Math 301A **Sketch of Solutions for Test 2** **04/15/02**

1. (a) If G is a group of order 8740 and if H is a subgroup of G, then the following numbers are all possible as the number of cosets of H in G.

   Answer: **(IV)** $\{4, 76, 95, 1748\}$. All such numbers must divide $8740 = 2^3 \cdot 5 \cdot 19 \cdot 23$.

   (b) Consider the group S_{35} of permutations of the set $\{1, 2, \ldots, 35\}$; so S_{35} is the symmetric group on 35 letters. Write H for the subgroup of all permutations $\sigma \in S_{35}$ such that $\sigma(9) = 9$ and $\sigma(17) = 17$. Then

   Answer: **(I)** $(S_{35} : H) = 1190$. The remaining 33 letters may be permuted arbitrarily, and there are 33! such permutations. Hence, the index of H in G is $35!/33! = 34 \cdot 35 = 1190$.

   (c) Let G be a non-abelian finite group and let $\mathbb{Z}$ be the additive group of integers. Let $\phi : G \to \mathbb{Z}$ and $\psi : \mathbb{Z} \to G$ be two homomorphisms. Which of the following consists of *all* true statements?

   Answer: **(I)** ϕ is always zero and ψ is never surjective.

   Proof. We know that $\phi(1_G) = 0$, since ϕ is a homomorphism. G is finite, hence each element $a \in G$ has a finite order $o(a) > 0$. But then $0 = \phi(1_G) = \phi(a^{o(a)}) = o(a)\phi(a)$, so $\phi(a) = 0$ for any $a \in G$, so ϕ is a zero homomorphism (one that maps everything to the identity element, which is 0 in the case of $\mathbb{Z}$).

   Similarly, $\mathbb{Z}$ is abelian, so for any $a, b \in \mathbb{Z}$, we have $\psi(a)+\psi(b) = \psi(a+b) = \psi(b+a) = \psi(b)+\psi(a)$, so $\psi(\mathbb{Z})$ is an abelian subgroup of G. But G itself is non-abelian, hence $\psi(\mathbb{Z}) \neq G$. Therefore, ψ is never surjective.

2. If G is a group, and if $\sigma, \tau \in G$, we define $[\sigma, \tau] = \sigma\tau\sigma^{-1}\tau^{-1} = (\sigma\tau)(\tau\sigma)^{-1} \in G$ (we call $[\sigma, \tau]$ the *commutator* of σ and τ). Let $\Delta(G)$ denote the subgroup of G generated by all these elements $[\sigma, \tau]$ as σ and τ vary over G. Of course, $[\sigma, \tau] \in \Delta(G)$ for all $\sigma, \tau \in G$.

   (a) Prove that $\Delta(G) \lhd G$. *Hint:* First prove $h[\sigma, \tau]h^{-1} \in \Delta(G)$ for any $h, \sigma, \tau \in G$.

   Proof. Note that $\sigma\tau = [\sigma, \tau]\tau\sigma$ for any $\sigma, \tau \in G$. Then for any $\sigma, \tau, h \in G$, we have

   $$h[\sigma, \tau]h^{-1} = h\sigma\tau\sigma^{-1}\tau^{-1}h^{-1} = [h, \sigma]\sigma h\tau\sigma^{-1}\tau^{-1}h^{-1}$$
   $$= [h, \sigma]\sigma(h\tau)\sigma^{-1}(h\tau)^{-1} = [h, \sigma][\sigma, h\tau] \in \Delta(G).$$

   Since each element of $\Delta(G)$ is a product of a string of commutators of elements of G, and $(hah^{-1})(hbh^{-1}) = h(ab)h^{-1}$ for any $a, b, h \in G$, it follows that any element in $h\Delta(G)h^{-1}$ is a product of a string of elements of the form hah^{-1}, where $a \in \Delta(G)$. But we showed that all such elements are in $\Delta(G)$, hence $h\Delta(G)h^{-1} \subseteq \Delta(G)$ for any $h \in G$, so $\Delta(G) \lhd G$.

   (b) Assuming $\Delta(G) \lhd G$, write $\overline{G} = G/\Delta(G)$. Prove that $\overline{G}$ is always an abelian group.

   Denote the right coset of σ in $\overline{G}$ by $\bar{\sigma}$. Since $\sigma\tau = [\sigma, \tau]\tau\sigma$, it follows that $\Delta(G)\sigma\tau = \Delta(G)\tau\sigma$, i.e. $\bar{\sigma}\bar{\tau} = \overline{\sigma\tau} = \overline{\tau\sigma} = \bar{\tau}\bar{\sigma}$ for any $\bar{\sigma}, \bar{\tau} \in \overline{G}$. But any element of $\overline{G}$ is the form $\bar{\sigma}$ for some $\sigma \in G$. Thus, any two elements of $\overline{G}$ commute, i.e. $\overline{G}$ is abelian.

3. You are given G, a group of order 15, and it turns out that one can prove such a G must be abelian. (You may assume this.)

   (a) Without quoting Cauchy's theorem, prove directly that G possesses at least one element of order 3 and at least one element of order 5.

   Proof. We can still use Lagrange's theorem. The order of any element of G must divide 15, hence be 1, 3, 5 or 15. Only the identity has order 1, so the remaining 14 elements are or orders 3, 5

or 15. If G has an element a of order 15, then it is cyclic, a^5 is of order 3, and a^3 is of order 5. Suppose G has no element of order 15, then each non-identity element of G has order 3 or 5. Suppose the statement of the problem is false, then either all elements of G have order 3, or all elements of G have order 5. We will consider only the first case, since the second is very similar. Let $a \in G$, $a \neq e$, then $o(a) = 3$. Since G is abelian, we have $(a) \lhd G$ and $o(G/(a)) = 5$, so $G/(a)$ is cyclic of order 5. Consider the generator of $G/(a)$, it is of the form $b(a)$ for some $b \in G$. Then $b(a) \neq (a)$, i.e. $b \notin (a)$, but $(b(a))^5 = (a) \implies b^5(a) = (a) \implies b^5 \in (a)$. But $b^6 = (b^3)^2 = e^2 = e \in (a)$, so $b = b^6(b^5)^{-1} \in (a)$. Contradiction. Thus, G has an element of order 3 and an element of order 5.

(b) Assuming part (a), prove further that G is a cyclic group of order 15. *Hint:* Use elements from (a) to find an element of G of order 15.

Proof. Let $a, b \in G$ be such that $o(a) = 3$ and $o(b) = 5$. Consider the element $ab \in G$. If $(ab)^n = a^n b^n = e$, then $a^n = b^{-n}$. We have $o(a) = 3$ and $o(b) = 5$, hence $o(a^n)$ is either 1 or 3 (it must divide 3, since $(a^n)^3 = (a^3)^n = e$), and $o(b^{-n}) = o(b^n)$ is either 1 or 5 (it must divide 5, since $(b^n)^5 = (b^5)^n = e$). But $o(a^n) = o(b^{-n})$, so $o(a^n) = o(b^{-n}) = 1$, i.e. $a^n = b^{-n} = 1$. Therefore, $o(a) = 3|n$ and $o(b) = 5|n$, so $15|n$, hence $15|o(ab)$. But $(ab)^{15} = a^{15}b^{15} = (a^3)^5(b^5)^3 = e$, so $o(ab)|15$, and hence $o(ab) = 15$. Thus, ab generates all elements of G, so G is cyclic of order 15.

4. Let $\phi : G \to G_1$ and $\psi : G \to G_2$ be two different homomorphisms. Suppose the *only* element of $x \in G$ for which $\phi(x) = 1_{G_1}$ and $\psi(x) = 1_{G_2}$ is $x = 1_G$. Prove: If $y \in \ker \phi$ and $z \in \ker \psi$, then $yz = zy$.

Proof. Consider the element $yzy^{-1}z^{-1} \in G$. We have

$$\phi(yzy^{-1}z^{-1}) = \phi(y)\phi(z)\phi(y^{-1})\phi(z^{-1}) = \phi(y)\phi(z)\phi(y)^{-1}\phi(z)^{-1}$$
$$= 1_{G_1}\phi(z)1_{G_1}\phi(z)^{-1} = \phi(z)\phi(z)^{-1} = 1_{G_1}$$

and, similarly, $\psi(yzy^{-1}z^{-1}) = 1_{G_2}$, so $yzy^{-1}z^{-1} = 1_G$, i.e. $yz = zy$.

5. Let $\mathbb{F}_2$ be the set $\{0, 1\}$ with addition and multiplication defined as usual except for $1 + 1 = 0$ (i.e. $-1 = 1$). (Think of 0 as "even" and 1 as "odd" and of the facts about adding and multiplying even and odd numbers.) Let $GL(2, \mathbb{F}_2)$ be the group of 2×2 invertible matrices with coefficients in $\mathbb{F}_2$. Prove that $GL(2, \mathbb{F}_2) \simeq S_3$.

Proof. Each of the 4 entries of a matrix in $GL(2, \mathbb{F}_2)$ is either 0 or 1, hence there are $2^4 = 16$ candidates for elements of $GL(2, \mathbb{F}_2)$. Checking all those, we see that only 6 have non-zero determinant, i.e.

$$GL(2, \mathbb{F}_2) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\}.$$

Obviously, $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the identity element, hence we can find the respective orders of each of the elements above. They are: $1, 3, 3, 2, 2, 2$. To define a homomorphism $f : S_3 \to GL(2, \mathbb{F}_2)$, we only need to specify the images of the generators of S_3, then check that the multiplicative property $f(ab) = f(a)f(b)$ holds for any $a, b \in S_3$, i.e. does not contradict the group relations. S_3 is generated by ϕ and ψ satisfying $\phi^2 = e$, $\psi^3 = e$, $\phi\psi = \psi^{-1}\phi$ (or, equivalently, $\phi^2 = \psi^3 = (\phi\psi)^2 = e$). Let f be a homomorphism such that $f(\phi) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $f(\psi) = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$, then it is easy to check that f is well-defined, 1-1 and onto, hence, an isomorphism. Therefore, $GL(2, \mathbb{F}_2) \simeq S_3$.