CS21001 Discrete Structures, Autumn 2005

Class test 2

Total marks: 20 | November 10, 2005 | **Duration:** $1 + \epsilon$ hour

---

Roll No: ________________ **Name:** ______________________________

Answer all questions in the respective spaces provided.
Use extra sheets for rough work. Any such extra sheet will not be corrected.

1. Which of the following assertions is/are true. Give short justifications. No credits will be given without proper reasoning. **(2×5)**

(a) The set of all complex numbers of the form $x + \mathrm{i}y$ with x, y integers and with x even is a group under addition of complex numbers.

True: It suffices only to check closure and inverse. If x, y, x', y' are integers then $x + x'$ and $y + y'$ are also integers. Moreover, if x and x' are even, then so also is $x + x'$. Finally, the inverse of $x + \mathrm{i}y$ is $-x - \mathrm{i}y$. Here $-x, -y$ are also integers and $-x$ is also even (if x is so).

(b) Let G be a multiplicative group in which $(ab)^{-1} = a^{-1}b^{-1}$ for all $a, b \in G$. Then G is Abelian.

True: Let $a, b \in G$. By the given property $(a^{-1}b^{-1})^{-1} = (a^{-1})^{-1}(b^{-1})^{-1} = ab$. Moreover, in any group $(a^{-1}b^{-1})^{-1} = (b^{-1})^{-1}(a^{-1})^{-1} = ba$. Thus $ab = ba$.

(c) Let $f : G_1 \to G_2$ be a homomorphism of finite groups and $a \in G_1$. Then $\operatorname{ord} f(a)$ is an integral multiple of $\operatorname{ord} a$.

False: Take $G_1 = G_2$ to be any finite group and the trivial homomorphism $f : G_1 \to G_2$ that maps every $a \in G_1$ to the identity $e_2 \in G_2$. If $e_1 \neq a \in G_1$, then $\operatorname{ord} a > 1$, whereas $\operatorname{ord} f(a) = \operatorname{ord} e_2 = 1$.

(d) Let G be a group and $m, n \in \mathbb{N}$ with $\gcd(m, n) = 1$. Assume that G contains elements a, b with $\operatorname{ord} a = m$ and $\operatorname{ord} b = n$. Then G is cyclic.

False: Take $m, n > 1$ and $G = C_{mn} \times C_{mn}$, where C_{mn} is a multiplicative cyclic group of order mn. Let g be a generator of C_{mn}. Take $a = (g^n, e)$ and $b = (g^m, e)$.

(e) Let H, K be subgroups of a finite multiplicative group G with $K \subseteq H$. Then $[G\!:\!K] = [G\!:\!H][H\!:\!K]$.

True: By Lagrange's theorem $[G\!:\!K] = |G|/|K| = (|G|/|H|)(|H|/|K|) = [G\!:\!H][H\!:\!K]$.

---

2. Let G be a multiplicative group and H, K subgroups of G with $H \cap K = \{e\}$. Assume that $G = HK = \{hk \mid h \in H, k \in K\}$. Prove that every element $a \in G$ can be written as $a = hk$ for some *unique* elements $h \in H$ and $k \in K$. (Note: In this case G is called the *internal direct product* of H and K.) **(5)**

Solution Let $a \in G$ be written as $a = h_1k_1 = h_2k_2$ with $h_1, h_2 \in H$ and $k_1, k_2 \in K$. The element $h_1^{-1}h_2 = k_1k_2^{-1}$ belongs to $H \cap K$ and is the identity element by hypothesis. But then $h_1 = h_2$ and $k_1 = k_2$.

3. Prove that an infinite group has infinitely many subgroups. **(5)**

Solution Let G be an infinite multiplicative group. If G has an element a of infinite order, then for every $n \in \mathbb{N}$, G has a subgroup generated by g^n. These subgroups are different for different values of n.

Finally assume that all elements of G have finite orders. Let $a_1, a_2, \ldots, a_n, \ldots$ be distinct elements of G. Consider the subgroups $H_n = \langle a_n \rangle$ for all $n \in \mathbb{N}$. Suppose that there are only finitely many different subgroups in the family $H_1, H_2, H_3, \ldots$ of subgroups. This means there exists an $n \in \mathbb{N}$ such that $H_n = H_{n+1} = H_{n+2} = \cdots$. But a_n is of finite order, i.e., H_n is a finite group and cannot contain all of the infinitely many elements $a_{n+1}, a_{n+2}, a_{n+3}, \ldots$. If $a_m \notin H_n$ for some $m > n$, then $H_m \neq H_n$, a contradiction.