MATH 323: Algebra I. **Midterm 1.** LJB, 11 November 2016, Bilkent University.

Time allowed: 110 minutes. Please put your name on EVERY sheet of your manuscript. The use of telephones, calculators or other electronic devices is prohibited. The use of very faint pencils is prohibited too. You may take the question sheet home.

Remember to justify your answers, except in any cases where your answers are obvious.

1: 25 marks. (a) Find the inverse of 5 in the multiplicative group of units $(\mathbb{Z}/127)^\times$.

(b) Find the orders of the elements 2 and 19 in $(\mathbb{Z}/127)^\times$.

(c) How many elements of order 2 are there in $(\mathbb{Z}/127)^\times$?

(d) What are the prime numbers p such that $(\mathbb{Z}/127)^\times$ has an element of order p?

(e) Find the inverse of 2234 in $(\mathbb{Z}/8191)^\times$.

2: 32 marks. Which of the following statements hold for all subgroups B of all finite abelian groups A? (In each case, give a proof or a counter-example.)

(a) If A is cyclic, then B and A/B are cyclic.

(b) If B and A/B are cyclic, then A is cyclic.

(c) If A has a subgroup of order 127, then B or A/B has a subgroup of order 127.

(d) If B or A/B has a subgroup of order 127, then A has a subgroup of order 127.

3: 21 marks. Let G be a finite group with normal subgroups H and K. Let $\theta : G \to G/H \times G/K$ be the function such that $\theta(g) = (gH, gK)$ for each $g \in G$.

(a) Show that θ is a group homomorphism.

(b) Show that, if the positive integers $|G|/|H|$ and $|G|/|K|$ are coprime, then θ is surjective.

(c) In the case where θ is surjective, express $|H \cap K|$ in terms of $|G|$ and $|H|$ and $|K|$.

4: 22 marks. Let G be a finite group. We say that G is **perfect** provided every abelian quotient group of G is trivial. Show that G has a perfect normal subgroup N such that every perfect normal subgroup of G is contained in N.

Midterm 1 Solutions

There is no such thing as a "model solution". Often, there are many good ways of deducing a given conclusion.

1: Part (a). We have $127 = 25.5 + 2$ and $5 = 2.2 + 1$, hence

$$1 = 5 - 2.2 = 5 - 2(127 - 25.5) = 51.5 - 2.127 \, .$$

Therefore, in this group of units, $5^{-1} = 51$.

Part (b). For $1 \leq n \leq 6$, we have $2 \leq 2^n \leq 64$, perforce, $2^n \not\equiv 1$ modulo 127. But $2^7 = 128 \equiv 1$. So the order of 2 is 7.

We have $3.127 = 381$ and $19^2 = 361 = 381 - 20$ and $19.20 = 380 = 381 - 1$. Therefore $19^3 \equiv 1$ and 19 has order 3.

Part (c). We shall show that there is exactly 1 element of order 2. Let x be an integer such that $x^2 \equiv 1$ modulo 127. Then 127 divides the integer $x^2 - 1 = (x+1)(x-1)$. Since 127 is prime, it divides $x + 1$ or $x - 1$. In other words, $x \equiv 1$ or $x \equiv -1$. In the former case, x has order 1. Therefore the congruence class of $-1 \equiv 126$ is the unique element with order 2.

Part (d). The set of such p is $\{2, 3, 7\}$. Indeed, in parts (b) and (c) we saw that the elements 126, 19, 2 have orders 2, 3, 7, respectively. On the other hand, $|(\mathbb{Z}/127)^\times| = 126 = 2.3.3.7$, whereupon Lagrange's Theorem informs us that no element of the group has order divisible by a prime distinct from 2, 3, 7.

Part (e). We have $8191 = 4.2234 - 745$ and $2234 = 3.745 - 1$, hence

$$1 = 3.745 - 2234 = 3(4.2234 - 8191) - 2234 = 11.2234 - 3.8191 \, .$$

Therefore, $2234^{-1} = 11$.

Comment: Of course, part (e) can also be done using only positive remainders, exactly as in lectures, starting with $8191 = 3.2234 + 1489$. That variant takes a bit longer.

2: Part (a). The statement is true. Letting a be a generator of A, then aB is a generator of A/B and, in particular, A/B is cyclic. Let n be the order of A, and let m be the smallest positive integer such that $a^m \in B$. The greatest common divisor h of n and m has the form $h = xn + ym$ for some integers x and y. Therefore $a^h \in B$. The minimality of m now implies that $m = h$, in other words, m divides n. It is now easy to see that B is the cyclic subgroup generated by a^m.

Part (b). False. The case where $A = V_4$ and $1 < B < A$ is a counter-example.

Part (c). True. Since 127 is prime, the given assumtion implies that A has an element x with order 127. If the cyclic subgroup $X = \langle x \rangle$ is not contained in B, then $X \cap B = 1$ and the Second Isomorphism Theorem yields $X \cong XB/B \leq A/B$.

Part (d). True. One case being trivial, we may assume that A/B has a subgroup of order 127. Since 127 is prime, there exists an element $y \in A$ such that the element $yB \in A/B$ has order 127. The element $y \in A$ has order divisible by 127. So some power of y has order 127.

3: Part (a). We have $\theta(f)\theta(g) = (fH, fK)(gH, gK) = (fgH, fgK) = \theta(fg)$ for all $f, g \in G$.

Part (b). Since the kernel of θ is $H \cap K$, the First Isomorphism Theorem implies that $|\theta(G)| = |G|/|H \cap K|$, which is divisible by both $|G|/|H|$ and $|G|/|K|$. By the coprimality hypothesis, $|\theta(G)| = |G/H|.|G/K| = |G/H \times G/K|$.

Part (c). Supposing that θ is surjective then, applying the First Isomorphism Theorem as in part (b), we deduce that $|G : H \cap K| = |G : H||G : K|$. Therefore $|H \cap K| = |H||K|/|G|$.

4: Let $\mathcal{S}$ be the class of finite groups F for which there exist normal subgroups N_0, ..., N_r of G such that $1 = N_0 \trianglelefteq ... \trianglelefteq N_r = F$ and each N_i/N_{i-1} is abelian. It is not hard to see that $\mathcal{S}$ is closed under subgroups, quotient groups and direct products. We mean to say, given F and F' in $\mathcal{S}$, then every subgroup of F is in $\mathcal{S}$, every quotient group of F is in $\mathcal{S}$ and the direct product $F \times F'$ belong to $\mathcal{S}$. It follows that, given normal subgroups H and K of G such that G/H and G/K belong to $\mathcal{S}$, then every subgroup of $G/H \times G/K$ belongs to $\mathcal{S}$. Applying the First Isomorphism Theorem to the group homomorphism θ in Question 3, we deduce that $G/(H \cap K)$ belongs to $\mathcal{S}$. Therefore, G has a unique normal subgroup N that is minimal subject to G/N being in $\mathcal{S}$. In fact, given a normal subgroup N' of G, then G/N' is in $\mathcal{S}$ if and only if $N \leq N'$.

Let M be the unique normal subgroup of N that is minimal subject to N/M being in $\mathcal{S}$. Given $g \in G$, then ${}^gN = N$ and $N/{}^gM$ is in $\mathcal{S}$. By the uniqueness of M, we have ${}^gM = M$. in other words, $M \trianglelefteq G$. But G/M is in $\mathcal{S}$. By the definition of N, we have $M = N$. We have shown that N is perfect.

For any $L \trianglelefteq G$, the Second Isomorphism Theorem implies that $L/(L \cap N) \cong LN/N$. But LN/N belongs to $\mathcal{S}$. So, if L is perfect, then $L \cap N = L$, in other words, $L \leq N$. $\square$

Comment: The groups in $\mathcal{S}$ are called the **solvable finite groups**. The name derives from the following. Any polynomial equation over $\mathbb{Q}$ is associated with a finite group, called the Galois group, which expresses the symmetries of the equation. The Galois group is solvable if and only if the solutions to the equation can be expressed in terms of $\mathbb{Q}$, addition, subtraction, multiplication, division, square roots, cube roots and higher such roots.