Answers to Final Exam

MA441: Algebraic Structures I

20 December 2003

1) Definitions (20 points)

1. Given a subgroup $H \lhd G$, define the quotient group G/H. (Describe the set and the group operation.)

   The quotient group is the set of left (or right) cosets $\{aH | a \in G\}$ with group operation $(aH)(bH) = (ab)H$.

2. Given a permutation group $G < S_n$ acting on the set $\{1, 2, \ldots, n\}$, define the stabilizer $\mathrm{Stab}_G(i)$.

   $\mathrm{Stab}_G(i) = \{\phi \in G | \phi(i) = i\}$

3. Given an element $a \in G$, define the centralizer $C(a)$.

   $C(a) = \{g \in G | ag = ga\}$

4. Given $a \in G$, define the conjugacy class $\mathrm{cl}(a)$.

   $\mathrm{cl}(a) = \{gag^{-1} | g \in G\}$

2) Fill in the blanks or answer True/False (five from this list)

1. True or False: $(1234)(4567) \in A_7$. True

   A 4-cycle is odd (a product of three 2-cycles), and two odds make an even.

2. True or False: $\langle(14)\rangle$ is a normal subgroup of S_4. False

   For example, $(12)(14)(12) = (1)(24)$, which is not contained in $\langle(14)\rangle$.

3. True or False: If 7 divides $|G|$, then G has an element of order 7. True

   This follows from Cauchy's Theorem.

4. True or False: For every positive integer n, $\text{Aut}(\mathbb{Z}_n) \approx U(n)$. True

   This is Theorem 6.5.

5. True or False: Let G be a cyclic group of order n. If $k|n$, then there is an $H < G$ such that H has order k. True

   This follows from the Fundamental Theorem of Cyclic Groups (Theorem 4.3).

3) Let H be a nonempty finite subset of a group G. Prove that H is a subgroup of G if H is closed under the operation of G.

This is Theorem 3.3, the Finite Subgroup Test. One need only prove that any element $a \in H$ has an inverse. If $a = e$, then a is its own inverse. Assume $a \neq e$. Consider $\langle a \rangle$. Since H is finite, by the Pigeonhole Principle, there are i, j such that $a^i = a^j$. We may assume that $0 < i < j$. Then $a^{j-i} = e$ and $a \cdot a^{j-i-1} = e$. Since $a \neq e$, $j - i - 1 > 0$. Therefore $a^{-1} = a^{j-i-1}$.

4) Use Lagrange's Theorem to prove Fermat's Little Theorem: for every integer a and every prime p, $a^p \equiv a \pmod{p}$.

This is Corollary 5 to Lagrange's Theorem, Theorem 7.1. Apply Lagrange's Theorem to $U(p)$, which has order $p-1$. Because $a^{p-1} \equiv 1 \pmod{p}$, we multiply both sides by a to get $a^p \equiv a \pmod{p}$.

5) Cosets

1. Given a subgroup $H < G$ and any $a, b \in G$, prove that either $aH = bH$ or $aH \cap bH = \emptyset$, i.e., aH and bH are disjoint.

   This is from the Lemma on page 135 of Chapter 7.

   Suppose x is in both aH and bH. Then we can write $x = ah_1 = bh_2$ for some $h_1, h_2 \in H$. Therefore $a = bh_2h_1^{-1}$ and $b = ah_1h_2^{-1}$. So $aH = bh_2h_1^{-1}H \subseteq bH$ and conversely $bH = ah_1h_2^{-1}H \subseteq aH$. Therefore $aH = bH$.

   Alternatively, one could cite the property that $aH = H$ iff $a \in H$. Then $aH = b(h_2h_1^{-1}H) = bH$, since $h_2h_1^{-1}H = H$.

2. Given a subgroup $H < G$ and any $a \in G$, prove that $aH < G$ iff $a \in H$.

   If $a \in H$, then by the first part, $aH = H$ ($a \in aH \cap H$) so $aH < G$. If $aH < G$, then $e \in aH$. Since $e \in H$, $aH = H$. Alternatively, since $e \in aH$, we can write $e = aa^{-1}$. Since $a^{-1} \in H, a \in H$.

6) Homomorphisms. Let $\phi : G_1 \to G_2$ be a homomorphism, and let $H < G_1$.

1. Prove that $\phi(H)$ is a subgroup of G_2.

   This is Theorem 10.2, part 1.

2. Prove that if $H \lhd G_1$ then $\phi(H) \lhd \phi(G_1)$.

   This is Theorem 10.2, part 4.

7) First Isomorphism Theorem. Let $\phi : G \to H$ be a homomorphism of groups and let $K = \operatorname{Ker} \phi$. Let $\psi : G/K \to H$ be the correspondence that sends $gK \mapsto \phi(g)$.

1. Prove that if $K = \{e\}$, then ϕ is one-to-one.

   This follows from Theorem 10.2, part 5. Alternatively, you can argue directly that if $\phi(x) = \phi(y)$, then $\phi(xy^{-1}) = e$, so $xy^{-1} \in K$. Since K is assumed to be trivial, $xy^{-1} = e$ and $x = y$.

2. Show that ψ is well-defined. Prove that for any $x, y \in G$ such that $xK = yK$, we have $\psi(xK) = \psi(yK)$.

   This is part of Theorem 10.3, the First Isomorphism Theorem. If $\psi(xK) = \psi(yK)$, then $\phi(x) = \phi(y)$, by the definition of ψ. Following the argument in the previous part, $xy^{-1} \in K$, so $xK = yK$.

8) Euclidean Algorithm

1. Use the Euclidean Algorithm to express $\gcd(13, 28)$ as an integer linear combination of 13 and 28. Show all work.

2. Find the inverse of 13 in $U(28)$.

We calculate

$$\begin{aligned} 28 &= 2 \cdot 13 + 2 \\ 13 &= 6 \cdot 2 + 1 \\ 1 &= 13 - 6 \cdot 2 \\ 2 &= 28 - 2 \cdot 13 \\ 1 &= 13 - 6(28 - 2 \cdot 13) \\ &= 13 \cdot 13 - 6 \cdot 28. \end{aligned}$$

Reducing the last equation modulo 28, we see that 13 is its own inverse in $U(28)$.

9) Prove that if $|a| = k$, then $\langle a \rangle = \{e, a, a^2, \ldots, a^{k-1}\}$.

This is Theorem 4.1. Note that $\langle a \rangle = \{a^n | n \in \mathbb{Z}\}$. The key idea here is to apply the Division Algorithm. For any n, we can divide by k and take the remainder to get $n = q \cdot k + r$, where $0 \leq r < k$. Then $a^n = a^r$. (For $n < 0$, the q will be negative, and this still works.)

10) Let G be the group $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ under addition, and let H be the group

$$H = \left\{ \left[\begin{array}{cc} a & 2b \\ b & a \end{array} \right] \;\middle|\; a, b \in \mathbb{Q} \right\}$$

under addition.

Show that G and H are isomorphic under addition.

This was problem 6.24 in Homework Assignment 9.

Let ϕ be the map such that

$$\phi(a + b\sqrt{2}) = \begin{pmatrix} a & 2b \\ b & a \end{pmatrix}.$$

The map ϕ is one-to-one because if $\phi(a + b\sqrt{2}) = \phi(c + d\sqrt{2})$, then

$$\begin{pmatrix} a & 2b \\ b & a \end{pmatrix} = \begin{pmatrix} c & 2d \\ d & c \end{pmatrix},$$

then the corresponding entries are equal, so $a = c$ and $b = d$.

The map ϕ is onto because for any a, b, the definition of ϕ above means $a + b\sqrt{2}$ is a preimage for

$$\begin{pmatrix} a & 2b \\ b & a \end{pmatrix}$$

under ϕ.

To show the homomorphism property, observe that

$$\begin{pmatrix} a & 2b \\ b & a \end{pmatrix} + \begin{pmatrix} c & 2d \\ d & c \end{pmatrix} = \begin{pmatrix} a+c & 2(b+d) \\ b+d & a+c \end{pmatrix},$$

So therefore

$$\phi((a+b\sqrt{2})+(c+d\sqrt{2})) = \phi((a+c)+(b+d)\sqrt{2}) = \phi(a+b\sqrt{2})+\phi(c+d\sqrt{2}).$$

11) Suppose that $|x| = n$. Find a necessary and sufficient condition on r and s such that $\langle x^r \rangle \subseteq \langle x^s \rangle$. Justify your answer.

This was problem 4.60 in Homework Assignment 7.

The proof we followed in the homework was to apply Theorem 4.2 to get

$$\langle x^r \rangle = \langle x^{\gcd(r,n)} \rangle, \ \langle x^s \rangle = \langle x^{\gcd(s,n)} \rangle,$$

and then deduce the divisibility condition $\gcd(s,n)$ divides $\gcd(r,n)$.

Alternatively, one could argue that by the Fundamental Theorem of Cyclic Groups, $\langle x^r \rangle \subseteq \langle x^s \rangle$ iff $|\langle x^r \rangle|$ divides $|\langle x^s \rangle|$. Since $\langle x^s \rangle$ is a cyclic group, there is exactly one subgroup for each order dividing $|\langle x^s \rangle|$.

12) (for 10 points of extra credit) Prove Lagrange's Theorem. You may cite basic properties of cosets, such as those listed in Gallian's Lemma in Chapter 7, if you state them accurately.

Please refer to the proof on page 137 of Gallian. It suffices to note that G can be partitioned by its cosets, that all cosets have the same size, and that therefore the order of G is an even multiple of the order of a coset.