MATH 323: Algebra I. Midterm 1. LJB, 31 October 2014, 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.

1: 20 points. Write down the orders and inverses of each of the 16 elements of the group $\mathbb{Z}/16\mathbb{Z}$. (No proofs are required. Just state the answers.)

2: The number $257 = 2^8 + 1$ is prime. Consider the multiplicative group

$$(\mathbb{Z}/257\mathbb{Z})^\times = \{[1], [2], ..., [255], [256]\} .$$

(a), 10 points. Using the Euclidian algorithm, find the inverse of $[19]$ in $(\mathbb{Z}/257\mathbb{Z})^\times$.

(b), 5 points. You may assume that $19^{128} \equiv -1$ modulo 257. What is the order of the element $[19]$ of $(\mathbb{Z}/257\mathbb{Z})^\times$? (Do not forget to justify your answer.)

3: Let G be a finite group with subgroups H and K such that $|G|/|K| = 2$ and H is not contained in K.

(a), 10 points. Show that K is a normal subgroup of G.

(b), 10 points. Show that $H/(H \cap K) \cong C_2$.

4: The dihedral group with order 10 is the group $D_{10} = \{1, a, a^2, a^3, a^4, b, ab, a^2b, a^3b, a^4b\}$ with $a^5 = b^2 = 1$ and $ba = a^{-1}b$.

(a), 10 points. Find all the subgroups of D_{10}.

(b), 5 points. Using Lagrange's theorem, explain why your list of subgroups is complete.

(c), 10 points. Draw a diagram of the subgroup lattice of D_{10}.

5: A group F is said to be **metabelian** provided F has an abelian normal subgroup A such that F/A is abelian.

(a), 10 points. Show that any subgroup of a metabelian group is metabelian.

(b), 10 points. Let $H \trianglelefteq G \trianglerighteq K$ be groups such that G/H and G/K are metabelian. Show that $G/(H \cap K)$ is metabelian.

Bonus Question: 10 points. (This question is very hard. You are advised not to spend time on it unless you have finished the questions above.) Let G be a finite group, let p be the smallest prime number dividing $|G|$, and let $H \leq G$ such that $|G|/|H| = p$. Show that H is a normal subgroup of G. (Hint: Consider the action of G on the set of left cosets of H in G. Construct a group homomorphism from G to the symmetric group S_p.)

Midterm 1 Solutions, version 10 November 2014

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

1: The orders and inverses of each element $x \in \mathbb{Z}/16/\mathbb{Z}$ are as shown in the table.

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
order of x	1	16	8	16	4	16	8	16	2	16	8	16	4	16	8	16
inverse of x	0	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

2: We have $257 = 13\,.\,19 + 10$ and $19 = 1\,.\,10 + 9$ and $10 = 1\,.\,9 + 1$. Now

$$1 = 10 - 9 = 10 - (19 - 10) = 2\,.\,10 - 19 = 2\,.\,(247 - 13\,.\,19) - 19 = 2\,.\,257 - 27\,.\,19\;.$$

So $[19]^{-1} = [-27] = [230]$.

3: Part (a). Let $g \in G$. If $g \in K$ then $gK = K = Kg$. If $g \notin K$ then $gK = G - K = Kg$.

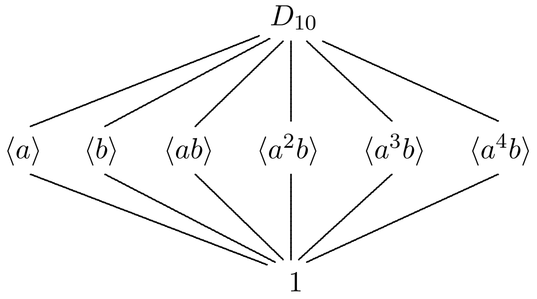
Part (b). We have $K < HK \leq G$. The integer $|G|/|HK|$ is smaller than $|G|/|K|$ and divides $|G|/|K|$. But $|G|/|K| = 2$. So $HK = G$. The group $HK/K = G/K$, being of order 2, must be isomorphic to C_2. The Second Isomorphism Theorem says that $H/(K \cap H) \cong HK/K$.

4: Part (a). The subgroups of D_{10} are:

$$1 = \{1\},\;\; \langle a \rangle \cong C_5,\;\; \langle b \rangle \cong C_2,\;\; \langle ab \rangle \cong C_2,\;\; \langle a^2b \rangle \cong C_2,\;\; \langle a^3b \rangle \cong C_2,\;\; \langle a^4b \rangle \cong C_2,\;\; D_{10}\;.$$

Part (b). Plainly, the elements a, a^2, a^3, a_4 are of order 5. It is easy to see that all elements having the form a^ib are of order 2. By Lagrange's Theorem, every proper subgroup of D_{10} has order 2 or 5. Since 2 and 5 are prime, every proper subgroup must be cyclic. Noting that $\langle a \rangle = \langle a^2 \rangle = \langle a^3 \rangle = \langle a^4 \rangle = \{1, a, a^2, a^3, a^4\}$, it is clear that we have listed all the cyclic subgroups of G.

Part (c). The subgroup lattice of D_{10} is as shown.



5: Part (a). Let F and A be as specified and let $H \leq F$. Define $B = H \cap A$. Then B is abelian because it is a subgroup of the abelian group A. Also, H/B is abelian because F/A is abelian and, by the Second Isomorphism Theorem, $H/B \cong HA/A \leq F/A$. We have shown that H is metabelian.

Part (b). It is easy to see that the direct product of two metabelian groups is metabelian. Consider the homomorphism $\theta : G \to G/H \times G/K$ such that $\theta(g) = (gH, gK)$ for $g \in G$. The kernel of θ is $H \cap K$. Hence, via the First Isomorphism Theorem, $G/(H \cap K)$ is isomorphic to a subgroup of the metabelian group $G/H \times G/K$. The required conclusion now follows from part (a).

Bonus Question: *Proof 1:* Enumerate the left cosets of H in G as a_1H, ..., a_pH. Let $\theta : G \to S_p$ be the function $g \mapsto \sigma_g$ where $ga_iH = a_{\sigma_g(i)}H$ for each integer $1 \leq i \leq p$. Given $f, g \in G$, then $a_{\sigma_{fg}(i)}H = fgaH = fa_{\sigma_g(i)}H = a_{\sigma_f(\sigma_g(i))}H$. So $\sigma_{fg} = \sigma_f \circ \sigma_g$, in other words, θ is a homomorphism. Let $K = \ker(\theta)$. The integers $|G|$ and $|S_p| = p!$ are divisible by the order of the group $G/K \cong \mathrm{Im}(\theta)$. Hence, thanks to the hypothesis on p, we have $|G|/|K| \in \{1, p\}$. But $K \leq H < G$, so $|G|/|K| = p$. Therefore $|K| = |H|$. We have shown that the normal subgroup K coincides with H. □

The ideas in the latest proof will be easier to follow and will seem more natural when we have spent more time on the notion of a permutation set. Let us present the same proof again, but in a smoother way which makes use of that notion.

Proof 2: Let $\mathcal{R}$ be the set of left cosets of H in G. We allow G to act on $\mathcal{R}$ such that an element $g \in G$ sends a coset aH to the coset gaH. The action is represented by a homomorphism $\theta : G \to \mathrm{Sym}(\mathcal{R})$ where $\mathrm{Sym}(\mathcal{R})$ is the group of permutations of $\mathcal{R}$. Let $K = \ker(\theta)$. Obviously, $|G : K|$ divides $|G|$. By the First Isomorphism Theorem, $|G : K|$ divides the integer $p! = |\mathrm{Sym}(\mathcal{R})|$. Since p is the smallest prime divisor of $|G|$ and $K \leq H < G$, we have $|G : K| = p = |G : H|$. Therefore $K = H$. □