1.3 Symmetric Groups

2) We have that

$$\sigma = (1\ 13\ 5\ 10)(3\ 15\ 8)(4\ 14\ 11\ 7\ 12\ 9)$$

and

$$\tau = (1\ 14)(2\ 9\ 15\ 13\ 4)(3\ 10)(5\ 12\ 7)(8\ 11),$$

thus

$$\sigma\tau = (1\ 13\ 5\ 10)(3\ 15\ 8)(4\ 14\ 11\ 7\ 12\ 9)(1\ 14)(2\ 9\ 15\ 13\ 4)(3\ 10)(5\ 12\ 7)(8\ 11),$$

$$= (1\ 11\ 3)(2\ 4)(5\ 9\ 8\ 7\ 10\ 15)(13\ 14).$$

10) Let σ be an n-cycle and assume indices are taken as their lowest positive residue mod n. We will show by induction that $\sigma^i(a_k) = a_{k+i}$. For $i = 1$, we have by definition that $\sigma(a_k) = a_{k+1}$. Now, assume the induction hypothesis $\sigma^{i-1}(a_k) = a_{k+i-1}$, then $\sigma^i(a_k) = \sigma(\sigma^{i-1}(a_k)) = \sigma(a_{k+i-1}) = a_{k+i}$. ■

15) Fix $\sigma \in S_n$ with disjoint cycle decomposition $\sigma = \sigma_1\sigma_2\cdots\sigma_m$. Let $|\sigma_i|$ divide k, then we have that σ^k fixes the elements in σ_i, and thus the smallest k that fixes the elements of σ_i for all i is the smallest number which is divisible by the orders of all σ_i, thus $k = \text{lcm}(|\sigma_1|, |\sigma_2|, \ldots, |\sigma_m|)$, which is the order of σ. ■

1.4 Matrix Groups

7) We have $p^2 - 1$ choices for the top row of the matrix since it cannot be the zero vector. Fixing the top row, we must choose the bottom row to be linearly independent, thus it cannot be a multiple of the top row, which means we have $p^2 - p$ options for the bottom row. Thus, the total number of 2×2 invertible matrices over $\mathbb{F}_p$ is given by $(p^2-1)(p^2-p) = p^4-p^3-p^2+p$. ■

10a) We have that

$$\begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix} \times \begin{bmatrix} a_2 & b_2 \\ 0 & c_2 \end{bmatrix} = \begin{bmatrix} a_1a_2 & a_1b_2 + b_1c_2 \\ 0 & c_1c_2 \end{bmatrix},$$

and thus G is closed.

10b) We have that

$$\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \times \frac{1}{ac}\begin{bmatrix} c & -b \\ 0 & a \end{bmatrix} = \frac{1}{ac}\begin{bmatrix} ac & 0 \\ 0 & ac \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

and thus G has inverses.

1.6 Homomorphisms and Isomorphisms

3) Let $\phi : G \to H$ be an isomorphism and suppose G is abelian. Fix $a, b \in H$. Since ϕ is surjective, we have $c, d \in G$ where $\phi(c) = a$ and $\phi(d) = b$, thus

$$ab = \phi(c)\phi(d) = \phi(cd) = \phi(dc) = \phi(d)\phi(c) = ba.$$

Now, assume H is abelian. Since ϕ is bijective, it has a well defined inverse $\phi^{-1} : H \to G$ that is also bijective, and so the previous argument can be applied to find that G is abelian. ■

5) $\mathbb{Q}$ is countable, but $\mathbb{R}$ is uncountable, so $|\mathbb{Q}| \neq |\mathbb{R}|$, and thus no bijection $\phi : \mathbb{Q} \to \mathbb{R}$ exists. ■

9) In D_{24} we have that $|r| = 12$, while there exist no elements in S_4 with order 12, thus these two groups cannot be isomorphic. ■

14) Let $\phi : G \to H$ be a homomorphism and $a, b \in \ker\phi$, then we have that $\phi(ab) = \phi(a)\phi(b) = e'$, and thus $ab \in \ker\phi$. We also have that $\phi(a^{-1}) = \phi(a)\phi(a^{-1}) = \phi(aa^{-1}) = \phi(e) = e'$, and thus $a^{-1} \in \ker\phi$. Since $\ker\phi$ satisfies the subgroup criterion, it is a subgroup of G.

Now, assume $\ker\phi = \{e\}$ and let $a, b \in G$ where $\phi(a) = \phi(b)$, then we have that $\phi(a)\phi(b^{-1}) = \phi(ab^{-1}) = e'$, but since $\ker\phi = \{e\}$, we have that $ab^{-1} = e$, and thus $a = b$. Finally, assume ϕ is injective. Since it is a homomorphism, $\phi(e) = e'$. If there existed $a \in G$ where $a \neq e$ and $\phi(a) = e'$, then ϕ wouldn't be injective, and thus $\ker\phi = \{e\}$. ■

22 Let $\phi : A \to A$ be defined as $\phi(a) = a^k$ for a fixed integer k Then, for $a, b \in A$, we have that $\phi(ab) = (ab)^k = a^k b^k = \phi(a)\phi(b)$ since A is abelian. Now, let $k = -1$, then ϕ takes $a \in A$ to its inverse. Since all elements in A have an inverse, ϕ is surjective, and since inverses are unique, it is injective, and thus an isomorphism. ■