

1. Problem-Points: 1-5 2-5 3-5 4-4 5-4 6-4 7-9 8-3 9-2 10-5 11-6 12-5

- (a) $f : X \rightarrow Y$ is one-to-one iff $\forall x, y \in X \quad f(x) = f(y) \rightarrow x = y$
- (b) $f : X \rightarrow Y$ is onto iff $\forall y \in Y \exists x \in X \quad f(x) = y$
- (c) g is the inverse of f iff $g : Y \rightarrow X$ and $\forall x \in X \quad g(f(x)) = x$ and $\forall y \in Y \quad f(g(y)) = y$.
 (It is not sufficient to say $f(x) = y$ implies $g(y) = x$. For example, if $X = \{1\}$ and $Y = \{1, 2\}$ and $f(1) = 1$ and $g(1) = 1$ and $g(2) = 1$.)
- (d) $\sigma \in S_N$ a permutation of $\{1, 2, \dots, N\}$ is an n -cycle iff there exists a sequence $a_1, a_2, \dots, a_n$ of distinct elements of $\{1, 2, \dots, N\}$ and σ satisfies
 $\sigma(a_i) = a_{i+1}$ for $i = 1, 2, \dots, n-1$,
 $\sigma(a_n) = a_1$, and
 $\sigma(x) = x$ for all other elements of $\{1, 2, \dots, N\}$.
 The n -cycle σ is written

$$\sigma = (a_1 \ a_2 \ \cdots \ a_n)$$

- (e) A transposition is a 2-cycle.

2. Prove: Every cycle is the product of transpositions.

To show that

$$(a_1 \ a_2 \ \cdots \ a_n) = (a_1 \ a_2)(a_2 \ a_3) \cdots (a_{n-1} \ a_n)$$

by induction on n , it suffices to see that:

$$(a_1 \ a_2 \ \cdots \ a_{n-1})(a_{n-1} \ a_n) = (a_1 \ a_2 \ \cdots \ a_{n-1} \ a_n)$$

For the permutation on the left if $i < n-1$ then a_i is sent to a_{i+1} since it is not effected by the transposition $(a_{n-1} \ a_n)$. But a_{n-1} is sent to a_n by the transposition and left there by the $n-1$ cycle. Finally a_n is sent to a_{n-1} by the transposition and then cycled to a_1 by the $n-1$ cycle.

3. How many elements of order 4 are there there in S_5 ?

The elements of order 4 are exactly the 4 cycles. There are 30. There are five choices of things to leave out. For each choice of 4 things there are $3!$ ways to arrange them around a circle. So its $5 \times 3! = 30$.

4.

(a) $\phi : G \rightarrow G'$ is a homomorphism iff

$$\forall x, y \in G \quad \phi(x *_G y) = \phi(x) *_G' \phi(y)$$

(b) An isomorphism is a homomorphism which is one-to-one and onto.

(c) An automorphism is isomorphism with the same domain and range.

(d) G is isomorphic to G' iff there exists an isomorphism $\phi : G \rightarrow G'$.

5. Suppose $\phi : G \rightarrow G'$ is a homomorphism. Then:

(a) $\phi(e) = e'$ because

$$\phi(e) = \phi(ee) = \phi(e)\phi(e)$$

and “multiplying” both sides by $\phi(e)^{-1}$ on the left we get

$$e' = \phi(e)^{-1}\phi(e) = \phi(e)^{-1}\phi(e)\phi(e) = \phi(e)$$

(b) for all $x \in G$ $\phi(x^{-1}) = (\phi(x))^{-1}$ because

$$e' = \phi(x^{-1}x) = \phi(x^{-1})\phi(x)$$

and “multiplying” both sides by $(\phi(x))^{-1}$ on the right gives

$$(\phi(x))^{-1} = e'(\phi(x))^{-1} = \phi(x^{-1})\phi(x)(\phi(x))^{-1} = \phi(x^{-1})$$

6. Let H be a subgroup of a group G and $a, b \in G$.

(a) $aH = \{ax : x \in H\}$.

(b) $Ha = \{xa : x \in H\}$.

(c) $aHbH = \{axby : x, y \in H\}$.

(d) $H \triangleleft G$ iff $aH = Ha$ for every $a \in G$.

7. If H is a subgroup of the finite group G , then $|H|$ divides $|G|$.

The two main points of the proof are:

(1) $|aH| = |H|$ for any $a \in G$

(2) aH and bH are either equal or disjoint for any two $a, b \in G$.

It follows that G is partitioned into cosets of H each of which has size $|H|$ and so $|G| = (\text{number of cosets})|H|$ and hence $|H|$ divides $|G|$.

Proof of (1): Define the function $f : H \rightarrow aH$ by $f(x) = ax$. Clearly f is onto. To see that f is one-to-one, suppose $f(x) = f(y)$. Then $ax = ay$ and so $x = a^{-1}ax = a^{-1}ay = y$.

Proof of (2): Suppose that aH and bH are not disjoint and we show that $aH \subseteq bH$. If z is some element in both aH and bH , then for some $x, y \in H$ we have that $ax = z = by$ and so $a = byx^{-1}$. Now let $h \in H$ be arbitrary. Then $ah = byx^{-1}h$ and since $yx^{-1}h \in H$ (its a subgroup) it follows that $ah \in bH$. Thus $aH \subseteq bH$.

By a similar argument $bH \subseteq aH$ and hence they are equal.

8. Let $\alpha : G \rightarrow G$ be an automorphism. Then α^{-1} is an automorphism of G .
 α^{-1} is one-to-one: Suppose $\alpha^{-1}(x) = \alpha^{-1}(y)$. Then

$$x = \alpha(\alpha^{-1}(x)) = \alpha(\alpha^{-1}(y)) = y$$

α^{-1} is onto: Suppose $y \in G$. Then letting $x = \alpha(y)$

$$\alpha^{-1}(x) = \alpha^{-1}(\alpha(y)) = y$$

α^{-1} is a homomorphism: Given $u, v \in G$ let $\alpha(x) = u$ and $\alpha(y) = v$ and since α is a homomorphism we have that $\alpha(xy) = \alpha(x)\alpha(y) = uv$. Then

$$\alpha^{-1}(uv) = \alpha^{-1}(\alpha(x)\alpha(y)) = \alpha^{-1}(\alpha(xy)) = xy = \alpha^{-1}(u)\alpha^{-1}(v)$$

9. $G \times H$ is the group with underlying set:

$$\{(x, y) : x \in G, y \in H\}$$

and binary operation

$$(x, y) *_{G \times H} (x', y') = (x *_G x', y *_H y')$$

10. $S_3 \times S_4$ cannot be isomorphic to a subgroup of S_5 because $|S_n| = n!$ and $|S_3 \times S_4| = |S_3| \times |S_4| = 3!4!$ is bigger than $5!$.

11. For X any nonempty set let S_X be group of permutations of the set X . In this terminology $S_n = S_{\{1, 2, \dots, n\}}$.

Lemma. Suppose X and Y are disjoint nonempty sets. Then $S_X \times S_Y$ is isomorphic to a subgroup of $S_{X \cup Y}$.

Proof. Define the map $\phi : S_X \times S_Y \rightarrow S_{X \cup Y}$ by $\phi(\alpha, \beta) = \gamma$ where

$$\gamma(u) = \begin{cases} \alpha(u) & \text{if } u \in X \\ \beta(u) & \text{if } u \in Y \end{cases}$$

Since X and Y are disjoint γ is a permutation of $X \cup Y$. To see that ϕ is one-to-one suppose that $\gamma = \phi(\alpha, \beta) = \phi(\alpha', \beta') = \gamma'$. Then from the definition ϕ we have that $\alpha(u) = \alpha'(u)$ since $\gamma(u) = \gamma'(u)$ for $u \in X$. Similarly $\beta = \beta'$. Hence $(\alpha, \beta) = (\alpha', \beta')$.

To see that ϕ is a homomorphism note that

$$\gamma(\gamma'(u)) = \alpha(\alpha'(u)) \text{ if } u \in X \text{ and}$$

$$\gamma(\gamma'(u)) = \beta(\beta'(u)) \text{ if } u \in Y.$$

and so

$$\phi(\alpha, \beta)\phi(\alpha', \beta') = \gamma\gamma' = \phi(\alpha\alpha', \beta\beta') = \phi((\alpha, \beta)(\alpha', \beta'))$$

Since ϕ is 1-1 homomorphism it is an isomorphism to the subgroup $\phi(S_X \times S_Y) \subseteq S_{X \cup Y}$ and the Lemma is proved.

(Remark: ϕ is not onto since if $\gamma = (x \ y)$ is a transposition of an element $x \in X$ and $y \in Y$, then γ is not in the range ϕ .)

Note that $S_4 = S_{\{1,2,3,4\}} \simeq S_{\{4,5,6,7\}}$ via the map $\rho : S_{\{1,2,3,4\}} \rightarrow S_{\{4,5,6,7\}}$

$$\rho(\alpha) = \beta \text{ where } \beta(i) = \alpha(i - 3) + 3.$$

(In fact, $S_X \simeq S_Y$ whenever X and Y have the same number of elements.) Hence $S_3 \times S_4 \simeq S_{\{1,2,3\}} \times S_{\{4,5,6,7\}}$ which by the Lemma is isomorphic to a subgroup of $S_7 = S_{\{1,2,3,4,5,6,7\}}$.

Remark: Some people argued that since $3!4!$ divides $7!$ there must be such a subgroup. But $3!4!$ divides $6!$ and there is no such subgroup of S_6 .

12. What is the order of 14 in the group $\mathbb{Z}_{48}$? It the same as the order of the subgroup generated by 14. This is the same as the subgroup generated by $\gcd(14, 48) = 2$. But 2 obviously has order 24, so 14 has order 24.

What is the order of the coset $14 + 6\mathbb{Z}_{48}$ in the group $\mathbb{Z}_{48}/6\mathbb{Z}_{48}$? If G is an abelian group, then every subgroup is normal. If G is written additively and H is a subgroup, then the cosets of H are written $x + H$. The identity element of the factor group G/H is H , so we are asking for the least n such that $(x + H) + (x + H) + \cdots + (x + H) = H$ or equivalently $nx + H = H$ or equivalently $nx \in H$.

So what is the least n such that $n \otimes_{48} 14 \in 6\mathbb{Z}_{48}$. Which is equivalent to the least n such that $14n$ is divisible by 6. But $14n \equiv_6 2n$ so the answer is $n = 3$.

13. Prove: Suppose $\rho : G \rightarrow G'$ is any onto homomorphism and $H = \ker(\rho)$. Let $\phi : G \rightarrow G/H$ be the quotient map. Then there exists an isomorphism

$$\alpha : G/H \rightarrow G'$$

such that $\rho = \alpha \circ \phi$.

Proof. Define $\alpha(aH) = \rho(a)$. For this map to be well-defined we must check that $aH = bH$ implies $\rho(a) = \rho(b)$. This is true because $aH = bH$ implies that $b^{-1}a \in H$ and $H = \ker(\rho)$ implies that $\rho(b^{-1}a) = e$ and so $e = \rho(b)^{-1}\rho(a)$ and thus $\rho(b) = \rho(a)$.

α is a homomorphism because

$$\alpha(aHbH) = \alpha(abH) = \rho(ab) = \rho(a)\rho(b) = \alpha(aH)\alpha(bH)$$

α is onto because ρ is onto so if $b \in G'$ then there exists $a \in G$ with $\rho(a) = b$ and so $\alpha(aH) = \rho(a) = b$.

α is one-to-one: Suppose $\alpha(aH) = e$. Then $\rho(a) = e$ and hence a is in the $\ker(\rho) = H$ and so $aH = H$ the identity element of G/H . So $\ker(\alpha)$ is the identity element and so α is one-to-one.

$$\rho = \alpha \circ \phi \text{ because } \rho(a) = \alpha(aH) = \alpha(\phi(a))$$