James Lee Crowder

Math 430
Dr. Songhao Li
Spring 2016

HOMEWORK 2
Due 2/8/16

1. Let $(V, +, \cdot)$ be a vector space over a field $\mathbb{F}$. Show that the set of invertible linear transformations from V to itself $GL(V) = \{f : V \to V \mid f \text{ is linear and invertible}\}$ is a group, where the group operation is the composition of linear transformations.

Proof. We first show that composition is a binary operation on $GL(V)$. Let $f, g \in GL(V)$. Then each of f and g is linear and invertible. Then, for all $u, v \in V$ and every $\lambda \in \mathbb{F}$,

$$[f \circ g](u + \lambda v) = f(g(u + \lambda v)) = f(g(u) + \lambda g(v)) = f(g(u)) + \lambda f(g(v)) = [f \circ g](u) + \lambda[f \circ g](v)$$

i.e. $f \circ g$ is linear. We now show that, strictly as a function, $f \circ g$ is invertible, with inverse given by $g^{-1} \circ f^{-1}$. By associativity of function composition,

$$(f \circ g) \circ (g^{-1} \circ f^{-1}) = f \circ (g \circ g^{-1}) \circ f^{-1} = f \circ \mathrm{id}_V \circ f^{-1} = f \circ f^{-1} = \mathrm{id}_V$$

and similarly to show $[g^{-1} \circ f^{-1}] \circ [f \circ g] = \mathrm{id}_V$. Thus, $f \circ g \in GL(V)$.

We claim that id_V is in fact the identity element of $GL(V)$. First, we note that $\mathrm{id}_V^{-1} = \mathrm{id}_V$, so id_V is invertible, and $\mathrm{id}_V(u + \lambda v) = u + \lambda v = \mathrm{id}_V(u) + \lambda\,\mathrm{id}_V(v)$, i.e. id_V is linear, and so $\mathrm{id}_V \in GL(V)$. Moreover, for every $f \in GL(V)$, we have $f \circ \mathrm{id}_V = f = \mathrm{id}_V \circ f$, and so id_V is the identity element of $GL(V)$.

Finally, we show that $f^{-1} \in GL(V)$ for every $f \in GL(V)$. Clearly, $\left(f^{-1}\right)^{-1} = f$, so f^{-1} is invertible. Furthermore,

$$\begin{aligned}
f^{-1}(u + \lambda v) &= f^{-1}\left(\mathrm{id}_V(u) + \lambda\,\mathrm{id}_V(v)\right) \\
&= f^{-1}\left([f \circ f^{-1}](u) + \lambda[f \circ f^{-1}](v)\right) \\
&= f^{-1}\left(f\left(f^{-1}(u)\right) + \lambda f\left(f^{-1}(v)\right)\right) \text{ ; since } f \text{ is linear,} \\
&= f^{-1}\left(f\left(f^{-1}(u) + \lambda f^{-1}(v)\right)\right) \\
&= [f^{-1} \circ f]\left(f^{-1}(u) + \lambda f^{-1}(v)\right) \\
&= \mathrm{id}_V\left(f^{-1}(u) + \lambda f^{-1}(v)\right) \\
&= f^{-1}(u) + \lambda f^{-1}(v)
\end{aligned}$$

and so f^{-1} is linear. Then $f^{-1} \in GL(V)$, and therefore, $(GL(V), \circ)$ is a group. ∎

2. Show that the dihedral group D_{2016}, which is the symmetry group of the regular polygon with 2016 edges, is generated by two elements.

Proof. In lieu of this, we will show the more general case. Let $n \in \mathbb{N}$ such that $n \geqslant 3$, and let P_n be a regular n-gon in $\mathbb{R}^2$ centered about the origin. Number the vertices counterclockwise $0, 1, \ldots, n-1$. Let r be the rotation of P_n counterclockwise by $\dfrac{2\pi}{n}$ radians and s be the reflection of P_n about the line of symmetry through vertex 0. We note that $r(i) = i+1 \pmod n$ and $s(i) = n-i = \text{-}i \pmod n$ for each $i \in \{0, 1, \ldots, n-1\}$; in particular, $s(0) = 0$ for all n and $s\left(\dfrac{n}{2}\right) = \dfrac{n}{2}$ for $n \in 2\mathbb{N}$.

We will now show that $|D_n| = 2n = |\langle r, s\rangle|$, and hence $D_m = \langle r, s\rangle$. First, to show $|D_n| = 2n$, we note that the vertex 0 can be mapped to any vertex i via the symmetry r^i, since $r^i(0) = \sum_{j=1}^{i} 1 = i$. Then, we can map vertex 1 to one of two positions; vertex $i + 1 \pmod n$ or vertex $i - 1 \pmod n$. The given symmetry r^i maps 1 to $i + 1 \pmod n$ since $r(0) = 1$, and the symmetry $r^i s$ maps 0 to i since s fixes 0 and maps 1 to $i - 1 \pmod n$:

$$r^i s(0) = r^i\left(s(0)\right) = r^i(0) = i$$

$$r^i s(1) = r^i\left(s(1)\right) = r^i(n-1) = n - 1 + i \pmod n = i - 1 \pmod n$$

Thus, there are $2n$ positions to which the vertices 0 and 1 may be mapped. Since the positions of any two vertices determines the positions of the remaining vertices and any symmetry must place vertex 0 adjacent to vertex 1, there are exactly $2n$ symmetries of P_n, i.e. $|D_n| = 2n$.

We now show that $|\langle r, s\rangle| = 2n$. Since $r^i(0) = i$, we have that each of $r^0 = \mathrm{id}_{P_n}, r, r^2, \ldots, r^{n-1}$ are each distinct and not id_{P_n}. Since $r^n(i) = i + n \pmod n = i \pmod n = i$ for every $i \in \{0, 1, \ldots, n-1\}$, $r^n = \mathrm{id}_{p_n}$, and hence $|r| = n$. Similarly, since $s(1) = n - 1 \neq 1$ and $s^2(i) = s\left(s(i)\right) = s(n-i) = n - (n-i) = i$, $|s| = 2$. Now, we will show that $s \neq r^i$ for any $i \in \{0, 1, \ldots, n-1\}$ (and thus for any $i \in \mathbb{Z}$ since $|r| = n$). Suppose to the contrary that $s = r^I$ for some $I \in \{0, 1, \ldots, n-1\}$. Then $s(0) = 0 = I = r^I(0)$ and $s(1) = n - 1 = I + 1 \pmod n = r^I(1)$. From the first equation, we have $I = 0$. But then, the second equation becomes $n - 1 = I + 1 \pmod n = 0 + 1 \pmod n = 1 \pmod n = 1$, and thus $n = 2$, a contradiction (since $n \geqslant 3$ by assumption). Thus, $s \neq r^i$ for any $i \in \{0, 1, \ldots, n-1\}$. Thus, we have now shown that s is distinct from each of $\mathrm{id}_{p_n}, r, \ldots, r^{n-1}$. By the cancellation law, we then must have $sr^i \neq r^j$ for any $i, j \in \{0, 1, \ldots, n-1\}$. Suppose $sr^i = sr^j$, where $0 \leqslant i, j \leqslant n-1$. Then $r^i = r^j$ by the cancellation law, and hence $i = j$ since $|r| = n$. Thus, each sr^i is distinct, and each is not equal to one of the r^i or to id_{P_n}. Thus, we have constructed $2n$ distinct elements of $\langle r, s\rangle$; $\mathrm{id}_{P_n}, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots,$ and sr^{n-1}. Since $\langle r, s\rangle \leqslant D_n$ and $|D_n| = 2n$, we must therefore have $D_n = \langle r, s\rangle$; in particular, this holds for $n = 2016$. ∎

Part 1 Section 6 Exercises

For problems 12, 13, and 15 from this section, we will prove a more general result that we will then apply to each problem.

Claim 1: Let G be a cyclic group generated by $g \in G$. Then $G = \langle \phi(g) \rangle$ for any $\phi \in \text{Aut}(G)$ and for any $x \in G$ such that $G = \langle x \rangle$, $\psi_x : G \to G$ defined by $\psi_x(g^n) = x^n$ is in $\text{Aut}(G)$.

Proof. Let $\phi \in \text{Aut}(G)$. Let $h \in G$. Then, since $\phi \in \text{Aut}(G)$ and $G = \langle g \rangle$, there exists some $n \in \mathbb{Z}$ such that $h = \phi(g^n) = \phi(g)^n$, i.e. $G = \langle \phi(g) \rangle$. Now, suppose $G = \langle x \rangle$ for some $x \in G$, and define ψ_x as given above. Let $g^m, g^n \in G$. Then $\psi_x(g^m g^n) = \psi_x(g^{m+n}) = x^{m+n} = x^m x^n = \psi_x(g^m)\psi_x(g^n)$, and so ψ_x is a group homomorphism. Suppose $g^m, g^n \in G$ such that $x^m = \psi_x(g^m) = \psi_x(g^n) = x^n$. Then $x^{n-m} = e$. If $n - m = 0$, then $m = n$, and so ψ_x is injective. Otherwise, since $G = \langle x \rangle$, we must have G finite. Then $|G| = |g|$ divides $n - m$, and thus $n - m = |g| \cdot z$ for some $z \in \mathbb{Z}$. Then $n = |g| \cdot z + m$, and thus $g^n = g^{|g| \cdot z + m} = (g^{|g|})^z g^m = e^z g^m = g^m$, and so ψ_x is injective. Let $x^n \in G$. Then $g^n \in G$ and $\psi_x(g^n) = x^n$, and so ψ_x is surjective. Therefore, $\psi_x \in \text{Aut}(G)$.

■

From Claim 1, we can very easily identify the automorphisms of any given cyclic group as follows; by Exercise 44, any automorphism (in fact, any homomorphism from G) ϕ of a cyclic group $G = \langle g \rangle$ is determined completely by $\phi(g)$. By our above result, we know that every automorphism must map g to some other generator $\phi(g)$, and each unique generator x of G has the unique associated automorphism ψ_x as above. Therefore, there are exactly as many automorphisms of G as there are generators of G. In particular, since $\mathbb{Z} = \langle 1 \rangle = \langle \text{-}1 \rangle$, there are only two automorphisms of $\mathbb{Z}$; $\text{id}_\mathbb{Z}$ and $z \mapsto \text{-}z$. Similarly, since $\mathbb{Z}/n\mathbb{Z} = \langle [m] \rangle$ if and only if $\gcd(m, n) = 1$ by Theorem 6.14, there are exactly as many automorphisms of $\mathbb{Z}/n\mathbb{Z}$ as there are positive integers relatively prime to and less than or equal to n. The function that associates each positive integer n with this number $\Big(\big|\{m \in \mathbb{N} \ : \ 1 \leqslant m \leqslant n \text{ and } \gcd(m, n) = 1\}\big|\Big)$ is called Euler's totient function, and is usually denoted by ϕ. Thus, using this notation, there are exactly $\phi(n)$ automorphisms of $\mathbb{Z}/n\mathbb{Z}$. Thus, $|\text{Aut}(\mathbb{Z}/2\mathbb{Z})| = \phi(2) = 1$ and $|\text{Aut}(\mathbb{Z}/6\mathbb{Z})| = \phi(6) = 2$. In particular, for p prime, there are $p - 1$ automorphisms of $\mathbb{Z}/p\mathbb{Z}$, namely each of $[a] \mapsto [am]$ such that $[m] \neq [0]$.

49. Show by a counterexample that the following "converse" of Theorem 6.6 is not true: If a group G is such that every proper subgroup is cyclic, then G is cyclic.

The Klein four-group serves as such a counterexample. Recall that the Klein four group is the set $V = \{1, a, b, ab\}$ and the binary operation $*$ with the following Cayley table:

$*$	1	a	b	ab
1	1	a	b	ab
a	a	1	ab	b
b	b	ab	1	a
ab	ab	b	a	1

By direct inspection, we see that the only subgroups of V are $\langle 1\rangle, \langle a\rangle, \langle b\rangle$, and $\langle ab\rangle$, each of which is a proper cyclic subgroup, but that V is not cyclic since each element of V has order $2 < 4 = |V|$.

51. Let p and q be distinct prime numbers. Find the number of generators of $\mathbb{Z}/pq\mathbb{Z}$.

As we have already shown, there are exactly $\phi(pq)$ generators of $\mathbb{Z}/pq\mathbb{Z}$, where ϕ is Euler's totient function. However, more can be said, and we will prove a slightly more general result.

Claim 2: If $m, n \in \mathbb{N}$ such that $\gcd(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$, where ϕ is Euler's totient function.

Proof. If $m = 1$ or $n = 1$, then we are done since $\phi(1) = 1$. Otherwise, we may write the natural numbers $1, 2, \ldots, mn$ in the following array:

$$\begin{array}{cccccc} 1 & 1+m & 1+2m & \cdots & 1+(n-1)m \\ 2 & 2+m & 2+2m & \cdots & 2+(n-1)m \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ m & 2m & 3m & \cdots & mn \end{array}$$

Note that the entry in the ith row and the jth column is of the form $i + (j-1)m$. We will now compute $\phi(mn)$ using this diagram. First suppose $\gcd(i, m) > 1$. Then there is some $k \in \mathbb{N}\backslash\{1\}$ such that k divides both i and m. Then k divides $i + (j-1)m$ for every $1 \leqslant j \leqslant n$ and k divides mn (since k divides m and m divides mn), so $\gcd(i + (j-1)m, mn) \geqslant k > 1$; that is, for each i such that $\gcd(i, m) > 1$, none of the entries $i + (j-1)m$ in the ith row are relatively prime to mn. Thus, there are only $\phi(m)$ rows with any entries relatively prime to mn. Now, suppose $\gcd(i, m) = 1$. Since $\gcd(m, n) = 1$, m generates $\mathbb{Z}/n\mathbb{Z}$ by Theorem 6.14. That is, $\mathbb{Z}/n/Z = \{[m], [2m], \ldots, [(n-1)m]\}$. As in Cayley's Theorem, using the left regular representation of $\mathbb{Z}/n\mathbb{Z}$ and the associated permutation $[a] \mapsto [a] + [i] = [a + i]$, we see that $\mathbb{Z}/n\mathbb{Z} = \{[i + m], [i + 2m], \ldots, [i + (n-1)m]\}$. By Theorem 6.14, exactly $\phi(n)$ of these entries are relatively prime to n. We will now show that each of these is in fact relatively prime to mn.

Suppose to the contrary that $\gcd(m,i) = 1 = \gcd(i+(j-1)m, n)$ and there exists some prime p such that p divides both mn and $i+(j-1)m$. Since p is prime and divides mn, we must have p divides m or p divides n. If p divides m, then $m = pa$ and $i+(j-1)m = pb$ for some $a, b \in \mathbb{Z}$. Then

$$i = pb - (j-1)m = pb - (j-1)(pa) = p[b-(j-1)a]$$

i.e. p divides i. But then, since p also divides m, $gcd(i,m) \geqslant p > 1$, a contradiction. If p divides n, then $n = px$ and $i+(j-1)m = py$ for some $x, y \in \mathbb{Z}$. Since $\gcd(i+(j-1)m, n) = 1$, there exists $\alpha, \beta \in \mathbb{Z}$ such that $\alpha[i+(j-1)m] + \beta n = 1$. Then

$$1 = \alpha[i+(j-1)m] + \beta n = \alpha(py) + \beta(px) = p(\alpha y + \beta x)$$

and so p divides 1, a contradiction. Thus, for each i such that $\gcd(i,m) = 1$, each of the entries $i+(j-1)m$ that are relatively prime to n are relatively prime to mn. Therefore, since there are $\phi(m)$ such i and $\phi(n)$ such j for each such i, there are $\phi(m)\phi(n)$ natural numbers relatively prime to mn, i.e. $\phi(mn) = \phi(m)\phi(n)$. ■

Since any two distinct primes p and q satisfy $\gcd(p,q) = 1$, we conclude that there are $\phi(pq) = \phi(p)\phi(q)$ generators of $\mathbb{Z}/pq\mathbb{Z}$.

52. Let p be a prime number. Find the number of generators of $\mathbb{Z}/p^r\mathbb{Z}$, where $r \in \mathbb{N}$.

As previously, we know that the number of generators is $\phi(p^r)$. However, as before, more can be said.

Claim 3: If p is prime and $r \in \mathbb{N}$, then $\phi(p^r) = p^r - p^{r-1} = p^{r-1}(p-1)$.

Proof. First, we note that $\phi(p) = (p-1)$, and that the only divisors of p are itself and 1. Thus, the only divisors of p^r are p^l where $0 \leqslant l \leqslant r$. Moreover, each p^l for $l \geqslant 2$ is itself a multiple of p. Thus, the only numbers not relatively prime to p^r are the multiples of p, of which there are exactly p^{r-1} between 1 and p^r (including p^r). Therefore, $\phi(p^r) = p^r - p^{r-1} = p^{r-1}(p-1)$. ■

Thus, we conclude that there $\phi(p^r) = p^{r-1}(p-1)$ generators of $\mathbb{Z}/p^r\mathbb{Z}$. In fact, this result, our previous result concerning ϕ, and The Fundamental Theorem of Arithmetic allow us to relatively quickly compute $\phi(n)$ for any $n \in \mathbb{N}$; by The Fundamental Theorem, let $n = \prod_{i=1}^{N} p_i^{e_i}$ be the prime factorization of n into distinct prime powers. Then $\gcd(p_i, p_j) = 1$ for all $i \neq j$, and thus $\phi(n) = \phi\left(\prod_{i=1}^{N} p_i^{e_i}\right) = \prod_{i=1}^{N} \phi(p_i^{e_i}) = \prod_{i=1}^{N} p_i^{e_i-1}(p_i-1)$.

53. Show that in a finite cyclic group G of order n, written multiplicatively, the equation $x^m = e$ has exactly m solutions for x in G for every positive divisor m of n.

Again, we are able to show a slightly stronger result with little extra effort.

Claim 4: For $m \in \mathbb{N}$, $x^m = e$ has exactly $\gcd(m, n)$ solutions in G.

Proof. Let $m \in \mathbb{N}$, and $d = \gcd(m, n)$. Then d divides both m and n, and so $\frac{m}{d}, \frac{n}{d} \in \mathbb{N}$. Thus,

$$(x^{\frac{n}{d}})^m = (x^n)^{\frac{m}{d}} = e^{\frac{m}{d}} = e$$

and so $x^{\frac{n}{d}}$ is one of the desired solutions. Thus, each integer power $(x^{\frac{n}{d}})^a = x^{\frac{an}{d}}$ is also a solution. Since $|x| = n$, there are exactly d distinct powers of $x^{\frac{n}{d}}$, namely $x^{\frac{n}{d}}, x^{\frac{2n}{d}}, \ldots x^{\frac{dn}{d}} = x^n = e$. Thus, it remains to be show that any solution must be one of these powers of $x^{\frac{n}{d}}$. Suppose $x^z = e$. By the Division Algorithm, $z = q\frac{n}{d} + r$ for some $q, r \in \mathbb{Z}$ with $0 \leqslant r < \frac{n}{d}$. Then

$$e = x^z = x^{q\frac{n}{d}+r} = x^{q\frac{n}{d}}x^r = (x^{\frac{n}{d}})^q x^r = e^q x^r = x^r$$

Since $n \geqslant \frac{n}{d}$ and $|x| = n$, we must have $r = 0$, and therefore z is a multiple of $\frac{n}{d}$ as desired. ■

Applying this to the special case that m divides n gives that there are $\gcd(m, n) = m$ solutions.

55. Show that $\mathbb{Z}/p\mathbb{Z}$ has no proper non-trivial subgroups if p is prime

Proof. As in class, if $H \leqslant \mathbb{Z}/p\mathbb{Z}$, then $H = \langle [d] \rangle$ for some $[d] \in \mathbb{Z}/p\mathbb{Z}$. If $\{[0]\} \lneq H$, then $[d] \neq [0]$. But then $\gcd(d, p) = 1$, and so $H = \langle [d] \rangle = \mathbb{Z}/p\mathbb{Z}$ by Theorem 6.14. ■

56 Let G be an abelian group, and let H and K be finite cyclic groups of order r and s respectively. Show that G contains a cyclic group of order $\operatorname{lcm}(r, s)$.

Proof. We will first show the case where $\gcd(r, s) = 1$, and will then use this result to generalize. Since $\gcd(r, s) = 1$ and $rs = \operatorname{lcm}(r, s)\gcd(r, s)$ (which we will use without proof), we then have $\operatorname{lcm}(r, s) = rs$. We claim that $|hk| = rs$. First, we note that since G is abelian, $(hk)^{rs} = h^{rs}k^{rs} = (h^r)^s(k^s)^r = e^s e^r = e$, and so $|hk| \leqslant rs$. Suppose $n \in \mathbb{N}$ such that $(hk)^n = e$. By the Division Algorithm, we can write $n = ar + b = xs + y$, where $a, b, x, y \in \mathbb{Z}$ such that $0 \leqslant b < r$ and $0 \leqslant y < s$. Then, since G is abelian,

$$(hk)^n = h^n k^n = h^{ar+b}k^{xs+y} = (h^r)^a h^b (k^s)^x k^y = e^a h^b e^x k^y = h^b k^y$$

and thus $h^{-b} = k^y$. Call this group element x. Then $x \in H, K$, and thus $x \in H \cap K$. Since H and K are cyclic with $|H| = r$ and $|K| = s$, $|x|$ must divide both r and s by Theorem 6.14, i.e. $|x|$ is a common divisor of r and s. Thus, since $\gcd(r, s) = 1$, $|x| = 1$, i.e. $x = e$. Then $h^b = (h^{-b})^{-1} = e^{-1} = e$, and hence we must have $b = 0$ since $0 \leqslant b < r = |h|$. Similarly, $y = 0$. Then $n = ar = xs$, i.e. n is a common multiple of r and s. Then, by definition, $\text{lcm}(r, s) = rs \leqslant n$, and thus we must in fact have $|hk| = rs$ as desired.

We now do the general case. By the Fundamental Theorem of Algebra, $r = \prod_{i=1}^{M} p_i^{\lambda_i}$ and $s = \prod_{j=1}^{N} p_j^{\sigma_j}$ for some primes p_i, p_j and $\lambda_i, \sigma_j \in \mathbb{N}$. Then, allowing $\lambda_k, \sigma_k = 0$, $r = \prod_{k=1}^{M+N} p_k^{\lambda_k}$ and $s = \prod_{k=1}^{M+N} p_k^{\sigma_k}$, where each p_k is distinct. Then, let $\Lambda = \{k : \lambda_k \geqslant \sigma_k\}$ and let $\Sigma = \{1, 2, \ldots, M + N\} \backslash \Lambda = \{k : \sigma_k > \lambda_k\}$. Then, since $\gcd(r, s) = \prod_{k=1}^{M+N} p_k^{\min(\lambda_k, \sigma_k)}$ and $\text{lcm}(r, s) = \prod_{k=1}^{M+N} p_k^{\max(\lambda_k, \sigma_k)}$, we have $\gcd(r, s) = \prod_{k \in \Lambda} p_k^{\sigma_k} \prod_{k \in \Sigma} p_k^{\lambda_k}$ and $\text{lcm}(r, s) = \prod_{k \in \Lambda} p_k^{\lambda_k} \prod_{k \in \Sigma} p_k^{\sigma_k}$. Thus, $\gcd(r, s) = \prod_{k=1}^{M+N} p_k^{m_k} = \prod_{k \in \Lambda} p_k^{\sigma_k} \prod_{k \in \Sigma} p_k^{\lambda_k}$ and $\text{lcm}(r, s) = \prod_{k \in \Lambda} p_i^{\lambda_k} \prod_{k \in \Sigma} p_k^{\sigma_k}$. Then, by Theorem 6.14, since $|h| = r$, $|h^m| = \prod_{k \in \Lambda} p_i^{\lambda_k}$, where $m = \prod_{k \in \Sigma} p_k^{\lambda_k}$, since $r = \prod_{k=1}^{M+N} p_k^{\lambda_k} = \prod_{k \in \Lambda} p_k^{\lambda_k} \prod_{k \in \Sigma} p_k^{\lambda_k}$. Similarly, $|k^n| = \prod_{k \in \Sigma} p_k^{\sigma_k}$, where $n = \prod_{k \in \Lambda} p_k^{\sigma_k}$. Since $\Lambda \cap \Sigma = \varnothing$, we have

$$\gcd(|h^m|, |k^n|) = \gcd\left(\left[\prod_{k \in \Lambda} p_i^{\lambda_k}\right], \left[\prod_{k \in \Sigma} p_i^{\sigma_k}\right]\right) = 1$$

Thus, by our prior result, $|h^m k^n| = |h^m||k^n| = \prod_{k \in \Lambda} p_k^{\lambda_k} \prod_{k \in \Sigma} p_k^{\sigma_k} = \text{lcm}(r, s)$, and therefore, $\langle h^m k^n \rangle \leqslant G$ is the desired cyclic subgroup. ■

Part 1 Section 8 Exercises

18. Consider the group S_3 of Example 8.7

i Compute $\langle\rho_1\rangle, \langle\rho_2\rangle$, and $\langle\mu_1\rangle$.

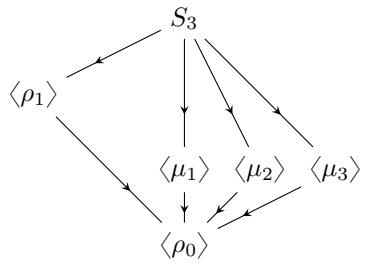
ii Give the subgroup lattice for S_3.

Proof.

i. Directly, we compute $\langle\rho_1\rangle = \{\rho_0, \rho_1, \rho_2\} = \langle\rho_2\rangle$ and $\langle\mu_1\rangle = \{\rho_0, \mu_1\}$.

ii. Again, by direct computation and comparison we construct the following:

Subgroup Lattice of S_3



■

21 ii. The given group is isomorphic to S_3.

Proof. It can be varified directly that the map

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \mapsto \iota, \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \mapsto (12) \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} \mapsto (13)$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \mapsto (23) \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \mapsto (123) \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 2 \\ 1 & 0 & 0 \end{bmatrix} \mapsto (132)$$

is a group isomorphism into S_3. ■

44. Compute $|D_n|$ and find a subgroup pf D_n with order $\dfrac{|D_n|}{2}$.

Proof. Our arguments from Problem 2 give $|D_n| = 2n$, and the desired subgroup is $\langle r \rangle$. ■

49. If A is a set, then $H \leqslant S_A$ is said to be transitive on A if for all $a, b \in A$, there exists $\sigma \in H$ such that $\sigma(a) = b$. Show that if A is a nonempty finite set, then there exists a finite cyclic subgroup $H \leqslant S_A$ with $|H| = |A|$ such that H is transitive on A.

Proof. Let $A = \{0, 1, \ldots, n-1\}$. Let $\sigma = (0\,1\,\cdots\,n-1)$. We claim that $\langle \sigma \rangle$ is transitive on A and $|\sigma| = n$. Since $\sigma(i) = i+1 \pmod n$, $|\sigma| = n$ since $\sigma^n(i) = i$ for all $i \in A$ and $\sigma^m(1) = 1+m \neq 1 \pmod n$ if $1 \leqslant m < n$. Furthermore, for any $i, j \in A$, $\sigma^{j-i} \in \langle \sigma \rangle$ and $\sigma^{j-i}(i) = i + (j-i) \pmod n = j \pmod n = j$, so $\langle \sigma \rangle$ is transitive on A (in fact, viewing D_n as a subgroup of S_n, $\sigma = r$ as in Problem 2). ■

53 i. Show that every finite group of order n is isomorphic to a group of $n \times n$ permutation matrices under matrix multiplication.

Proof. We will essentially mimic the isomorphism given in Problem 21 part ii of this same section. Let G be a finite group. Let G be a group with $|G| = n$. Let $G = \{g_1, g_2, \ldots, g_n\}$ be some enumeration of G. By Cayley's Theorem, G is isomorphic to some subgroup of S_G. Since $|G| = n$, G is isomorphic to S_n as a set, and so S_G is isomorphic to S_n. Thus, G is isomorphic to some subgroup of S_n. We now show that S_n is isomorphic to the set of matrices with distinct elementary basis elements as rows under matrix multiplication, i.e. $S_n \equiv P_{n\times n} = \big\{A \in O(n, \mathbb{R}) : A = [e_i\, e_j\, \ldots\, e_k] \text{ and } \{i, j, \ldots, k\} = \{1, 2, \ldots, n\}\big\}$, where e_i is the column vector with a 1 in the ith position and zero for all other entries. We claim that $\phi : S_n \to P_{n\times n}$ defined by $\phi(\sigma) = [e_{\sigma(1)}\, e_{\sigma(2)}\, \cdots\, e_{\sigma(n)}]$ is a group isomorphism. Clearly ϕ maps S_n into $P_{n\times n}$ since $\sigma[\{1, 2, \ldots, n\}] = \{1, 2, \ldots, n\}$ by definition of S_n. Suppose $\sigma, \lambda \in S_n$ such that $\phi(\sigma) = \phi(\lambda)$. Then $[e_{\sigma(1)}\, e_{\sigma(2)}\, \cdots\, e_{\sigma(n)}] = [e_{\lambda(1)}\, e_{\lambda(2)}\, \cdots\, e_{\lambda(n)}]$. Equating columns gives $e_{\sigma(i)} = e_{\lambda(i)}$ for all i, and hence $\sigma(i) = \lambda(i)$, i.e. $\sigma = \lambda$. Let $[e_i\, e_j\, \cdots\, e_k] \in P_{n\times n}$. Then the map $1 \mapsto i, 2 \mapsto j, \ldots, n \mapsto k$ is in S_n since $\{i, j, \ldots, k\} = \{1, 2, \ldots, n\}$ and $|\{i, j, \ldots, k\}| = n$. Call this map μ. Then
$\phi(\mu) = [e_{\mu(1)}\, e_{\mu(2)}\, \cdots\, e_{\mu(n)}] = [e_i\, e_j\, \cdots\, e_k]$, and so ϕ is surjective.

To show that ϕ is a homomorphism, we first show a result that will aid in later computation. Let $\rho \in S_3$. Then $\phi(\rho) = [e_{\rho(1)}\, e_{\rho(2)}\, \cdots e_{\rho(n)}]$. Thus, the entry in the ith row and jth column is 1 if and only if $\rho(j) = i$. But this occurs if and only if $i = \rho^{-1}(j)$, which is equivalent to the entry in the ith row and jth column of $[e_{\rho^{-1}(1)}\, e_{\rho^{-1}(2)}\, \cdots\, e_{\rho^{-1}(n)}]^T$ is 1. That is, we have shown
$\phi(\rho) = [e_{\rho(1)}\, e_{\rho(2)}\, \cdots e_{\rho(n)}] = [e_{\rho^{-1}(1)}\, e_{\rho^{-1}(2)}\, \cdots\, e_{\rho^{-1}(n)}]^T$. With this result in mind, for $\sigma, \lambda \in S_3$, we have
$\phi(\sigma \circ \lambda) = [e_{\sigma\circ\lambda(1)}\, e_{\sigma\circ\lambda(2)}\, \cdots\, e_{\sigma\circ\lambda(n)}]$. In this matrix, the entry in the ith row and jth column is 1 if and

only if $\sigma \circ \lambda(j) = i$, which is true if and only if $\lambda(j) = \sigma^{-1}(i)$. But this is equivalent to $\langle e_{\sigma^{-1}(i)}, e_{\lambda(j)} \rangle = 1$ (where $\langle \cdot, \cdot \rangle$ is the standard inner product on $\mathbb{R}^n$), which occurs if and only if the entry in the ith row and jth column of $[e_{\sigma^{-1}(1)}\, e_{\sigma^{-1}(2)}\, \cdots\, e_{\sigma^{-1}(n)}]^T [e_{\lambda^{-1}(1)}\, e_{\lambda^{-1}(2)}\, \cdots\, e_{\lambda^{-1}(n)}]$ is 1 since the entry in the ith row and jth column of this product is defined to be $\langle e_{\sigma^{-1}(i)}, e_{\lambda(j)} \rangle$. Thus, by our above result that $[e_{\sigma(1)}\, e_{\sigma(2)}\, \cdots\, e_{\sigma(n)}] = [e_{\sigma^{-1}(1)}\, e_{\sigma^{-1}(2)}\, \cdots\, e_{\sigma^{-1}(n)}]^T$, we have

$$\begin{aligned}
\phi(\sigma \circ \lambda) &= [e_{\sigma\circ\lambda(1)}\, e_{\sigma\circ\lambda(2)}\, \cdots\, e_{\sigma\circ\lambda(n)}] \\
&= [e_{\sigma^{-1}(1)}\, e_{\sigma^{-1}(2)}\, \cdots\, e_{\sigma^{-1}(n)}]^T [e_{\lambda(1)}\, e_{\lambda(2)}\, \cdots\, e_{\lambda(n)}] \\
&= [e_{\sigma(1)}\, e_{\sigma(2)}\, \cdots\, e_{\sigma(n)}][e_{\lambda(1)}\, e_{\lambda(2)}\, \cdots\, e_{\lambda(n)}] \\
&= \phi(\sigma)\phi(\lambda)
\end{aligned}$$

i.e. ϕ is a group homomorphism. Then ϕ is in fact an isomorphism. To recap, we now know that G is isomorphic to a subgroup of S_n by Cayley's Theorem, and we have just shown that $S_n \equiv P_{n\times n}$. In particular, in the argument of Cayley's Theorem, we constructed the left regular representation of G, which embeds G as a subgroup of S_n. Call this embedding $\mathcal{L}$. Then $\phi \circ \mathcal{L} : G \to P_{n\times n}$ is an injective homomorphism since both ϕ and $\mathcal{L}$ are injective homomorphisms. Here, we only show the homomorphism property: for $x, y \in G$,

$$[\phi \circ \mathcal{L}](x * y) = \phi\big(\mathcal{L}(x * y)\big) = \phi\big(\mathcal{L}(x) \circ \mathcal{L}(y)\big) = \phi\big(\mathcal{L}(x)\big)\, \phi\big(\mathcal{L}(y)\big)$$

Therefore, since $\phi \circ \mathcal{L}$ is an injective group homomorphism, $G \equiv (\phi \circ \mathcal{L})\,[G] \leqslant P_{n\times n}$, i.e. G is isomorphic to the subgroup $(\phi \circ \mathcal{L})\,[G]$ of $P_{n\times n}$. ■