MATH 71: ALGEBRA
FUNDAMENTAL LONG EXERCISES (FLEX)

FLEX (Fundamental Long EXercise) problems concern a theorem in group theory we did not prove in class. You will be guided through the proof and asked to fill in the details carefully. The intended audience is your peers, so you should write in a way that you would have wanted something explained to you. You must choose one of the topics on the next page. Your solution should contain:

- An introduction and motivation, explaining context and why we should care, including the statement of the main results, and any relevant acknowledgements
- Examples, lemmas, propositions, preliminary setup, etc.
- Proof of the main results
- A conclusion, giving applications, corollaries, further examples, future directions

The goal is that the reader (a fellow student) could read your paper and understand very well the theorem and where it comes from—and they should also be convinced that you understood it! There is no minimum or maximum length requirement. Maybe 5 pages is a general ballpark. More just for the sake of more in describing mathematics isn't helpful: you want to be both concise and complete. Of course, more examples and different/reinforcing explanations are good, reviewing concepts and generally being careful is all good! But boring us with associativity axioms is not. You can write it out by hand (pencil or pen is OK), or you can type it out using LaTeX or a word processor. A LaTeX template is provided on Canvas, so you can copy-paste into Overleaf (`http://overleaf.com`) and just modify it for your paper. Even if you do not use LaTeX, the template will hopefully give you some sense of what to be aiming for. You do not have to prove everything from scratch, but you must give precise references when you are using something important (e.g., "By Lagrange's theorem [DF, §3.2, Theorem 8, p. 89]" or "we follow the proof of Dummit–Foote [DF, §2.4, Proposition 9, p. 63]"). You are certainly encouraged to use the textbook (indeed, some of the steps are worked out by Dummit–Foote, but they could often use elaboration or other TLC), but the whole point is not to take anything for granted: fill in the details, break things up into steps, explain it in a way that makes sense to you, etc. You are discouraged (but not forbidden) from using references other than the textbook. If you refer to any materials (a website, another book, a random Youtube video, a blog, you talk with another student) other than Dummit–Foote at *any* time while working on this paper, you must explicitly say so: both in the acknowledgements "We consulted [Wikipedia, …]" *and* any specific use in the proof as in the previous paragraph. Yes: each and every thing you consult, cite it. You are very much encouraged to talk to the instructor! If you're not sure about a lemma, or you are stuck on a step, or you're not sure what else to say in terms of framing or application, etc.

Grading

- 10 points: Mathematical correctness/completeness
- 10 points: Organization and clarity/conciseness
- 5 points: Copyediting

The flex problem is due in class on Monday, 14 November 2022. You must hand in a physical copy (e.g. a print out) and do so in person. No late assignments will be accepted.

Date: 17 October 2022; due Monday, 14 November 2022.

POSSIBLE TOPIC 1: CAUCHY'S THEOREM

Difficulty level: medium.

(a) Using Lagrange's theorem, motivate and state Cauchy's theorem (DF, section 3.2, Theorem 11, p. 93).
(b) Read

`https://www.sciencedirect.com/science/article/pii/S031508600300003X`

and provide a few historical remarks (whatever you find interesting and relevant).
(c) Give three proofs of Cauchy's theorem, as follows.
  (a) First, fill in details of the elementary proof in DF, section 3.2, Exercise 9, p. 96. Explain what is happening in this proof by group actions (e.g. the orbit-stabilizer theorem).
  (b) Second, prove Cauchy's theorem for G an abelian group (see DF, section 3.5, Proposition 21, p. 102), then finish with the class equation. *[Hint: if $p \, midZ(G)$, the case of abelian groups applies; otherwise, show that $p \mid C_G(a)$ for some noncentral $a \in G$.]*
  (c) Third, observe that Cauchy's theorem is a corollary of Sylow's theorem (DF, section 4.5, Exercise 3, p. 146).
(d) Show that Cauchy's theorem is best possible: give examples of groups G and integers $d \mid \#G$ such that there is no element of order d in G, in particular give an example of a group G and a prime p with $p^2 \mid \#G$ but such that G has no element of order p^2.
(e) As a first application, show that for a finite abelian group G with $\#G = n$, the map $G \to G$ by $x \mapsto x^k$ is an isomorphism if and only if $\mathbf{gcd}\ ((,\ k), n) = 1$.
(f) As a second application, show that a finite abelian group G with $\#G = n$ has a subgroup of order d for every positive divisor $d \mid n$ (DF, section 3.4, Exercise 4, p. 106).

POSSIBLE TOPIC 2: FINITE ABELIAN GROUPS

Difficulty level: additional technicality (+2 bonus).

(a) Motivate the fundamental theorem of finite abelian groups (DF, section 5.2, Parts 1 and 2 of Theorem 5) by analogy with a basis for a vector space, and go beyond the analogy to a direct statement by considering a finite-dimensional vector space over the field $F = \mathbb{Z}/p\mathbb{Z}$.
(b) Prove the fundamental theorem of finite abelian groups, using the sketch in DF, section 6.1, pp. 196–197, with the following advice:
  (a) Give a complete proof of the recognition theorem for direct products (DF, section 5.4, Theorem 9, p. 171), including a proof of DF, section 5.4, Proposition 8, p. 171.
  (b) Do not take DF, section 6.1, Corollary 4, for granted. Argue directly, as follows. Let G be a finite abelian group.
    - For any $m \in \mathbb{Z}_{\geq 1}$, let $G_m \subseteq G$ be the subset of elements whose order divides m. Show that $G_m \leq G$ is a subgroup.
    - Suppose that $\#G = p^e m$ where $p \nmid m$ is prime. Show that $G \simeq G_{p^e} \times G_m$. *[Hint: to show $G_{p^e} G_m = G$, note that for any $x \, inG$ we have $x^{p^e} \in G_m$ and $x^m \in G_{p^e}$, so then apply the extended Euclidean algorithm.]*
    - Finally, if we have a factorization $\#G = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ into primes, show (by induction) that $G \simeq G_{p_1^{e_1}} \times G_{p_2^{e_2}} \times$ $cdots \times G_{p_r^{e_r}}$.
(c) Illustrate the key steps in this somewhat involved proof by showing what happens in examples. (You can do this before, during, or after the proof.)

(d) As an application, prove that a finite subgroup $H \leq F^\times$ of the multiplicative group of a field F is cyclic (see DF, section 9.5, Proposition 18, p. 314). We will almost surely prove DF, section 9.5, Proposition 17, p. 313, in class; but you should just prove it directly (it is not necessary to know that $F[x]$ is a UFD).

POSSIBLE TOPIC 3: GROUPS OF SMALL ORDER

Difficulty level: more concepts, but some optionality (starts with +2 bonus, plus whatever extra below)

(a) Motivate the classification of groups of small order up to isomorphism; quickly review the case of groups of prime order, providing context to why the factorization of the order $n = \#G$ is reflected in the list of possible groups of order n up to isomorphism.
(b) State Cauchy's theorem and the fundamental theorem of finite abelian groups (giving references, but without proofs; if these are of interest, consider one of the other projects!).
(c) Recall the proof why every group of order p^2 with p prime is abelian.
(d) Classify the *abelian* groups of order $n \leq 15$ up to isomorphism using the fundamental theorem.
(e) Classify groups of order 6 by hand: using Cauchy's theorem, there exists $a \in G$ of order 2 and $b \in G$ of order 3; show that $G = \{1, b, b^2, a, ab, ab^2\}$, in a direct manner that $ba = ab$ or $ba = ab^2$, and show that these two possibilities uniquely determine the Cayley table of G.
(f) Show that every nonabelian group G of order 8 is isomorphic to either D_8 or Q_8, as follows.
- Show that G has an element $a \in G$ of order 4. *[Hint: what happens if every nonidentity element has order 2?]*
- Let $H := \langle a \rangle$ and let $b \notin H$. Observe that $H \trianglelefteq G$ is normal; argue that $bab^{-1} = a^3$ (the order under conjugation is preserved), and then that $G \simeq D_4, Q_8$ according as b has order 2 or 4.

(g) Pause to show we have classified groups of order $n \leq 9$.
(h) Now let G be a group of order pq where p, q are primes with $p < q$ (without loss of generality).
- Let $P \leq G$ be a p-Sylow subgroup and $Q \leq G$ be a q-Sylow subgroup. Show that $Q \trianglelefteq G$ is normal. *[Hint: it has index p, so go through DF, section 4.2, Corollary 5, pp. 120–121.]* Write $P = \langle x \rangle$ and $Q = \langle y \rangle$ with $x, y \in G$.
- Show that $xyx^{-1} = y^k$ with $k \in \{1,$ $cdots, q-1\}$, and use this to define a group homomorphism

$$\phi \colon P \to (\mathbb{Z}/q\mathbb{Z})^\times$$

where $x \mapsto k$. *[Hint: use $x^i y x^{-i} = y^{\phi(i)}$.]* Conclude that either ϕ is the trivial homomorphism (mapping every element to 1) or phi is injective.
- If ϕ is trivial, prove that G is cyclic (DF, section 4.4, Exercise 2, p. 137).
- Show that ϕ is injective if and only if G is nonabelian and $p \mid (q-1)$. (In particular, observe that if $p \nmid (q-1)$ then G is abelian.)
- If $p \mid (q-1)$, exhibit a nonabelian group of order pq (following DF, Example, section 4.5, p. 143; see also DF, section 4.3, Exercise 34, p. 132). Show that when $p = 2$ we obtain the dihedral group D_{2q} of order $2q$ for $q \geq 3$ as a subgroup of S_q via the action on the vertices of a q-gon.
- Suppose that G is nonabelian and $p \mid (q-1)$. Show that P $/triangleleftteqG$ (DF, Example, section 4.5, p. 143), so there exists an injective homomorphism $G \hookrightarrow S_q$ whose image up to conjugation lies in the the normalizer of the cyclic subgroup generated by the q-cycle $(1\ 2$ $cdots\ q)$ (DF, section 4.3, Exercise 28, p. 132). When $p = 2$, show that this group is unique up to conjugation. *[Hint: show that there is a unique subgroup of $(\mathbb{Z}/q\ Z)^\times$ of order 2.]*

(8′) For +3 bonus going a more conceptual route, replace step (8) as follows.
- Read DF, section 4.4.

- Prove that the automorphism group of Z_p is $\mathrm{Aut}(Z_p) \simeq (\mathbb{Z}/p\mathbb{Z})^\times$ (DF, section 4.4, Proposition 16, p. 135 proves something more general). State (but you do not need to prove) that $(\mathbb{Z}/p\mathbb{Z})^\times \simeq Z_{p-1}$ is cyclic.
- Suppose that $p \nmid (q-1)$. Show that G is abelian (DF, Example, section 4.4, p. 135–136) and therefore cyclic (DF, section 4.4, Exercise 2, p. 137).
- Now suppose that $p \mid (q-1)$. Let $P \leq G$ be a p-Sylow subgroup and $Q \leq G$ be a q-Sylow subgroup. Show that $Q \trianglelefteq G$ is normal in G (DF, Example, section 4.5, p. 143).
- Read section 5.5. Show that if $p \mid (q-1)$ then either $G \simeq Z_p \, times Z_q \simeq Z_{pq}$ or $G \simeq Z_p \rtimes Z_q$, the semi-direct product with respect to the homomorphism $Z_p \to \mathrm{Aut}(Z_q) \simeq (\mathbb{Z}/q\mathbb{Z})^\times = \, langleg\rangle$ mapping $x \mapsto g^{(q-1)/p}$ (DF, Example, section 5.5, pp. 181–182; section 5.5, Exercise 6, pp. 184–185).

(i) Classify groups of order $n \leq 15$ except $n = 12$.

(j) For +2 bonus, classify the groups of order 12. Let P_2 be a 2-Sylow subgroup (of order 4) and P_3 a 3-Sylow subgroup.

- Show that either $P_2 \trianglelefteq G$ is normal or $P_3 \trianglelefteq G$ is normal. *[Hint: if P_3 is not normal, count the number of elements of order 3.]* Conclude that in either case, $G = P_2P_3$.
- Show that if both P_2 and P_3 are normal, then $G \simeq P_2 \times P_3$ is abelian. *[Hint: either state and use the recognition theorem for direct products, DF, section 5.4, Theorem 9, p. 171–172; or understand the proof and apply the argument here directly.]*
- Proceeding by cases, first suppose that $P_2 \trianglelefteq G$ and $P_2 \, simeq Z_4$. Arguing as in (8), show that the homomorphism $P_3 \to \mathrm{Aut}(P_2)$ is trivial, so G is abelian and therefore cyclic. *[Hint: $\#\,\mathrm{Aut}(Z_4) = \#(\mathbb{Z}/4\mathbb{Z})^\times = 2$.]*
- Suppose $P_2 \trianglelefteq G$ and $P_2 \simeq Z_2 \times Z_2$ but $P_3 \, not \trianglelefteq G$. Show that there is an injective group homomorphism $G \, hookrightarrow S_4$, and conclude that $G \simeq A_4$.
- Suppose $P_3 \trianglelefteq G$ and $P_2 \simeq Z_4$ but $P_2 \, /triangleleftG$. Write $P_2 = \langle x \rangle$ and $P_3 = \langle y \rangle$ and show that $xyx^{-1} = y^{-1}$, then show that this uniquely determines the Cayley table of G, with presentation
$$G \simeq \langle x, y \mid x^4 = y^3 = 1, xyx^{-1} = y^{-1} \rangle.$$
- Finally, suppose $P_3 \trianglelefteq G$ and $P_2 \simeq Z_2 \times Z_2$ but $P_2 \not\trianglelefteq G$. Writing $P_3 = \langle y \rangle$, show that $P_2 = \, langlex_1\rangle \times \langle x_2 \rangle$ for some $x_1, x_2 \in P_2$ with $x_1 y x_1^{-1} = y$ and $x_2 y x_2^{-1} = y^{-1}$. Conclude that $x_1 y$ has order 6 and then that $G \simeq D_{12}$, the dihedral group of order 12.

(k) Give a table of groups of order $n \leq 15$ up to isomorphism (DF, section 5.3, p. 168), giving the answer even if you don't do (10).

(l) As an application, identify in the table the three groups $G_1 = Z_2 \times D_6$,
$$G_2 := \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbb{Z}/2\mathbb{Z} \right\} \leq \mathrm{GL}_3(\mathbb{Z}/2\mathbb{Z})$$
and $G_3 = S/Z(S)$ where
$$S = \mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}/3\mathbb{Z} \text{ and } ad - bc = 1 \right\} \leq \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}).$$