MATH 3030, Abstract Algebra
FALL 2012
Toby Kenney
Midterm Examination
Model Solutions

Basic Questions

1. *Are the following multiplication tables groups? Justify your answers.*

(a)

	a	b	c
a	c	a	c
b	a	b	a
c	c	a	c

This is not a group, since it does not have an identity element. It is also not assiciative: for example $(ba)c = c$, but $b(ac) = a$.

(b)

	a	b	c	d	e
a	a	b	c	d	e
b	b	a	e	c	d
c	c	d	a	e	b
d	d	e	b	a	c
e	e	c	d	b	a

This is not a group — it has 5 elements, and we know the only 5 element group is cyclic, which this is not, so it is not a group. [It is not associative: for example $(bc)d = b$, but $b(cd) = d$. It does have an identity and inverses for all elements.]

(c)

	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

This is a group. It is the Klein 4 group $\mathbb{Z}_2 \times \mathbb{Z}_2$. a is the identity, and all elements are their own inverses.

2. *Which of the following are groups:*

(a) $\mathbb{N} = \{n \in \mathbb{Z} | n \geqslant 0\}$ *with the operation $a * b$ given by addition without carrying, that is, write a and b (in decimal, including any leading zeros necessary) and in each position add the numbers modulo 10, so for example* $2456 * 824 = 2270$.

This is a group. 0 is the identity element. It is clear that adding two digits modulo 10 gives another well-defined digit, so the operation is well defined, and since modular arithmetic is associative, so is $*$. Finally, each digit n has an additive inverse modulo 10, given by $10-n$ and taking the additive inverse of each digit gives the inverse of the whole number, so that for example, the inverse of 2439 is 8671.

(b) The set of functions $f:\mathbb{R}\to\mathbb{R}$ such that $f(1)=0$ with pointwise addition (i. e. $(f+g)(x)=f(x)+g(x)$).

This is a group. Pointwise addition is well-defined on this set, and is clearly associative. The constantly zero function is the identity, and the inverse function of f is g given by $g(x)=-f(x)$.

(c) The set of real numbers with the operation $x*y=\frac{xy}{x+y}$.

This operation is not well defined — if $x+y=0$, then $x*y$ is not defined.

3. *How many generators are there in the cyclic group $\mathbb{Z}_{28}$?*

Generators of this group are numbers that are coprime to 28. That is, the generators are $\{1,3,5,9,11,13,15,17,19,23,25,27\}$, so there are 12 generators.

4. *Which of the following are subgroups of $\mathbb{Z}\times\mathbb{Z}$?*

(a) The set of all pairs (a,b) where a is divisible by 6.

This is a subgroup. If we add two elements $(a_1,b_1)+(a_2,b_2)$ we get (a_1+a_2,b_1+b_2), and since a_1 and a_2 are both divisible by 6, so is a_1+a_2. 0 is divisible by 6. If a is divisible by 6, then so is $-a$, so this set is closed under inverses. Therefore, it is a subgroup.

(b) The set of all pairs (a,b) such that $a+3b=0$.

This is a subgroup. If we add two elements $(a_1,b_1)+(a_2,b_2)$ we get (a_1+a_2,b_1+b_2), and $a_1+a_2+3(b_1+b_2)=a_1+3b_1+a_2+3b_2=0$. Similarly, $-a+3(-b)=-(a+3b)=0$, and $0+3\times 0=0$.

(c) The set of all pairs (a,b) such that $2a+b=2$.

This is not a subgroup because it does not contain 0. Also it is not closed under addition.

(d) The set of all pairs (a,b) such that $5a+2b$ is divisible by 4.

This is a subgroup. If we add two elements $(a_1,b_1)+(a_2,b_2)$ we get (a_1+a_2,b_1+b_2), and $5(a_1+a_2)+2(b_1+b_2)=5a_1+2b_1+5a_2+2b_2$ is divisible by 4. Similarly, $5(-a)+2(-b)=-(5a+2b)$ is divisible by 4, and $5\times 0+2\times 0=0$ is divisible by 4.

(e) The set of all pairs (a,b) such that a^2+b^2 is a square number (i.e. $a^2+b^2=c^2$ for some $c\in\mathbb{Z}$.)

This is not a subgroup because it is not closed. For example it contains $(3,4)$ and $(4,3)$ but not $(3,4)+(4,3)=(7,7)$.

(f) The set of all pairs (a,b) such that $a\geqslant b$.

This is not a subgroup because it is not closed under inverses. For example it contains $(3,1)$ but not $(-3,-1)$.

5. *Which of the following are subgroups of the group of permutations of the 6 element set* $\{1, 2, 3, 4, 5, 6\}$*?*

   (a) The set of permutations σ *such that* $\sigma(1) + \sigma(4) + \sigma(5) = 10$.

   This is not a subgroup, since it contains $(12)(364)$ but not its square: (463).

   (b) The set of permutations σ *that either fix the set of odd numbers of send it to the set of even numbers. That is: either* $\sigma(\{1, 3, 5\}) = \{1, 3, 5\}$ *or* $\sigma(\{1, 3, 5\}) = \{2, 4, 6\}$.

   This is a subgroup. The identity element fixes the set of odd numbers. If a permutation fixes $\{1, 3, 5\}$ then so does its inverse. If a permutation sends $\{1, 3, 5\}$ to $\{2, 4, 6\}$ then so does its inverse. Finally we can see that this subset is closed under composition by considering 4 cases.

6. *(a) Describe the subgroup of* $\mathbb{Z} \times \mathbb{Z}_{12}$ *generated by* $(2, 8)$.

   This group is cyclic, and it is clearly infinite, so it must be isomorphic to $\mathbb{Z}$.

   (b) Describe the subgroup of $\mathbb{Z} \times \mathbb{Z}_{12}$ *generated by* $(2, 8)$ *and* $(3, 4)$.

   This subgroup clearly also contains $(2, 8) + (2, 8) - (3, 4) = (1, 0)$ and $(3, 4) - (1, 0) - (1, 0) - (1, 0) = (0, 4)$. Meanwhile it is clear that $(1, 0)$ and $(0, 4)$ generate the subgroup, so this subgroup is isomorphic to $\mathbb{Z} \times \mathbb{Z}_3$.

7. *(a) Write* $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 5 & 4 & 9 & 7 & 6 & 8 & 1 & 3 \end{pmatrix}$ *as a product of disjoint cycles.*

   $\sigma = (12578)(394)$.

   (b) What is the order of σ*?*

   The order of σ is the least common multiple of its cycle lengths, which is 15.

   (c) Is σ *odd or even?*

   Sigma is a product of a 5-cycle (which is a product of 4 transpositions) and a 3-cycle (which is a product of 2 transpositions), so it is even.

   Alternatively, σ^{15} is the identity, which is even, and an odd permutation to an odd power must be odd, so σ must be even.

   (d) Which of the following permutations are conjugate to σ *in* S_9*?*

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

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

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

A permutation is conjugate to σ if and only if it is of the same cycle type. The above permutations have the following representations as products of disjoint cycles:

(i) $(12586)(394)$

(ii) $(15)(3749)(68)$

(iii) $(14)(23)(789)$

so only (i) is conjugate to σ.

8. *Draw the Cayley graph of* A_4 *with generators* (123) *and* (234).

9. *Which of the following subgroups are normal?*

   (a) The subgroup of the group of symmetries of a hexagon generated by a $120°$ *rotation.*

   This is normal. Conjugating a $120°$ rotation by any symmetry of the hexagon gives either a $120°$ rotation or a $240°$ rotation.

   (b) The subgroup of the group of symmetries of a hexagon generated by a $180°$ *rotation.*

   This is normal. A $180°$ rotation is central (commutes with all symmetries of the hexagon).

   (c) The subgroup of the additive group of real numbers generated by the numbers whose square is rational.

   The additive group of real numbers is abelian, so any subgroup is normal.

   (d) The subgroup of the multiplicative group of all invertible 3×3 *matrices with real coefficients consisting of matrices with rational determinant.*

   The determinant is a homomorphism from the multiplicative group of invertible 3×3 matrices to the multiplicative group of non-zero real numbers. The rational numbers are a normal subgroup of the real numbers, so their inverse image under this homomorphism is a normal subgroup of the multiplicative group of invertible 3×3 matrices.

   This subgroup is the group of permutations that fix the set $\{1, 2\}$. This is not normal, since conjugation by (13) for example does not fix this group.

10. *Find the index of* $\langle (1, 4), (5, 7) \rangle$ *in* $\mathbb{Z} \times \mathbb{Z}$.

    The cosets of $\langle (1, 4), (5, 7) \rangle$ in $\mathbb{Z} \times \mathbb{Z}$ are represented by $(0, 0)$, $(1, 2)$, $(1, 3)$, $(2, 3)$, $(2, 4)$, $(2, 5)$, $(3, 5)$, $(3, 6)$, $(4, 6)$, $(4, 7)$, $(4, 8)$, $(5, 8)$ and $(5, 9)$, so the index is 13.

11. *Is there a transitive permutation group on 4 elements in which every element has order less than 4?*

    Yes, the subgroup $\{e, (12)(34), (13)(24), (14)(23)\}$ of S_4 is transitive, but all elements have order 2 or 1.

12. *Which of the following functions are homomorphisms.*

(a) $f : S_6 \to S_3$ given by $f(\sigma)(1) = \sigma(1) + \sigma(4)(\pmod 3)$) $f(\sigma)(2) = \sigma(2) + \sigma(5)(\pmod 3)$) $f(\sigma)(3) = \sigma(3) + \sigma(6)(\pmod 3)$)

This is not a well defined function. For example, if $\sigma = (46)$, then we have $f(\sigma)(1) = f(\sigma)(2) = f(\sigma)(3) = 1$, so $f(\sigma)$ is not a permutation.

(b) $f : D_6 \to D_3$ given by $f(x) = x$ if x preserves the triangles formed by alternating vertices of the hexagon, and $f(x)$ is x followed by a $180°$ rotation otherwise.

This is a homomorphism. If x and y preserve the triangles, then $f(x)f(y) = xy = f(xy)$; if one of x and y preserves the triangles then $f(x)f(y)$ is xy followed by a $180°$ rotation, since $180°$ rotation commutes with all elements of D_6; if neither x nor y preserves the triangles, then $f(x)f(y) = xy = f(xy)$.

13. *(a) Calculate the commutator subgroup of $\mathbb{Z} \times S_3$.*

Given elements (a, x) and (b, y) of $\mathbb{Z}\times S_3$, their commutator is $(aba^{-1}b^{-1}, xyx^{-1}y^{-1}) = (0, xyx^{-1}y^{-1})$. The commutator subgroup of S_3 is A_3, so the commutator subgroup of $\mathbb{Z} \times S_3$ is $\{(0, x)|x$ is an even permutation$\}$.

(b) Calculate the factor group of $\mathbb{Z} \times S_3$ over its commutator subgroup.

The factor group of S_3 over A_3 is $\mathbb{Z}_2$, so the factor group of $\mathbb{Z} \times S_3$ over its commutator subgroup is $\mathbb{Z} \times \mathbb{Z}_2$.

14. *Calculate the centre of $S_3 \times \mathbb{Z}_6$.*

Elements (a, x) and (b, y) of $S_3 \times \mathbb{Z}_6$ commute if and only if a and b commute and x and y commute, so the centre of $S_3 \times \mathbb{Z}_6$ consists of pairs of the form (x, y) where x is in the centre of S_3 and y is in the centre of $\mathbb{Z}_6$. The centre of S_3 is trivial, and $\mathbb{Z}_6$ is abelian, so is its own centre. Therefore the centre of $S_3 \times \mathbb{Z}_6$ is the set of elements (e, x) for $x \in \mathbb{Z}_6$.

Theoretical Questions

15. *Prove that the intersection of two subgroups of a group is another subgroup.*

Let H and K be subgroups of a group G. We want to show that $H \cap K$ is a subgroup of G.

- If $x, y \in H \cap K$, then $x, y \in H$, so $xy \in H$ since H is a subgroup, and also $x, y \in K$, so $xy \in K$ since K is a subgroup. Therefore, $xy \in H \cap K$.
- We have $e \in H$ and $e \in K$, so $e \in H \cap K$.
- If $x \in H \cap K$, then $x^{-1} \in H$ and $x^{-1} \in K$, so $x^{-1} \in H \cap K$.

16. *Show that any finite group of even order has an element of order 2. [Hint: Suppose all non-identity elements have order at least 3. Now partition the group into a collection of disjoint pairs and the identity element.]*

    Let G have even order. We can partition the non-identity elements of G into subsets of the form $\{x, x^{-1}\}$. Since there are an odd number of non-identity elements, one of these partitions must have an odd number of elements, but this only happens if $x = x^{-1}$, i.e. when x is of order 2.

17. *Let G be a permutation group on a finite set with orbits of sizes $a_1, \ldots, a_m$. Show that $|G|$ is at least the lowest common multiple of $a_1, \ldots, a_m$.*

    Recall the orbit stabiliser theorem that the size of the orbit of any element under a permutation group divides the order of the group. That is $a_1, \ldots, a_n$ all divide $|G|$, so $|G|$ is divisible by their lowest common multiple, and therefore must be at least their lowest common multiple.

18. *State and prove Lagrange's theorem about the order of a subgroup of a finite group.*

    Theorem 1 (Lagrange)**.** *If G is a finite group, and H is a subgroup of G, then $|H|$ divides $|G|$.*

    Proof. Consider the cosets xH for elements $x \in G$. These form a partition of G. Each of them has $|H|$ elements, and G is the disjoint union of these cosets, so $|G|$ is a sum of copies of $|H|$, so it is divisible by $|H|$. $\square$

19. *Show that for subgroups $H \leqslant K \leqslant G$, if $(G : K)$ and $(K : H)$ are finite, then $(G : H) = (G : K)(K : H)$.*

    Consider the left cosets of K. We have that K is a disjoint union of $(K : H)$ left cosets of H, so any left coset of K is a disjoint union of $(K : H)$ left cosets of H. (Let the cosets of H in K be $x_1H, x_2H, \ldots, x_mH$ where $m = (K : H)$; then the cosets of H in aK are $ax_1H, ax_2H, \ldots, ax_mH$.) Now since G is a disjoint union of $(G : K)$ cosets of K, each of which is a disjoint union of $(K : H)$ cosets of H, we have that G is a disjoint union of $(G : K)(K : H)$ cosets of H. Therefore $(G : H) = (G : K)(K : H)$.

20. *Let H be a subgroup of G. Show that $N_G(H) = \{x \in G | xHx^{-1} = H\}$ is the largest subgroup of G which contains H as a normal subgroup.*

    We first need to show that $N_G(H)$ is a subgroup.

    - Let $x, y \in N_G(H)$. Now $xyH(xy)^{-1} = xyHy^{-1}x^{-1} = xHx^{-1} = H$, so $xy \in N_G(H)$.
    - Let $x \in N_G(H)$. Then $xHx^{-1} = H$, so $xH = Hx$ and so $H = x^{-1}Hx$. Therefore $x^{-1} \in N_G(H)$.
    - Clearly $e \in N_G(H)$.

Next we need to show that H is a normal subgroup of $N_G(H)$, but this is automatic by the definition of $N_G(H)$. Finally, we need to show that if $K \leqslant G$ contains H as a normal subgroup, then $K \leqslant N_G(H)$. Let $x \in K$. Since H is a normal subgroup of K, we have $xHx^{-1} = H$, so $x \in N_G(H)$.

21. *Show that the composite of two group homomorphisms is another group homomorphism.*

    Let $G \xrightarrow{f} H$ and $H \xrightarrow{g} K$ be homomorphisms. We want to show that $G \xrightarrow{gf} K$ is also a homomorphism. We have that $gf(xy) = g(f(xy)) = g(f(x)(f(y)) = g(f(x))g(f(y)) = gf(x)gf(y)$ as required.

22. *Let $H \leqslant G$. Show that the commutator subgroup of H is a subgroup of the commutator subgroup of G, and that the centre $Z(H)$ contains $Z(G) \cap H$.*

    Let C be the commutator subgroup of G. It clearly contains the commutator subgroup of H because the commutator subgroup of H is generated by the commutators $aba^{-1}b^{-1}$ for $a, b \in H$, but then $a, b \in G$, so $aba^{-1}b^{-1} \in C$.

    Let $x \in Z(G) \cap H$. Then x commutes with any element of G. In particular it commutes with any element of H, so $x \in Z(H)$.