Algebra I

Homework 1

Nutan Nepal

September 10, 2022

(1.3 - 13) Show that an element has order 2 in S_n if and only if its cycle decomposition is a product of commuting 2-cycles.

(1.4 - 11) Let $H(F) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in F \right\}$ be called the Heisenberg group over F. Let $X = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$ and $Y = \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix}$ be elements of $H(F)$.

(a) Compute the matrix product XY and deduce that $H(F)$ is closed under matrix multiplication. Exhibit explicit matrices such that $XY \neq YX$ (so that $H(F)$ is always non-abelian).

$XY = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+d & e+af+b \\ 0 & 1 & f+c \\ 0 & 0 & 1 \end{pmatrix}$. Hence $H(F)$ is closed under matrix multiplication.

Let $X = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ and $Y = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$. Then $XY = \begin{pmatrix} 1 & 1 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$ and $YX = \begin{pmatrix} 1 & 1 & 2 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$. Hence we see that $XY \neq YX$.

(b) Find an explicit formula for the matrix inverse X^{-1} and deduce that $H(F)$ is closed under inverses.

Let Y be the inverse of X with their respective entries from previous exercise. Then

$$a + d = 0, \ f + c = 0, \ e + af + b = 0$$

Solving these equations gives us

$$X^{-1} = \begin{pmatrix} 1 & -a & ac - b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix}$$

Since X^{-1} is also an upper triangular matrix, $H(F)$ is closed under inverses.

(c) Prove the associative law for $H(F)$ and deduce that $H(F)$ is a group of order $|F|^3$. (Do not assume that matrix multiplication is associative.)

Let $Z = \begin{pmatrix} 1 & g & h \\ 0 & 1 & i \\ 0 & 0 & 1 \end{pmatrix}$. Then

$$\begin{aligned}
(XY)Z &= \left[\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix}\right] \cdot \begin{pmatrix} 1 & g & h \\ 0 & 1 & i \\ 0 & 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & a+d & e+af+b \\ 0 & 1 & f+c \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & g & h \\ 0 & 1 & i \\ 0 & 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & a+d+g & h+ai+di+e+af+b \\ 0 & 1 & c+f+i \\ 0 & 0 & 1 \end{pmatrix}
\end{aligned}$$

and

$$\begin{aligned}
X(YZ) &= \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \cdot \left[\begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & g & h \\ 0 & 1 & i \\ 0 & 0 & 1 \end{pmatrix}\right] \\
&= \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & d+g & h+di+e \\ 0 & 1 & f+i \\ 0 & 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & a+d+g & h+ai+di+e+af+b \\ 0 & 1 & c+f+i \\ 0 & 0 & 1 \end{pmatrix}.
\end{aligned}$$

Hence, $H(F)$ is associative and is a subgroup of $GL_3(F)$. If the order of F is finite. Then for $X \in H(F)$ each $a, \ b, \ c$ has $|F|$ choices. So, $|H(F)| = |F|^3$.

(d) Find the order of each element of the finite group $H(\mathbb{Z}/2\mathbb{Z})$.

There are $2^3 = 8$ elements in the group $H(\mathbb{Z}/2\mathbb{Z})$ which are given below with their orders:

$$e = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad |e| = 1$$

$$x_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad x_1^2 = e \Longrightarrow |x_1| = 2$$

$$x_2 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad x_2^2 = e \Longrightarrow |x_2| = 2$$

$$x_3 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad x_3^2 = e \Longrightarrow |x_3| = 2$$

$$x_4 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad x_4^2 = e \Longrightarrow |x_4| = 2$$

$$x_5 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad x_5^2 = e \Longrightarrow |x_5| = 2$$

$$x_6 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad x_6^4 = e \Longrightarrow |x_6| = 4$$

$$x_7 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad x_7^4 = e \Longrightarrow |x_7| = 4$$

(e) Prove that every nonidentity element of the group $H(\mathbb{R})$ has infinite order.

(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) $S_1 = \{a^n : \ a \in A\}$

(b) $S_2 = \{a \in A : \ a^n = 1\}$

(2.2 - 10) Let H be a subgroup of order 2 in G. Show that $N_G(H) = C_G(H)$. Deduce that if $N_G(H) = G$ then $H \leq Z(G)$.

(2.3 - 16) Assume $|x| = n$ and $|y| = m$. Suppose that x and y commute: $xy = yx$. Prove that $|xy|$ divides the least common multiple of m and n. Need this be true if x and y do not commute? Give an example of commuting elements x, y such that the order of xy is not equal to the least common multiple of $|x|$ and $|y|$.

(2.3 - 23) Show that $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is not cyclic for any $n \geq 3$. [Find two distinct subgroups of order 2.]

(2.4 - 9) Prove that $SL_2(\mathbb{F}_3)$ is the subgroup of $GL_2(\mathbb{F}_3)$ generated by $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$. [Recall from Exercise 9 of Section 1 that $SL_2(\mathbb{F}_3)$ is the subgroup of matrices of determinant 1. You may assume this subgroup has order 24 - this will be an exercise in Section 3.2.]

(3.1 - 17) Let G be the dihedral group of order 16 (whose lattice appears in Section 2.5):

$$G = \langle r, s : \ r^8 = s^2 = 1, rs = sr^{-1} \rangle$$

and let $\overline{G} = G \backslash \langle r^4 \rangle$ be the quotient of G by the subgroup generated by $\langle r^4 \rangle$ (this subgroup is the center of G, hence is normal).

(a) Show that the order of $\overline{G}$ is 8.

Since $\langle r^4 \rangle = \{1, r^4\}$, $|\langle r^4 \rangle| = 2$. Then by Lagrange's theorem,

$$|\overline{G}| = \frac{|G|}{|\langle r^4 \rangle|} = 8.$$

(b) Exhibit each element of $\overline{G}$ in the form $\overline{s}^a \overline{r}^b$, for some integers a and b.

The elements of $\overline{G}$ are $\overline{1}$, $\overline{r}$, $\overline{r}^2$, $\overline{r}^3$, $\overline{s}$, $\overline{s}.\overline{r}$, $\overline{s}.\overline{r}^2$, $\overline{s}.\overline{r}^3$.

(c) Find the order of each of the elements of $\overline{G}$ exhibited in (b).

(d) Write each of the following elements of $\overline{G}$ in the form $\overline{s}^a \overline{r}^b$, for some integers a and b as in (b): $\overline{rs}, \overline{sr^{-2}s}, \overline{s^{-1}r^{-1}sr}$.

(e) Prove that $\overline{H} = \langle \bar{s}, \overline{r}^2 \rangle$ is a normal subgroup of $\overline{G}$ and $\overline{H}$ is isomorphic to the Klein 4-group. Describe the isomorphism type of the complete preimage of $\overline{H}$ in G.

(f) Find the center of $\overline{G}$ and describe the isomorphism type of $\overline{G} \backslash Z(\overline{G})$.

(3.2 - 4) Show that if $|G| = pq$ for some primes p and q (not necessarily distinct) then either G is abelian or $Z(G) = 1$. [See Exercise 36 in Section 1.]

(3.2 - 16) Use Lagrange's Theorem in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ to prove Fermat's Little Theorem: if p is a prime then $a^p \equiv a \mod p$ for all $a \in \mathbb{Z}$.

We first note that $|(\mathbb{Z}/p\mathbb{Z})| = p - 1$ by Euler's totient function.