PURDUE UNIVERSITY

Department of Mathematics

HONORS ALGEBRA

MA 45000 - SOLUTIONS

3rd October 2022 50 minutes

This paper contains **SIX** *questions.*
All SIX answers will be used for assessment.
Calculators, textbooks, notes and cribsheets are **not** *permitted in this examination.*

Do not turn over until instructed.

1. [4+4+4+4+4=20 points] Decide which of the following statements are necessarily true, and which may be false. Mark those which are true with "T", and those which are false with "F".

a. If G is a non-abelian group, then every proper subgroup of G is non-abelian.

Solution: FALSE (Let $a \in G \setminus \{e\}$. Then the subgroup $\langle a \rangle$ is an abelian, proper subgroup of G).

b. Any abelian group of order 2022 has an element of order 337.

Solution: TRUE ($2022 = 6 \times 337$ and 337 is prime – plainly not divisible by 2, 3, 5, 7, 11, and easy to check also not divisible by 13 or 17, and any other potential prime divisor is too large to be a divisor – by Cauchy's theorem, since 337 divides the order of the abelian group G in question, one finds that G has an element of order 337).

c. There exists no homomorphism of groups $\varphi : G \to H$ with G non-abelian and H abelian.

Solution: FALSE (Define $\varphi(g) = e'$, for all $g \in G$, where e' is the identity in H. This is trivially a homomorphism, no matter what the group H may be, and $\{e'\}$ is abelian).

d. There is a surjective homomorphism of groups $\varphi : G \to H$ with G abelian and H non-abelian.

Solution: FALSE (Suppose that φ is such a surjection. Given any elements $a, b \in H$, the surjectivity of φ implies that there exist $g, h \in G$ with $\varphi(g) = a$ and $\varphi(h) = b$. But then the homomorphism property of φ combines with the fact that G is abelian to show that $ab = \varphi(g)\varphi(h) = \varphi(gh) = \varphi(hg) = \varphi(h)\varphi(g) = ba$. Since this holds for all $a, b \in H$, we have shown that H is abelian, contradicting that H is non-abelian. So no such surjective homomorphism exists).

e. Suppose that H and K are subgroups of a group G with $H \lhd G$ and $K \lhd G$. Then one has $HK \lhd G$.

Solution: TRUE (This is implicit in the 2nd Homomorphism Theorem, where we need assume only that $H \leq G$).

2. [5+5+5+5=20 points]

(a) Define what is meant by the *kernel* of a homomorphism of groups $\varphi : G \to H$.

Solution: The kernel of φ is $\ker(\varphi) = \{a \in G : \varphi(a) = e'\}$, where e' is the identity of H.

(b) Define what is meant by the statement that two groups G and H are *isomorphic*.

Solution: The groups G and H are isomorphic if there is an isomorphism (i.e. a bijective homomorphism) $\varphi : G \to H$.

(c) Let G be a group and let $N \lhd G$. Define what is meant by the *quotient group* G/N.

Solution: The quotient (or factor) group G/N is the set $\{Na : a \in G\}$ of right cosets, equipped with the binary operation $(Na)(Nb) = N(ab)$.

(d) Define what is meant by the statement that the group G is *cyclic*.

Solution: A cyclic group G is a group generated by a single element $a \in G$, so that $G = \langle a \rangle = \{a^n : n \in \mathbb{Z}\}$.

Continued...

3. [6+6=12 points] Suppose that G is a group of order 4 that is **not** cyclic.

(a) Apply Lagrange's theorem to show that G has at least two distinct subgroups of order 2, say $\{e, a\}$ and $\{e, b\}$.

Solution: Since $|G| = 4$, there is an element $a \in G \setminus \{e\}$ whose order, by Lagrange's theorem, is an integer d exceeding 1 that divides 4. One cannot have $d = 4$, for then $|\langle a \rangle| = 4 = |G|$, which would imply that $G = \langle a \rangle$ and that G is cyclic (which is not the case). So $d = 2$ and $\langle a \rangle = \{e, a\}$. Hence, there exists $b \in G \setminus \{e, a\}$, and by the same argument, one has $\langle b \rangle = \{e, b\}$. Thus G has at least two distinct subgroups of order 2, namely $\{e, a\}$ and $\{e, b\}$.

(b) Show that G is abelian, and that G can be written as the set $\{e, a, b, ab\}$ subject to the rules $a^2 = b^2 = e$ and $ab = ba$.

Solution: Assume the solution of part (a). By the closure property of G, one has $ab \in G$. Since $a^2 = e$, one has $a^{-1} = a$, and thus one cannot have $ab \in \{e, a\}$. For in the latter circumstances, either $ab = e$ and hence $b = a$, or else $ab = a$ and hence $b = e$. Neither is tenable, and similarly one cannot have $ab \in \{e, b\}$. Likewise, one has $b^2 = e$ and one cannot have $ba \in G \setminus \{e, a, b\}$. The only possibility, therefore, is that ab is the fourth element of the group, and likewise so is ba, whence $ab = ba$. Thus we have $G = \{e, a, b, ab\}$ with $a^2 = b^2 = e$ and $ab = ba$, as required. This relation shows that $gh = hg$ for all $g, h \in \{e, a, b, ab\}$, so G abelian.

4. [12 points] If G is a group and $Z(G)$ is the center of G, show that if $G/Z(G)$ is cyclic, then G is abelian.

Solution: Suppose that G is a group satisfying the property that $G/Z(G)$ is cyclic, say $G/Z(G) = \langle Z(G)a \rangle = \{Z(G)a^j : j \in \mathbb{Z}\}$. Consider two elements $g, h \in G$. For some integers j and k, one has $g \in Z(G)a^j$ and $h \in Z(G)a^k$. Hence, there exist $z_1, z_2 \in Z(G)$ for which $g = z_1 a^j$ and $h = z_2 a^k$. Notice that from the definition of $Z(G)$, the elements z_1 and z_2 commute with all elements of G. In particular, one sees that $gh = (z_1 a^j)(z_2 a^k) = (z_1 z_2)a^{j+k} = (z_2 z_1)a^{k+j} = (z_2 a^k)(z_1 a^j) = hg$. Since this relation holds for all $g, h \in G$, we are forced to conclude that G is abelian.

5. [12 points] Let G be a group and define the map $\varphi : G \to G$ by putting $\varphi(a) = a^{-1}$ for each $a \in G$. Prove that φ is an isomorphism if and only if G is abelian.

Solution: If φ is an isomorphism, then in particular it is a homomorphism. Hence, whenever $a, b \in G$, one has $(ab)^{-1} = \varphi(ab) = \varphi(a)\varphi(b) = a^{-1}b^{-1}$. Given any $g, h \in G$, put $a = g^{-1}$ and $b = h^{-1}$. Then since $a^{-1} = g$ and $b^{-1} = h$, and $(ab)^{-1} = b^{-1}a^{-1}$, one sees that $hg = b^{-1}a^{-1} = (ab)^{-1} = a^{-1}b^{-1} = gh$. Since $hg = gh$ for all $g, h \in G$, one concludes that whenever φ is an isomorphism, then G is abelian.

Conversely, if G is abelian, then whenever $a, b \in G$, one has $\varphi(ab) = (ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1} = \varphi(a)\varphi(b)$, so that φ is a homomorphism. But $\varphi(\varphi(a)) = \varphi(a^{-1}) = (a^{-1})^{-1} = a$, for each $a \in G$, so that φ has itself as an inverse mapping. Thus φ is necessarily bijective, and so φ is a bijective homomorphism, and hence an isomorphism.

Continued...

6. [8+8+8=24 points] This question concerns the set of 2×2 matrices

$$G = \left\{ \begin{pmatrix} a & 0 \\ b & a \end{pmatrix} : a, b \in \mathbb{Q}, a \neq 0 \right\}.$$

(a) Show that G forms an abelian group with the operation of matrix multiplication.

Solution: Whenever $A = \begin{pmatrix} a & 0 \\ b & a \end{pmatrix} \in G$ and $B = \begin{pmatrix} c & 0 \\ d & c \end{pmatrix} \in G$, one has $a \neq 0$ and $c \neq 0$. Hence $ac \neq 0$ and thus

$$AB = \begin{pmatrix} a & 0 \\ b & a \end{pmatrix} \begin{pmatrix} c & 0 \\ d & c \end{pmatrix} = \begin{pmatrix} ac & 0 \\ bc + ad & ac \end{pmatrix} \in G,$$

so the set G is closed under matrix multiplication. Associativity of matrix multiplication is inherited from associativity of all matrix multiplication. The element $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in G$ serves as the identity element. Also, the element $A^{-1} = \begin{pmatrix} a^{-1} & 0 \\ -ba^{-2} & a^{-1} \end{pmatrix} \in G$ serves as an inverse element to A, since $a \neq 0$. Thus G satisfies the group axioms with the group operation of matrix multiplication.

(b) Consider the map $\varphi : G \to \mathbb{Q}^\times$, from the group G into the multiplicative group of rational numbers $\{a \in \mathbb{Q} : a \neq 0\}$, defined by $\begin{pmatrix} a & 0 \\ b & a \end{pmatrix} \mapsto a$. Show that φ is a group homomorphism, and determine its kernel.

Solution: The map φ is clearly well-defined. Also, whenever $A, B \in G$, and are defined as above, then $\varphi(AB) = ac = \varphi(A)\varphi(B)$, so that φ satisfies the homomorphism property. Moreover, one has

$$\ker(\varphi) = \left\{ \begin{pmatrix} a & 0 \\ b & a \end{pmatrix} \in G : a = \varphi \begin{pmatrix} a & 0 \\ b & a \end{pmatrix} = 1 \right\} = \left\{ \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} : b \in \mathbb{Q} \right\}.$$

(c) Let H denote the subset of G defined by $H = \left\{ \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} : b \in \mathbb{Q} \right\}$. Show that H is isomorphic to the group $(\mathbb{Q}, +)$ of rational numbers with the binary operation of addition, and that $G/H \cong \mathbb{Q}^\times$.

Solution: Define the map $\psi : H \to \mathbb{Q}$ by taking $\begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} \mapsto b$. Then the map ψ is well-defined, and whenever $C = \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} \in H$ and $D = \begin{pmatrix} 1 & 0 \\ d & 1 \end{pmatrix} \in H$, one has

$$\psi(CD) = \psi \begin{pmatrix} 1 & 0 \\ c + d & 1 \end{pmatrix} = c + d = \psi(C) + \psi(D),$$

so that ψ satisfies the homomorphism property from H to $\mathbb{Q}$ (as an additive group). Moreover the map $\psi^{-1} : \mathbb{Q} \to H$ defined by taking $\psi^{-1}(b) = \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix}$ acts as an inverse to ψ for each $b \in \mathbb{Q}$. Hence ψ is bijective, and thus is an isomorphism. So H is indeed isomorphic to $\mathbb{Q}$ as an additive group. Moreover, since $H = \ker(\varphi)$ and $\varphi : G \to \mathbb{Q}^\times$ is surjective, it follows from the First Homomorphism Theorem that $G/\ker(\varphi) \cong \mathbb{Q}^\times$, whence $G/H \cong \mathbb{Q}^\times$.

End of examination.