ for some $j \in \mathbb{Z}$, and $j = qm + r$, where r is the remainder on dividing j by m, and $0 \leqslant r < m$. Now $x^{qm}x^r \in H$ and $x^{qm} \in H$ and so $x^r \in H$. It follows that $r = 0$ since m is the least positive integer for which $x^m \in H$. Then $y = x^{qm} = (x^m)^q$ so $y \in \langle x^m \rangle$ and $H = \langle x^m \rangle$. This is what we needed to show, that H is a cyclic group.