Math 128A, problem set 02
Outline due: Mon Aug 31
Due: Wed Sep 02
Last revision due: Mon Oct 19
(Problem 2(b) modified Tue Sep 22)

Problems to be done, but not turned in: (Ch. 2) 1–51 odd; (Ch. 3) 1–17 odd.
Fun: (Ch. 2) 39, 48 (should be "multiple of 4").

Problems to be turned in:

1. Let G be a group and $a, b, t \in G$ be elements such that $t^{-1}at = b^{-1}$. Prove that for any integer $n > 0$, $a^n t b^n = t$. Does this extend to $n < 0$? Prove or disprove.

2. We can describe/define a group as a purely algebraic object by using what is known as a *presentation*. For example, we can define

$$G_6 = \left\langle R, F \mid F^2 = e,\ R^6 = e,\ FRF = R^{-1} \right\rangle . \qquad (*)$$

This means that:

- The elements of G_6 are all possible *words* in R, F, and e, i.e., all possible algebraic expressions in powers of R, F, and e, like $R^7F^{-1}R^2F^6$ or $F^{-2}RF^3$ or e.
- We multiply two words by *concatenation*, e.g.,

$$(R^7F^{-1}R^2F^6) \cdot (F^{-2}RF^3) = R^7F^{-1}R^2F^6F^{-2}RF^3.$$

- Two words are equal exactly when they can be proven to be equal as a result of the rules in (*) and rules that hold for all possible groups, like $FF^{-1} = e$, $R^kR^n = R^{k+n}$ (the "laws of exponents"), and $eg = g$ for any $g \in G_6$. In practice, this means that you use (*) to simplify words in R, F, and e as much as possible. For example,

$$\begin{aligned} R^7F^{-1}R^2F^6F^{-2}RF^3 &= R^6RF^{-1}R^2F^3FRFF^2 && \text{(laws of exponents)} \\ &= eRF^{-1}R^2F^3FRFe && (R^6 = e,\ F^2 = e) \\ &= RF^{-1}R^2F^3FRF && (e \text{ is identity}) \\ &= RF^{-1}R^2F^3R^{-1}, && (FRF = R^{-1}) \end{aligned}$$

and so on.

(a) The rule $FRF = R^{-1}$ implies what I call a *move-past* rule, as follows. If we multiply both sides of $FRF = R^{-1}$ on the right by F^{-1}, we get:

$$\begin{aligned} FRFF^{-1} &= R^{-1}F^{-1}, \\ FR &= R^{-1}F^{-1}. \end{aligned}$$

In other words, if we have an F on the left-hand side of an R, we can move the F to the right of the R, at the cost of inverting both the F and the R.
There are three other move-past rules, of the form $F^{\pm 1}R^{\pm 1} = R^{?}F^{?}$. Figure out what those rules are and prove them as a consequence of $FRF = R^{-1}$.

(b) Explain how the move-past rules imply that every element of G_6 is equal to a word of the form $R^n F^k$ for some $n, k \in \mathbf{Z}$.

Alternative problem: Carefully prove that $FR^3F^{-1}R^{-5}F^7R^2 = R^nF^k$ for some $n, k \in \mathbf{Z}$, using the move-past rules. (The same ideas show that something similar works for any word in R and F, though explaining that fact is more complicated.)

3. Construct a Cayley table for $U(20)$.

4. (Ch. 2) 46. (To prove this is a group, you can use known facts about 3×3 matrix multiplication, which is the operation here; the most interesting part is the inverse axiom.)

5. Let G be a group and $a \in G$, and suppose that $a^{10} = e$. What could the value of $|a|$ be? Explain your answer in terms of the definition of the order of an element.

6. Suppose H is a subgroup of $\mathbf{Z}$ under addition, and H contains 14 and 35. What are the possibilities for H? Prove your answer.