Nathan Bickel
MATH 701: Section 001
Professor: Dr. Tsai
October 16, 2024

MATH 701 Homework 4

Problem 2.1.3 Show that the following subsets of the dihedral group D_8 are actually subgroups:

(a) $\{1, r^2, s, sr^2\}$

(b) $\{1, r^2, sr, sr^3\}$

(a) We write the operation table:

$\cdot$	1	r^2	s	sr^2
1	1	r^2	s	sr^2
r^2	r^2	1	sr^2	s
s	s	sr^2	1	r^2
sr^2	sr^2	s	r^2	1

Here, we have $sr^2sr^2 = 1$ because we can use $rs = sr^{-1}$ to write

$$sr^2sr^2 = srsr^{-1}r^2 = srsr = ssr^{-1}r = ss = 1.$$

The other entries are obtained similarly. Since each element is its own identity, the set contains 1, and all entries are in the set, the set is a subset.

(b) We write the operation table:

$\cdot$	1	r^2	sr	sr^3
1	1	r^2	sr	sr^3
r^2	r^2	1	sr^3	sr
sr	sr	sr^3	1	r^2
sr^3	sr^3	sr	r^2	1

The set is a subgroup by the same reasoning as (a).

Problem 2.1.4 Give an explicit example of a group G and an infinite subset H of G that is closed under the group operation but is not a subgroup of G.

Let $G = (\mathbb{Z}, +)$ and let H be the subset of positive integers. Then H is infinite and is closed under addition, but it is not a subgroup of G since the identity is not in G.

Problem 2.1.5 Prove that G cannot have a subgroup H with $|H| = n - 1$, where $n = |G| > 2$.

For any $n > 2$, any divisors d other than n will have $d \leq \frac{n}{2} < n - 1$. Thus, by Lagrange's theorem, no subgroup can have size $n - 1$.

Problem 2.1.6 Let G be an abelian group. Prove that $\{g \in G \mid |g| < \infty\}$ is a subgroup of G (called the torsion subgroup of G). Give an explicit example where this set is not a subgroup when G is non-abelian.

Let a, b in the defined set. Then we have $|a| < \infty$ and $|b| < \infty$. Then since G is abelian, we have

$$(ab^{-1})^{|a||b|} = a^{|a||b|}(b^{-1})^{|a||b|} = a^{|a||b|}(b^{|a||b|})^{-1} = 1 \cdot 1^{-1} = 1.$$

Thus, we have $|ab^{-1}| \leq |a||b|$, so it is finite and thus ab^{-1} is in the set. Thus, the set is a subgroup of G.

An example of a non-abelian group that does not have a torsion subgroup is $GL_2(\mathbb{Z})$. In particular, we have that

$$\begin{pmatrix} -1 & 0 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 2 \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{Z})$$

both with order 2, but it is straightforward to prove with induction that

$$\begin{pmatrix} -1 & 0 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} -1 & 2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -2 \\ -2 & 5 \end{pmatrix}$$

does not have finite order. Thus, the set does not satisfy closure and is therefore not a subgroup.

Problem 2.1.8 Let H and K be subgroups of G. Prove that $H \cup K$ is a subgroup if and only if either $H \subseteq K$ or $K \subseteq H$.

($\Leftarrow$) If $H \subseteq K$, then $H \cup K = K$, and if $K \subseteq H$, then $H \cup K = H$. In either case, $H \cup K$ is a subgroup of G by the assumption.

($\Rightarrow$) Suppose $H \not\subseteq K$ and $K \not\subseteq H$. Then there exists $h \in H \setminus K$ and $k \in K \setminus H$. Then we have that hk is not in H (if it were, then $h^{-1}hk = k$ would be in H by closure) and hk is not in K (if it were, then $hkk^{-1} = h$ would be in K), so $hk \notin H \cup K$. But then closure does not hold for $H \cup K$, so it is not a subgroup of G. $\square$

Problem 2.1.9 Let $G = GL_n(F)$, where F is any field. Define

$$SL_n(F) = \{A \in GL_n(F) \mid \det(A) = 1\}$$

(called the special linear group). Prove that $SL_n(F) \leq GL_n(F)$.

Let $A, B \in SL_n(F)$. Then $\det(A) = \det(B) = 1$, so

$$\det(B^{-1}) = \det(B^{-1})\det(B) = \det(B^{-1}B) = \det(I) = 1.$$

Thus, we have

$$\det(AB^{-1}) = \det(A)\det(B^{-1}) = 1 \cdot 1 = 1$$

and thus $AB^{-1} \in SL_n(F)$. Since $I \in SL_n(F)$, we have $SL_n(F) \leq GL_n(F)$. $\square$

Problem 2.1.10

(a) Prove that if H and K are subgroups of G then so is their intersection $H \cap K$.

(b) Prove that the intersection of an arbitrary nonempty collection of subgroups of G is again a subgroup of G (do not assume the collection is countable).

(a) Let $a, b \in H \cap K$. Then we have $a, b \in H$ and $a, b \in K$, so $ab^{-1} \in H$ and $ab^{-1} \in K$ since H and K are subgroups. So $ab^{-1} \in H \cap K$. Since $1 \in H$ and $1 \in K$ (H and K are both subgroups), we have $1 \in H \cap K$ and thus $H \cap K \neq \varnothing$. So $H \cap K \leq G$.

(b) Let $\{H_\alpha\}_{\alpha \in I}$ be a nonempty collection of subgroups of G. Let $a, b \in H := \bigcap_{\alpha \in I}\{H_\alpha\}$. Then we have $a, b \in H_\alpha$ for all $\alpha \in I$, so $ab^{-1} \in H_\alpha$ since H_α is a subgroup. So $ab^{-1} \in H$. Since $1 \in H_\alpha$ for all $\alpha \in I$, we have $1 \in H$ and thus $H \neq \varnothing$. Therefore, $H \leq G$. $\square$

Problem 2.1.12 Let A be an abelian group and fix some $n \in \mathbb{Z}$. Prove that the following sets are subgroups of A:

(a) $\{a^n \mid a \in A\}$

(b) $\{a \in A \mid a^n = 1\}$.

(a) Fix $n \in \mathbb{Z}$, and let $H := \{a^n \mid a \in A\}$. Let $a, b \in H$. Then there exist $\alpha, \beta \in A$ such that $a = \alpha^n$ and $b = \beta^n$. We can use this along with A being abelian to write

$$ab^{-1} = \alpha^n(\beta^n)^{-1} = \alpha^n(\beta^{-1})^n = (\alpha\beta^{-1})^n.$$

Thus, since $\alpha\beta^{-1} \in A$, we have $ab^{-1} \in H$. Since $1 = 1^n \in H$, we have $H \neq \varnothing$, so $H \leq A$.

(b) Fix $n \in \mathbb{Z}$, and let $K := \{a \in A \mid a^n = 1\}$. Let $a, b \in K$. Then since A is abelian, we have

$$(ab^{-1})^n = a^n(b^{-1})^n = a^n(b^n)^{-1} = 1 \cdot 1^{-1} = 1,$$

so $ab^{-1} \in K$. Since $1 \in K$, we have $K \neq \varnothing$, so $K \leq A$.

Problem 2.1.15 Let $H_1 \leq H_2 \leq \ldots$ be an ascending chain of subgroups of G. Prove that $\bigcup_{i=1}^{\infty} H_i$ is a subgroup of G.

Let $U := \bigcup_{i=1}^{\infty} H_i$. Let $a, b \in U$. Then for some $k \in \mathbb{N}$, we have that $a \in H_{k'}$ for all $k' \geq k$, and for some $m \in \mathbb{N}$, we have $b \in H_{m'}$ for all $m' \geq m$. Let $n := \max\{k, m\}$. Then $a, b \in H_n$, and since H_n is a subgroup, $ab^{-1} \in H_n$. So $ab^{-1} \in U$, and therefore since U is clearly nonempty, $U \leq G$.

Problem 2.3.3 Find all generators for $\mathbb{Z}/48\mathbb{Z}$.

The generators are the equivalence classes with elements mod 48 coprime to 48. These are the elements in

$$\{\overline{1}, \overline{5}, \overline{7}, \overline{11}, \overline{13}, \overline{17}, \overline{19}, \overline{23}, \overline{25}, \overline{29}, \overline{31}, \overline{35}, \overline{37}, \overline{41}, \overline{43}, \overline{45}, \overline{47}\}.$$

Problem 2.3.4 Find all generators for $\mathbb{Z}/202\mathbb{Z}$.

Since $202 = 2 \cdot 101$, the generators for $\mathbb{Z}/202\mathbb{Z}$ are the odd integers other than $\overline{101}$.

Problem 2.3.12 Prove that the following groups are not cyclic:

(a) $Z_2 \times Z_2$

(b) $Z_2 \times \mathbb{Z}$

(c) $\mathbb{Z} \times \mathbb{Z}$.

(a) Every element in $Z_2 \times Z_2$ has order 1 or 2, but $|Z_2 \times Z_2| = 4$.

(b) Since $Z_2 \times \mathbb{Z}$ has a subgroup isomorphic to $Z_2 \times Z_2$, which is not cyclic from part (a). Therefore, $Z_2 \times \mathbb{Z}$ is not cyclic.

(c) Since $\mathbb{Z} \times \mathbb{Z}$ has a subgroup isomorphic to $Z_2 \times Z_2$, which is not cyclic from part (a). Therefore, $\mathbb{Z} \times \mathbb{Z}$ is not cyclic.

Problem 2.3.13 Prove that the following pairs of groups are not isomorphic.

(a) $\mathbb{Z} \times Z_2$ and $\mathbb{Z}$

(b) $\mathbb{Q} \times Z_2$ and $\mathbb{Q}$.

(a) We have that $\mathbb{Z} \times Z_2$ is not cyclic from (a modification of) Problem 2.3.12b. Since $\mathbb{Z}$ is cyclic, the groups are not isomorphic.

(b) We have that $(0, \overline{1})$ has order 2 in $\mathbb{Q} \times Z_2$, but there are no elements in $\mathbb{Q}$ with order 2. Thus, the groups cannot be isomorphic.

Problem 2.3.15 Prove that $\mathbb{Q} \times \mathbb{Q}$ is not cyclic.

It suffices to show that $\mathbb{Q}$ is not cyclic. Suppose (toward contradiction) that $\mathbb{Q}$ is cyclic. Then there exists a generator $x \in \mathbb{Q}$. Then, since $\frac{x}{2} \in \mathbb{Q}$, we have that there exists some $n \in \mathbb{Z}$ such that $\frac{x}{2} = nx$. But then $n = \frac{1}{2} \notin \mathbb{Z}$, a contradiction. Therefore, neither $\mathbb{Q}$ nor $\mathbb{Q} \times \mathbb{Q}$ is cyclic. $\square$

Problem 2.3.21 Let p be an odd prime and let n be a positive integer. Use the Binomial Theorem to show that $(1+p)^{p^{n-1}} \equiv 1 \pmod{p^n}$ but $(1+p)^{p^{n-2}} \not\equiv 1 \pmod{p^n}$. Deduce that $1+p$ is an element of order p^{n-1} in the multiplicative group $(\mathbb{Z}/p^n\mathbb{Z})^\times$.

We proceed with induction on n to show that $(1+p)^{p^{n-1}} \equiv 1 \pmod{p^n}$. For $n = 1$ we have

$$(1+p)^{p^{1-1}} = (1+p)^{p^0} = 1 + p \equiv 1 \pmod{p^1}.$$

Now let $n \in \mathbb{N}$, $n > 1$, and suppose that $(1+p)^{p^{n-2}} \equiv 1 \pmod{p^{n-1}}$. Then, there exists some $m \in \mathbb{Z}$ such that $(1+p)^{p^{n-2}} = 1 + mp^{n-1}$, so we can write

$$\begin{aligned}
(1+p)^{p^{n-1}} &= \left((1+p)^{p^{n-2}}\right)^p \\
&= (1 + mp^{n-1})^p && \text{(by IH)} \\
&= \sum_{k=0}^{p} \binom{p}{k} (mp^{n-1})^k && \text{(binomial theorem)} \\
&= \binom{p}{0}\left(mp^{n-1}\right)^0 + \binom{p}{1}\left(mp^{n-1}\right)^1 + \sum_{k=2}^{p} \binom{p}{k}\left(mp^{n-1}\right)^k && \text{(splitting sum)} \\
&= 1 + mp^n + \sum_{k=2}^{p} \binom{p}{k} m^k \left(p^{n-1}\right)^k \\
&= 1 + mp^n + \left(p^{n-1}\right)^2 \sum_{k=2}^{p} \binom{p}{k} m^k \left(p^{n-1}\right)^{k-2} && \text{(factoring)} \\
&= 1 + mp^n + (p^n)\left(p^{n-2}\right) \sum_{k=2}^{p} \binom{p}{k} m^k \left(p^{n-1}\right)^{k-2}
\end{aligned}$$

$$
\begin{aligned}
&= 1 + p^n \left[m + p^{n-2} \sum_{k=2}^{p} \binom{p}{k} m^k \left(p^{n-1}\right)^{k-2} \right] \\
&\equiv 1 \pmod{p^n}.
\end{aligned}
$$

We now use induction to show that $(1+p)^{p^{n-2}} \equiv 1 + p^{n-1} \pmod{p^n}$. For the base case, we have that

$$(1+p)^{p^{2-2}} = (1+p)^1 = 1 + p = 1 + p^{2-1},$$

so the claim holds for $n = 2$. Now, let $n \in \mathbb{N}$, $n > 2$, and suppose that $(1+p)^{p^{n-3}} \equiv 1 + p^{n-2} \pmod{p^{n-1}}$. Then, there exists $m \in \mathbb{Z}$ such that $(1+p)^{p^{n-3}} = 1 + p^{n-2} + mp^{n-1}$. Then, we can write

$$
\begin{aligned}
(1+p)^{p^{n-2}} &= \left((1+p)^{p^{n-3}}\right)^p \\
&= \left(1 + p^{n-2} + mp^{n-1}\right)^p \\
&= \left(1 + p^{n-2}(1+mp)\right)^p \\
&= \sum_{k=0}^{p} \binom{p}{k} \left(p^{n-2}\right)^k (1+mp)^k \\
&= \binom{p}{0} \left(p^{n-2}\right)^0 (1+mp)^0 + \binom{p}{1} \left(p^{n-2}\right)^1 (1+mp)^1 + \sum_{k=2}^{p} \binom{p}{k} \left(p^{n-2}\right)^k (1+mp)^k \\
&= 1 + p\left(p^{n-2}\right)(1+mp) + \sum_{k=2}^{p} \binom{p}{k} \left(p^{n-2}\right)^k (1+mp)^k \\
&= 1 + p^{n-1} + mp^n + \left(p^{n-2}\right)^2 \sum_{k=2}^{p} \binom{p}{k} \left(p^{n-2}\right)^{k-2} (1+mp)^k \\
&= 1 + p^{n-1} + mp^n + (p^n)\left(p^{n-2}\right) \sum_{k=2}^{p} \binom{p}{k} \left(p^{n-2}\right)^{k-2} (1+mp)^k \\
&= 1 + p^{n-1} + p^n \left[m + p^{n-2} \sum_{k=2}^{p} \binom{p}{k} \left(p^{n-2}\right)^{k-2} (1+mp)^k \right] \\
&\equiv 1 + p^{n-1} \pmod{p^n}.
\end{aligned}
$$

Since $1 + p^{n-1} < p^n$, this shows that $(1+p)^{p^{n-2}} \not\equiv 1 \pmod{p^n}$.

We have shown in the first induction proof that $1+p$ has order at most p^{n-1}. Suppose $1+p$ has order $a < p^{n-1}$. We must have that $a | p^{n-1}$, so there exists some k such that $a = p^k$ since p is prime, and since $a < p^{n-1}$ we must have $k \le n-2$. Then we have $n - k - 2 \ge 0$, so we can write

$$(1+p)^{p^{n-2}} = (1+p)^{p^{k+n-k-2}} = \left((1+p)^{p^k}\right)^{p^{n-k-2}} \equiv 1^{p^{n-k-2}} = 1 \pmod{p^n},$$

contradicting the second induction proof. So $1+p$ has order $n-1$. □

Problem 2.4.13 Prove that the multiplicative group of positive rational numbers is generated by the set $\left\{\frac{1}{p} \mid p \text{ is a prime}\right\}$.

Let $x \in \mathbb{Q}$. Then $x = \frac{a}{b}$ for some $a, b \in \mathbb{N}$. By the fundamental theorem of algebra, there exist primes $\alpha_1, \dots, \alpha_k$ and $\beta_1, \dots, \beta_\ell$ and powers $m_1, \dots, m_k$ and $n_1, \dots, n_\ell$ such that $a = \alpha_1^{m_1} \cdots \alpha_k^{m_k}$ and

$b = \beta_1^{n_1} \cdots \beta_\ell^{n_\ell}$. Then, we have

$$x = \left(\frac{1}{\alpha_1}\right)^{-m_1} \cdots \left(\frac{1}{\alpha_k}\right)^{-m_k} \cdot \left(\frac{1}{\beta_1}\right)^{n_1} \cdots \left(\frac{1}{\beta_\ell}\right)^{n_\ell},$$

so x is generated by the set.

Problem 2.4.14 A group H is called finitely generated if there is a finite set A such that $H = \langle A \rangle$.

(a) Prove that every finite group is finitely generated.

(b) Prove that $\mathbb{Z}$ is finitely generated.

(c) Prove that every finitely generated subgroup of the additive group $\mathbb{Q}$ is cyclic.

(d) Prove that $\mathbb{Q}$ is not finitely generated.

(a) Every group G has $G = \langle G \rangle$, so if G is finite, G is finitely generated.

(b) We have that $\mathbb{Z} = \langle \overline{1} \rangle$.

(c) Let H be a finitely generated subgroup of $\mathbb{Q}$, and let A be a finite set that generated H. So $A = \{x_1, \ldots, x_n\} \subset \mathbb{Q}$. Then for each i, there exist $a_i, b_i \in \mathbb{R}$ such that $x_i = \frac{a_i}{b_i}$. Let $x = \frac{1}{b_1 b_2 \cdots b_n}$. Then for all i, we have

$$x_i = \frac{a_i}{b_i} = a_i \left(\frac{b_1 \cdots b_{i-1} \cdot b_{i+1} \cdots b_n}{b_1 \cdots b_n} \right) = x(a_i \cdot b_1 \cdots b_{i-1} \cdot b_{i+1} \cdots b_n),$$

so every element of A can be written as a power of x. Therefore, $H = \langle x \rangle$, so H is cyclic.

(d) If $\mathbb{Q}$ were finitely generated, then $\mathbb{Q}$ would be a finitely generated subgroup of $\mathbb{Q}$, so by part (c) $\mathbb{Q}$ would be cyclic. But $\mathbb{Q}$ is not cyclic as shown in Problem 2.3.15, so $\mathbb{Q}$ is not finitely generated.