MATH 120 MIDTERM

Write your name at the top of each page. Give complete proofs except for problem 1, where answers will suffice. Each problem is worth the same. If you would like to know how you did before the drop date (Sunday), please send me an e-mail, and I'll respond on Saturday.

1.
(a) Is the set of rational numbers in lowest terms whose denominators are even, along with zero, a subgroup of the (additive group of) rational numbers?
(b) How many elements of D_8 have order exactly 2?
(c) Must every subgroup of an abelian group be normal?

2. Show that if H and K are normal subgroups of G, then $H \cap K$ is normal in G too.

3. Let M and N be normal subgroups of G such that $G = MN$. Prove that

$$G/(M \cap N) \cong (G/M) \times (G/N).$$

4. Show that $GL_2(\mathbb{F}_2)$ is isomorphic to S_3.

5. Let G be any group. (a) Prove that the map $G \to G$ defined by $g \mapsto g^2$ is a homomorphism if and only if G is abelian. (b) If G is abelian and finite show that this map is an isomorphism if and only if G has odd order.

6. Let G be a group of order pq, where $p > q$ are primes.
(a) Show that there is one subgroup of order p in G. (Hint: if A and A' were two such, what can you say about $|AA'|$?)
(b) Suppose $a \in G$ has order p. Show that $A = \langle a \rangle$ (the subgroup generated by a) is normal in G.
(c) Show that if $x \in G$, then $x^{-1}ax = a^i$ for some $0 < i < p$ (depending on x).
(d) *(harder)* Show that if q is not a factor of $p - 1$, then G is cyclic.

E-mail address: `vakil@math.stanford.edu`

Math 120 midterm — hints and solutions

1. a) No (Eg. $1/6 + 1/6 = 1/3$)
   b) 5 (s, r^2, sr^2, sr, sr^3)
   c) Yes (conjugation in an abelian group fixes each element) $\square$

2. Suppose $x \in H \cap K$, $g \in G$. Since [redacted] $x \in H$ and $H \trianglelefteq G$, we have $gxg^{-1} \in H$; since $x \in K$ and $K \trianglelefteq G$, we also have $gxg^{-1} \in K$. Thus $gxg^{-1} \in H \cap K$, and the claim follows. $\square$

3. Let $\varphi : G \longrightarrow G/M \times G/N$ be the map $g \mapsto (gM, gN)$. For all $g_1, g_2 \in G$ we have

$$\varphi(g_1 g_2) = (g_1 g_2 M, g_1 g_2 N)$$

Def. of group str on G/M, G/N ($M, N \trianglelefteq G$!) $\rightarrow$ $= ((g_1M)(g_2M), (g_1N)(g_2N))$

Def. of group str on $G/M \times G/N$ $\rightarrow$ $= (g_1M, g_1N) \cdot (g_2M, g_2N)$

$$= \varphi(g_1)\varphi(g_2),$$

whence φ is a homomorphism. Suppose $(g_1M, g_2N) \in G/M \times G/N$. Since $G = MN$, we can find $m \in M$, $n \in N$ s.t. $g_1^{-1} g_2 = mn$. Then $g_1 m = g_2 n^{-1}$, and so

$$\varphi(g_1 m) = (g_1 m M, g_1 m N) = (g_1 m M, g_2 n^{-1} N)$$

$$= (g_1 M, g_2 N),$$

whence φ is a surjection. Finally, observe that

$$\varphi(g) = 1_{G/M \times G/N}$$

$$\Leftrightarrow \quad (gM, gN) = (M, N)$$

$$\Leftrightarrow \quad g \in M \ \& \ g \in N$$

$$\Leftrightarrow \quad g \in M \cap N.$$

Thus $\ker \varphi = M \cap N$, and the claim follows from the First Isomorphism Theorem. $\square$

4. Let $X = \{(0,1), (1,0), (1,1)\}$ be the set of non-zero vectors in $\mathbb{F}_2^2$, and let

$$\varphi : GL_2(\mathbb{F}_2) \longrightarrow S_X \quad (\overset{\text{since } |X| = 3}{\approx} S_3)$$

be the permutation representation induced by the usual multiplication of vectors by matrices (so that

$$\varphi(A)(v) = Av$$

for all $A \in GL_2(\mathbb{F}_2)$ and $v \in X$). Then φ is injective, for if $\varphi(A) = \mathrm{id}_X$, then

$$Av = \varphi(A)(v) = v$$

for all $v \in X$, and taking $v = (1,0), (0,1)$ we see that $A = I_2$. To complete the proof, it

only remains to show that φ is surjective. Observe that $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \in GL_2(\mathbb{F}_2)$ has order 3 and that $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in GL_2(\mathbb{F}_2)$ has order 2. Since φ is injective, it follows that $\varphi\left(\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\right)$ and $\varphi\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right)$ also have orders 3 and 2, respectively. Thus $3 \mid |\mathrm{Im}\,\varphi|$ and $2 \mid |\mathrm{Im}\,\varphi|$, whence $|\mathrm{Im}\,\varphi| \geq 6$. Since

$$|S_X| = |S_3| = 6,$$

it follows that $\mathrm{Im}\,\varphi = S_X$, as desired. $\square$

5. Let φ denote the map $G \to G$, $g \mapsto g^2$.

a) Suppose first that φ is a homomorphism. Then for all $a, b \in G$ we have

$$abab = (ab)^2 = \varphi(ab) = \varphi(a)\varphi(b) = a^2b^2,$$

Multiplying by a^{-1} from the left and by b^{-1} from the right we see that

$$ba = ab,$$

whence G is abelian as claimed. Conversely, suppose G is abelian. Then for all $a, b \in G$ we have

$$\varphi(ab) = (ab)^2 = a\underbrace{ba}_{\text{swap}}b = a^2b^2 = \varphi(a)\varphi(b),$$

whence φ is a homomorphism. $\square$

b) Let G be abelian and finite. If $|G|$ is even, then Cauchy's theorem implies that there exists an element $g \in G$ of order 2. Then $g \in \operatorname{Ker} \varphi$, $g \neq 1_G$, whence φ is not an isomorphism. OTOH, if $|G|$ is odd, then G cannot contain elements of order 2. Thus in this case $\operatorname{Ker} \varphi = \{1_G\}$, and φ is injective. Since G is finite it follows that φ is bijective, and hence an isomorphism. $\square$

6. a) By Cauchy's theorem there exists an element $g \in G$ of order p. Then

$$A = \langle g \rangle \leq G$$

is a subgroup of order p. Suppose $A' \leq G$ also has order p. Then $A \cap A' \leq A$, whence $|A \cap A'| \mid |A| = p$. Since p is a prime, it follows that $|A \cap A'| = 1$ or $|A \cap A'| = p$. In the former case we would have

$$|AA'| = \frac{|A||A'|}{|A \cap A'|} = p^2 > pq = |G|,$$

a contradiction. Thus $|A \cap A'| = p$, and hence $A = A'$. We have shown that G has a unique subgroup of order p, as claimed. $\square$

b) Observe that $A \leq G$ is a subgroup of order p, as is gAg^{-1} for all $g \in G$. Thus by a) we have $gAg^{-1} = A$ for all $g \in G$, whence A is normal in G.

c) From part b) we know that for any $x \in G$

$$x^{-1} a x \in A = \langle a \rangle \underset{\substack{\uparrow \\ (\text{since } |a| = p)}}{=} \{1, a, \dots, a^{p-1}\}.$$

Since $a \neq 1$, we have $x^{-1} a x \neq 1$, and the claim follows. $\blacksquare$

d) Assume $q \nmid (p-1)$. By Cauchy's theorem, we can find an element $x \in G$ of order q. By part c), we have

$$(*) \qquad x^{-1} a x = a^{i}$$

for some $0 < i < p$. Denote $y = x^{p-1}$. Then

$$y^{-1} a y = x^{-(p-1)} a x^{p-1} \overset{(1)}{=} a^{i^{p-1}} \overset{(2)}{=} a,$$

where (1) follows from $(*)$ and (2) follows from Fermat's little theorem, which implies that $i^{p-1} \equiv 1 \pmod{p}$. Thus a and y commute. Moreover, by the assumptions $q \nmid (p-1)$, $q < p$, we have

$$|y| = |x^{p-1}| = \frac{|x|}{\gcd(|x|, p-1)} = \frac{q}{\gcd(q, p-1)} = q.$$

Since $|ay| \mid |G| = pq$, we have $|ay| = 1, p, q$ or pq. If we had $|ay| = 1$, then $a = y^{-1}$, [redacted] and hence $p = |a| = |y^{-1}| = q$, a contradiction. If we had $|ay| = p$, then

$$1 = (ay)^p \underset{\substack{\uparrow \\ (\text{since } a, y \text{ commute})}}{=} a^p y^p = y^p,$$

whence $q = |y| \mid p$, a contradiction. Finally,

If we had $|ay| = q$, then

$$1 = (ay)^q = a^q y^q = a^q,$$

whence $p = |a| \mid q$, again a contradiction. Thus we must have $|ay| = pq$, whence $G = \langle ay \rangle$. $\square$