Exercise 1

Holo

Friday 19th January, 2024

Exercise 1.

Part 1.1.

There is no identity element.

Part 1.2.

It is a group, whose identity is 1 and inverse of x is $\frac{1}{x}$.

Part 1.3.

There is no inverse element to any $x \neq 1, -1$.

Part 1.4.

This is not even a structure (addition is not total on the domain).

Part 1.5.

The identity is 1.

Part 1.6.

The identity is 1 and the inverse of z is $\frac{1}{z}$.

Part 1.7.

This is again not a structure, as multiplication is not total on the domain ($\sqrt{2}\sqrt{2} = 2 \neq \frac{a}{b} + \frac{c}{d}\sqrt{2}$).

Part 1.8.

The identity is I_2 and the inverse of $\begin{pmatrix} x & y \\ -y & x \end{pmatrix}$ is $\frac{1}{x^2+y^2}\begin{pmatrix} x & -y \\ y & x \end{pmatrix}$

Part 1.9.

The identity is the identity function, and the inverse of f is the unique function g such that $g(f(x)) = x$

Exercise 2.

Part 2.1.

$\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ is the left identity, indeed $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} x \cdot 1 + 0 \cdot 1 & 0 \cdot 1 + y \cdot 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix}$

Part 2.2.

The right inverse of $\begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix}$ is $\begin{pmatrix} \frac{1}{x} & \frac{1}{x} \\ 0 & 0 \end{pmatrix}$

Part 2.3.

We saw at class that given a group H, the left identity is always the identity, so if G were to be a group, then $\begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix}$, but this is absurd.

Exercise 3.

Part 3.1.

If G is Abelian then $a^2b^2 = aabb = abab = (ab)^2$.
If G satisfy this equality, then given a, b we have $aabb = abab \implies a^{-1}aabb = a^{-1}abab \implies abbb^{-1} = babb^{-1} \implies ab = ba$

To see an example, let $G = D_4$ and chose a to be 90° rotation and b to be rotation through the y-axis.

Then $a^2b^2 = a^2$ =rotation by 180° but $(ab)^2 = e$

Part 3.2.

If G is such group then $(ab)^2 = e = ee = a^2b^2$, and by exercise 3.1 it is an Abelian group.

Part 3.3.

The only non trivial vector space axioms are the distributivity axioms. (I will use $+$ for the group operator as accustomed in vector spaces)
Let $g, h \in G$ then $0(g + h) = e = e + e = 0g + 0h$ and $1(g + h) = e + (g + h) = g + h = (e + g) + (e + h) = 1g + 1h$.
Let $g \in G$, then $g = 1g = (1 + 0)g = (1 + 0)g$ and $1g + 0g = g + e = e + g = g$. Symmetric argument works for $0 + 1$. The $0 + 0$ case is trivial. Lastly $(1 + 1)g = 0g = e$ and $e = g + g = 1g + 1g$

Exercise 4.

Part 4.1.

Assume that $x^k = x^m$ for $0 \leq k < m < n, \ell = m - k$, then in particular $e = x^0 = x^{k-k} = x^{m-k} = x^\ell$ because multiplying by x^{-1} is a an injective function. But that means that $|x| = \ell < n$, contradiction. And clearly, if $y \in \langle x \rangle$, then $y = x^p$ for some $p \in \mathbb{Z}$, because $x^{-1} = x^{n-1}$, we can assume $p \in \mathbb{N}$, but we have that $x^p = x^{p \mod n}$, so $y \in \{e, x, \ldots, x^{n-1}\}$, hence $|\langle x \rangle| = |x|$.

Part 4.2.

Given $n < m$, assume $n \geq 0$ then if $x^n = x^m$ then, just like before, we can multiple by x^{-1} n-times to show that $e = x^{m-n} \implies x = x^{m-n+1}$, contradict the assumption.

If $n < 0$ then we do the same by instead of multiplying by x^{-1} we multiply by x.

Part 4.3.

Assume that there is no element of order 2.

For each $x \in G \setminus \{e\}$ we look at $\tilde{x} = \{x, x^{-1}\}$, then $G \setminus \{e\} = \bigcup_{x \in G \setminus \{e\}} \tilde{x}$. Because multiplication is injective, those sets are all disjoint then $2n = |G| = 1 + \sum_{0 \leq i < |G \setminus \{e\}|} |\tilde{x}| = 1 + 2k$, contradiction.

Exercise 5.

Part 5.1.

Because the determinate is multiplicative, $SL_n(\mathbb{Z})$ is clearly closed under matrix multiplication, which inherent the associativity.
Clearly $\det(I_n) = 1$, so $SL_n(\mathbb{Z})$ has an identity.
Now if $A \in SL_n(\mathbb{Z})$ then $1 = \det(I_n) = \det(AA^{-1}) = \det(A)\det(A^{-1}) = \det(A^{-1})$, hence every $A \in SL_n(\mathbb{Z})$ has an inverse.

Part 5.2.

For a matrix $A \in GL_n(\mathbb{Z})$ with determinate 1, we know that $\det(A) = \det(A^{-1})$, for A to be invertible in $\mathbb{Z}$ it means that it's inverse also must have only integer values, in particular if we consider a minimal path in Gaussian elimination at no point we multiply a row by anything other than -1, otherwise we would have non-integer enteries in the inverse.

Furthermore, after multiplying a row by -1 or switching 2 rows we must either multiply another row by -1 or switch another 2 rows.

Now let E_+ be the set of elementary matrices that adds 2 rows, and let $E_\times$ be the elementary matrices that multiply a row by -1, and let E_s be the matrices that swap 2 rows, from the argument above the set $E_+ \cup \{ab \mid a, b \in E_\times \cup E_s\}$ generates $SL_n(\mathbb{Z})$, and it is clearly finite.

Part 5.3.

Let $\tilde{S}_n$ be the set of matrices such that each row and column contains exactly one 1. $|\tilde{S}_n|$ is clearly $n!$.
The obviously the inverse of $A \in \tilde{S}_n$ is $A^{\in}\tilde{S}_n$, and a simply plugging in $A, B \in \tilde{S}_n$ to calculate AB shows that $AB \in \tilde{S}_n$.

Part 5.4.

Given a field $\mathbb{F}_p$, a matrix $A \in M_n(\mathbb{F}_p)$ has an inverse if and only if all of it's rows are independent.
In particular we can calculate all possible ways to choose n independent vectors:
The first vector can be anything but $0_{\mathbb{F}_p^n}$, so anything from a choice of $p^n - 1$ elements.
The $(k+1)^{\text{th}}$ vector can be anything that is not a linear combination of the previous rows, there are p^k many possible linear combinations, so there are $p^n - p^k$ possible choices.

Multiplying this all together and we get that $|GL_n(\mathbb{F}_p)| = \prod_{i=0}^{n-1}(p^n - p^i)$