Math 393: Homework 2

Anthony Brice

October 4, 2016

Exercise 4.6

$$
\begin{aligned}
\langle 0 \rangle &= \{0\} \\
\langle 1 \rangle &= \mathbb{Z}_{12} \\
\langle 2 \rangle &= \{0, 2, 4, 6, 8, 10\} \\
\langle 3 \rangle &= \{0, 3, 6, 9\} \\
\langle 4 \rangle &= \{0, 4, 8\} \\
\langle 5 \rangle &= \mathbb{Z}_{12} \\
\langle 6 \rangle &= \{0, 6\} \\
\langle 7 \rangle &= \mathbb{Z}_{12} \\
\langle 8 \rangle &= \langle 4 \rangle \\
\langle 9 \rangle &= \langle 3 \rangle \\
\langle 10 \rangle &= \langle 2 \rangle \\
\langle 11 \rangle &= \mathbb{Z}_{12} \,.
\end{aligned}
$$

Figures 1–6 exhibit each visually.

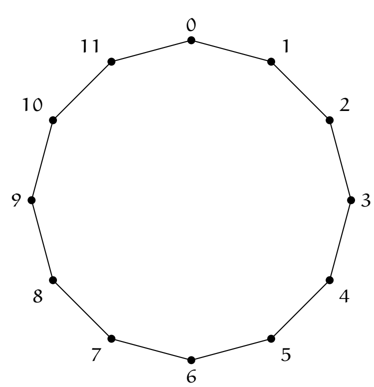

Figure 1: A visual representation of $\mathbb{Z}_{12} = \langle 1 \rangle = \langle 5 \rangle = \langle 7 \rangle = \langle 11 \rangle$.

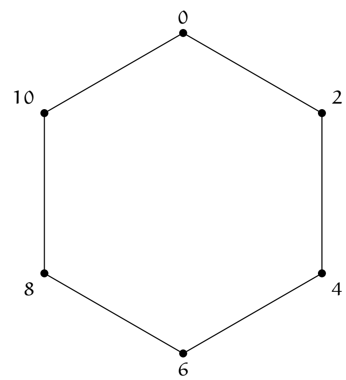

Figure 2: A visual representation of $\langle 2 \rangle = \langle 10 \rangle$.

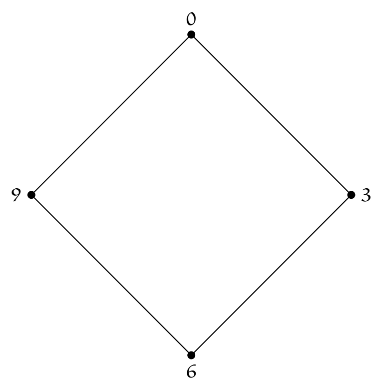

Figure 3: A visual representation of $\langle 3 \rangle = \langle 9 \rangle$.

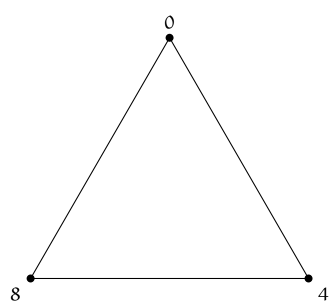

Figure 4: A visual representation of $\langle 4 \rangle = \langle 8 \rangle$.

Figure 5: A visual representation of $\langle 6 \rangle$.

Figure 6: A visual representation of $\langle 0 \rangle$.

Exercise 4.8

Claim. The cyclic subgroups of D_6 are exactly

$$\begin{aligned}
\langle s_n \rangle &= \{s_n, r_0\}, && \forall n \in \{0, 1, \ldots, 5\} \\
\langle r_1 \rangle &= \{r_0, r_1, r_2, r_3, r_4, r_5\} \\
\langle r_2 \rangle &= \{r_0, r_2, r_4\} \\
\langle r_3 \rangle &= \{r_0, r_3\} \\
\langle r_0 \rangle &= \{r_0\}.
\end{aligned}$$

Proof. Since a cyclic subgroup by definition must generate from a single element in the group, there exist at most 12 cyclic groups of D_6. Then we need only verify that $\langle r_4 \rangle$ and $\langle r_5 \rangle$ are already included in the above list. We have that $\langle r_4 \rangle = \langle r_2 \rangle$ and $\langle r_5 \rangle = \langle r_1 \rangle$. □

Exercise 4.12

Claim. Let a be an element of a group G of order n. Then the positive integer k satisfying $a^k = a^{-1}$ is defined by $k = |a|t - 1$ for all $t \in \mathbb{Z}_{>0}$ satisfying $a^{|a|t} = e$.

Proof.

$$\begin{aligned}
& a^k = a^{-1} \\
\iff \quad & aa^k = aa^{-1} \\
\iff \quad & a^{k+1} = e\,.
\end{aligned}$$

Thus $|a|$ divides $k+1$ and $k+1 = |a|t$ for some $t \in \mathbb{Z}$ (by Corollary 4.14). Then $k = |a|t - 1$. □

Exercise 4.19

Part a)

Claim. Let $GL_n(\mathbb{Z})$ be the set of all $n \times n$ matrices having integer entries and having determinant equal to 1 or -1. Then $GL_n(\mathbb{Z})$ is a subgroup of $GL_n(\mathbb{R})$.

Proof. We will show that $GL_n(\mathbb{Z})$ satisfies all three conditions of Proposition 4.3.

Let $A, B \in GL_n(\mathbb{Z})$. Then $AB = C$ must be integer valued, and $\det(C)$ must be 1 or -1 since $\det(AB) = \det(A)\det(B)$. Then $C \in GL_n(\mathbb{Z})$, and $GL_n(\mathbb{Z})$ is closed under our operation, satisfying the first condition.

Clearly the identity matrix $I \in GL_n(\mathbb{Z})$, satisfying the second condition.

Consider $A \in GL_n(\mathbb{Z})$. We have that $\det(A^{-1}) = 1/\det(A) = 1$ or -1, and since $\det(A) = 1$ or -1 we also have that A^{-1} is integer valued. Then $A^{-1} \in GL_n(\mathbb{Z})$, satisfying the third condition. □

Part b)

Claim. Let $SL_n(\mathbb{Z})$ be the set of all $n \times n$ matrices having integer entries and having determinant equal to 1. Then $SL_n(\mathbb{Z})$ is a subgroup of $GL_n(\mathbb{Z})$.

Proof. Let $A, B \in SL_n(\mathbb{Z})$. Then $AB = C$ must be integer valued, and since

$$\begin{aligned} \det(C) &= \det(AB) \\ &= \det(A)\det(B) \\ &= 1, \end{aligned}$$

C must be in $SL_n(\mathbb{Z})$.

Clearly $I \in SL_n(\mathbb{Z})$.

Consider $A \in SL_n(\mathbb{Z})$. We have that

$$\det(A^{-1}) = \frac{1}{\det(A)} = 1.$$

And since $\det(A) = 1$, A^{-1} must also be integer valued. Thus $A^{-1} \in SL_n(\mathbb{Z})$. □

Part c)

Claim. Let S be the subset of $GL_n(\mathbb{R})$ consisting of all $n \times n$ matrices having integer entries. Then matrix multiplication does not define a group operation on S.

Proof. Assume for the purpose of contradiction that matrix multiplication does define a group operation on S. Then S is a subgroup of $GL_n(\mathbb{R})$.

Let $A \in S$ be an integer-valued matrix with determinant not equal 1 or -1. Then A^{-1} is not integer valued yet A^{-1} must be in S, thus we have a contradiction. □

Exercise 4.23

Claim. Let H be a finite subset of group G. Then H is a subgroup of G if and only if

(i) If a and b lie in H, then ab lies in H,

(ii) H is nonempty.

Proof. Let H be a finite subgroup of G. Then if $a, b \in H$ then $ab \in H$ by condition (1) of the subgroup test, and H is nonempty by condition (2).

Now let H be a finite subset of group G, and assume that H is nonempty and that if $a, b \in H$ then $ab \in H$. We will show that there exists an identity element $e \in H$ and for all a there exists $a^{-1} \in H$. Since H is finite we have that $a^m = a^k$ where $m \neq k$. Let $m > k$, then $a^{m-k} = e$. Then $aa^{m-k-1} = e$, thus $a^{m-k-1} = a^{-1}$. □

Exercise 5.2

Part a)

Since the groups are finite and commutative,

$$\begin{aligned}\langle 3,5\rangle \in U_{16} &= \{3^n 5^m : n, m \in \mathbb{Z}\}\\ &= \{3^0 5^0, 3^0 5^1, \ldots, 3^1 5^0, 3^1 5^1, \ldots\}\\ &= U_{16}\,.\end{aligned}$$

$$\begin{aligned}\langle 9,15\rangle \in U_{16} &= \{9^n 15^m : n, m \in \mathbb{Z}\}\\ &= \{9^0 15^0, 9^0 15^1, \ldots, 9^1 15^0, 9^1 15^1, \ldots\}\\ &= \{1,7,9,15\}\,.\end{aligned}$$

Part b)

$$\langle r_4, s_0\rangle \in D_8 = \{r_0, r_4, s_0, s_4\}\,.$$

$$\langle r_2, s_0\rangle \in D_8 = D_8\,.$$

Part c)

Exercise 5.3

Claim. U_{14} is cyclic.

Proof. It suffices to show that $\langle a\rangle = U_{14}$ for some $a \in U_{14}$.

$$\langle 3\rangle = \{1,3,5,9,11,13\}\,.$$ □

Claim. U_{15} is not cyclic.

Proof. It suffices to show that $\langle a\rangle \neq U_{15}$ for all $a \in U_{15}$.

$$\begin{aligned}\langle 1\rangle &= \{1\}\\ \langle 2\rangle &= \{1,2,4,8\}\\ \langle 4\rangle &= \{1,4\}\\ \langle 6\rangle &= \{1,6\}\\ \langle 7\rangle &= \{1,4,7,13\}\\ \langle 8\rangle &= \{1,2,4,8\}\\ \langle 11\rangle &= \{1,11\}\\ \langle 13\rangle &= \{1,4,7,13\}\\ \langle 14\rangle &= \{1,14\}\,.\end{aligned}$$ □

Exercise 5.5

Part a)

Claim. $\langle a, b\rangle = \langle \gcd(a, b)\rangle$ for any $a, b \in \mathbb{Z}$.

Proof. Note that addition is commutative, so

$$\begin{aligned}\langle a, b\rangle &= \{a^n b^m : n, m \in \mathbb{Z}\}\\ &= \{na + mb : n, m \in \mathbb{Z}\}.\end{aligned}$$

Note that since $\gcd(a, b)$ divides any linear combination of a and b, $\gcd(a, b)$ must be the smallest positive linear combination of a and b. Thus $\langle \gcd(a, b)\rangle = \langle a, b\rangle$. □

Part b)

Claim. $\langle a, b\rangle = \langle \gcd(a, b, n)\rangle$ for any $a, b, \in \mathbb{Z}_n$.

Proof. Addition modulo n is still commutative, so

$$\begin{aligned}\langle a, b\rangle &= \{a^p b^q : p, q \in \mathbb{Z}\}\\ &= \{pa + qb \bmod n : p, q \in \mathbb{Z}\}\end{aligned}$$

Then let $c = \gcd(a, b, n)$. *TODO:* Show that any $pa + qb$ can be expressed as rc and vice versa. □

Exercise 5.7

Part a)

Claim. $\langle a, b\rangle = \langle a^{-1}, b\rangle$.

Proof.

$$\begin{aligned}\langle a, b\rangle &= \{s_1^{n_1} s_2^{n_2} \cdots s_k^{n_k} : s_i \in \{a, b\}, n_i \in \mathbb{Z}_{\neq 0}\}\\ &= \langle a^{-1}, b\rangle\end{aligned}$$

since $\{a^{n_i} : n_i \in \mathbb{Z}_{\neq 0}\} = \{(a^{-1})^{n_i} : n_i \in \mathbb{Z}_{\neq 0}\}$. □

Part b)

Claim. $\langle a, b\rangle = \langle a, a^{-1}b\rangle$.

Proof. Similar to the proof above, note that one may map any expression for the elements of $\langle a, b\rangle$ of the form given in Proposition 5.5 to an equivalent expression for the elements of $\langle a, a^{-1}b\rangle$ by replacing each b in the first expression with $aa^{-1}b$. Since the mapped expression satisfies for $\langle a, a^{-1}b\rangle$ the form given in Proposition 5.5, and because this map forms a bijection by mapping any expression for an element of $\langle a, a^{-1}b\rangle$ that does not include $aa^{-1}b$ to itself, $\langle a, b\rangle = \langle a, a^{-1}b\rangle$. □

Part c)

Claim. $\langle a, b\rangle = \langle a, ab\rangle$.

Proof. As above, we can create a bijection from the expressions generated by $\langle a, b\rangle$ to equivalent elements generated by $\langle a, ab\rangle$ by replacing every b with $a^{-1}ab$ and vice versa, and mapping any expression in $\langle a, b\rangle$ that does not have b to itself and any expression in $\langle a, ab\rangle$ that does not have $a^{-1}ab$ to itself. Thus $\langle a, b\rangle = \langle a, ab\rangle$. $\square$