Name:

Abstract Algebra (Math 3063)
Midterm Exam I - Solutions

Professor Paul Bailey
Friday, April 3, 2009

Problem 1. Let $a, b, c \in \mathbb{Z}$. Show that if $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.

Solution. Since $a \mid bc$, we have
$$ak = bc \text{ for some } k \in \mathbb{Z}.$$
Since $\gcd(a, b) = 1$, we have
$$ax + by = 1 \text{ for some } x, y \in \mathbb{Z}.$$
Multiplying by c gives
$$acx + bcy = c.$$
Plugging the first equation into this gives
$$acx + aky = a(cx + ky) = c.$$
Thus $a \mid c$. □

Problem 2. Let $n = 401$ and $a = 202$.

(a) Show that $\overline{a} \in \mathbb{Z}_n^*$.

(b) Find the inverse of $\overline{a}$ in $\mathbb{Z}_n^*$.

Solution. Perform the first half of the Euclidean algorithm to first
$$\begin{aligned}401 &= 202(1) + 199\\ 202 &= 199(1) + 3\\ 199 &= 3(66) + 1\end{aligned}$$
Thus $\gcd(401, 202) = 1$, so $\overline{202} \in \mathbb{Z}_{401}^*$.

The second half the the Euclidean algorithm tells us that
$$\begin{aligned}1 &= 199 + 3(-66)\\ &= 199 + [202 - 199](-66)\\ &= 199(67) + 202(-66)\\ &= [401 - 202](67) + 202(-66)\\ &= 401(-67) + 202(-133).\end{aligned}$$
Thus $\overline{1} = \overline{202} \cdot \overline{-133}$ in $\mathbb{Z}_{401}$, and $\overline{202}^{-1} = \overline{-133} = \overline{268}$. □

Problem 3. Consider the five-cycles in S_5.

(a) How many five-cycles are in S_5? In A_5?

(b) How many distinct cyclic subgroups of order five are in A_5?

Solution. Each five cycle in S_5 may be written in cycle notation with 1 in the first position, and is thenceforth completely determined by the numbers in the next four positions, which are free to be any number from 2 to 5. There are 4! arrangements of these numbers, so there are $4! = 24$ five-cycles in S_5. Since five-cycles have odd length, they are even permutations, and all are in A_5.

Each cyclic subgroup of order five has a unique element which sends 1 to 2, and then is completely determined by the final three positions; there are 3! ways to arrange the the last three numbers (which must be 3, 4, or 5), so there are $3! = 6$ cyclic subgroups of order five.

Alternatively, we may note that any two distinct subgroups of order 5 intersect trivially (by LaGrange's Theorem), and each such subgroup contains four five-cycles, so the number of subgroups is 24 five-cycles divided by 4 five-cycles per subgroup; that is, $24/4 = 6$. □

Problem 4.
Let G be an abelian group. The *torsion subgroup* of G is

$$T(G) = \{g \in G \mid g^n = 1 \text{ for some } n \in \mathbb{Z}\}.$$

(a) Show the $T(G)$ is a normal subgroup of G.

(b) Show that every nontrivial element of $G/T(G)$ has infinite order.

(c) Define $\phi : \mathbb{R} \to \mathbb{C}^*$ by $\phi(x) = \operatorname{cis} 2\pi x$. Then ϕ is a homomorphism. Find $\phi^{-1}(T(G))$.

Solution. First, to show that $T(G) \leq G$, we verify the three properties of a subgroup.

(S0) Since $1^1 = 1$, we see that $1 \in T(G)$.

(S1) Let $x, y \in T(G)$. Then $x^m = 1$ and $y^n = 1$ for some $m, n \in T(G)$. Thus

$$\begin{aligned} (xy)^{mn} &= x^{mn} y^{mn} \qquad \text{because } G \text{ is abelian} \\ &= (x^m)^n (y^n)^m \\ &= 1^n \cdot 1^m \\ &= 1 \end{aligned}$$

Thus $xy \in T(G)$.

(S2) Let $x \in T(G)$. Then $x^n = 1$ for some $n \in \mathbb{Z}$.

$$(x^{-1})^n = x^n \cdot (x^{-1})^n = (xx^{-1})^n = 1^n = 1;$$

thus $x^{-1} \in T(G)$.

Next, we note that every subgroup of G is normal in G because G is abelian; thus $T(G) \triangleleft G$.

Now let $\overline{g} \in G/T(G)$; where $\overline{g} = gT(G)$. Suppose $\overline{g}$ has finite order; then $\overline{g}^m = \overline{1}$ for some $m \in \mathbb{Z}$. Thus $\overline{g^m} = \overline{1} = T(G)$, so $g^m \in T(G)$. Thus $(g^m)^n = 1$ for some $n \in \mathbb{Z}$, so $g^{mn} = 1$, so $g \in T(G)$; therefore $\overline{g} = \overline{1}$, so $\overline{g}$ is trivial (i.e., is the identity).

Finally, note that $\operatorname{cis}(2\pi x) = 1 \in \mathbb{C}^*$ if and only if $x \in \mathbb{Z}$. Now by DeMoivre's theorem, $\operatorname{cis}(\theta)^n = \operatorname{cis}(n\theta)$, so

$$\begin{aligned} \operatorname{cis}(2\pi x) \text{ has finite order } &\Leftrightarrow \operatorname{cis}(2\pi x)^n = \operatorname{cis}(2\pi n x) = 1 \text{ for some } n \in \mathbb{Z} \\ &\Leftrightarrow nx \in \mathbb{Z} \text{ for some } n \in \mathbb{Z} \\ &\Leftrightarrow x \in \mathbb{Q} \end{aligned}$$

Thus, $\phi^{-1}(T(G)) = \mathbb{Q}$.

Let $\mathbb{U} = \{z \in \mathbb{C} \mid |z| = 1\}$ denote the unit circle in $\mathbb{C}$. Then $\phi(\mathbb{R}) = \mathbb{U}$, and when we compose ϕ with the canonical homomorphism $\beta : \mathbb{U} \to \mathbb{U}/T(\mathbb{U})$, we note that $\ker(\beta \circ \phi) = \phi^{-1}(\ker(\beta)) = \phi^{-1}(T(\mathbb{U})) = \mathbb{Q}$, and by the Isomorphism Theorem we obtain $\mathbb{R}/\mathbb{Q} \cong \mathbb{U}/T(\mathbb{U})$. □

Problem 5. Let G be a group and let $a, b \in G$. The *commutator* of a and b is

$$[a, b] = a^{-1}b^{-1}ab.$$

(a) Let $\phi : G \to H$ be a group homomorphism and let $a, b \in G$.
Show that $\phi(a)$ and $\phi(b)$ commute if and only if $[a, b] \in \ker(\phi)$.

(b) Let $K \triangleleft G$ such that $[a, b] \in K$ for every $a, b \in G$. Show that G/K is abelian.

Solution. We have

$$\begin{aligned}
\phi(a), \phi(b) \text{ commute} &\Leftrightarrow \phi(b)\phi(a) = \phi(a)\phi(b) \\
&\Leftrightarrow \phi(a)^{-1}\phi(b)^{-1}\phi(a)\phi(b) = 1 \\
&\Leftrightarrow \phi(a^{-1})\phi(b^{-1})\phi(a)\phi(b) = 1 \\
&\Leftrightarrow \phi(a^{-1}b^{-1}ab) = 1 \\
&\Leftrightarrow a^{-1}b^{-1}ab \in \ker(\phi) \\
&\Leftrightarrow [a, b] \in \ker(\phi).
\end{aligned}$$

Let $\overline{a}, \overline{b} \in G/K$, where $\overline{x} = xK$. With $K \triangleleft G$, we have a canonical homomorphism $\beta : G \to G/K$, given by $\beta(x) = \overline{x}$, with kernel K. Thus

$$\overline{x}, \overline{y} \text{ commute} \Leftrightarrow \beta(x), \beta(y) \text{ commute} \Leftrightarrow [a, b] \in \ker(\beta) = K.$$

Since $\overline{a}$ and $\overline{b}$ were selected arbitrarily, G/K is abelian. $\square$