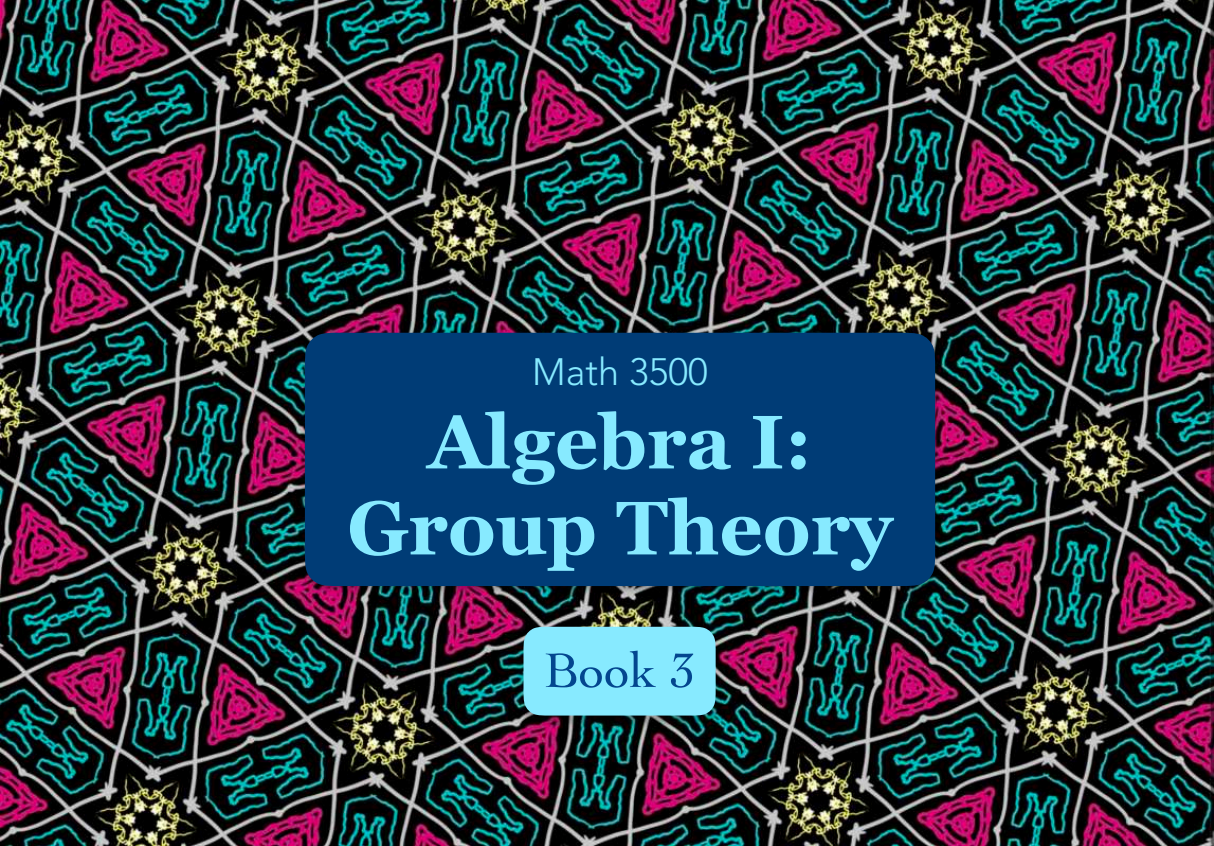
Math 3500
Algebra I:
Group Theory
Book 3

Eg. $F = \mathbb{F}_p = \{0, 1, 2, \cdots, p-1\}$ where p is a prime
(finite field of order p).

Take $n=2$ and consider the vector space $V = F^2 = \left\{ \begin{bmatrix} a \\ b \end{bmatrix} : a, b \in F \right\}$,
an additive abelian group of order p^2.

Every homomorphism $V \to V$ is a linear transformation over the field F.

If $T: V \to V$ is a homomorphism then $T(v+w) = T(v) + T(w)$.

$T(2v) = T(v+v) = T(v) + T(v) = 2T(v)$.

$T(3v) = T(2v+v) = T(2v) + T(v) = 2T(v) + T(v) = 3T(v)$.

In fact $T(kv) = kT(v)$ for all $k \in \mathbb{F}_p$.

So $Tv = Av$ for some 2×2 matrix A over F.

There are exactly p^4 homomorphisms $V \to V$.

How many of these p^4 homomorphisms are automorphisms of V?

$(p^2-1)(p^2-p) = |GL_2(F)|$.

The Klein four-group (any group of order 4 which is not cyclic)

	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

eg. $G \cong \{1, 3, 5, 7\}$ under multiplication mod 8

or $\langle (12)(34), (13)(24) \rangle < S_4$

$= \{ (), (12)(34), (13)(24), (14)(23) \}$

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

$F = \mathbb{F}_2 = \{0, 1\}$ (integers mod 2)

$G \cong F^2 = \left\{ \begin{bmatrix} x \\ y \end{bmatrix} : x, y \in F \right\} = \left\{ \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right\}$ is an additive abelian group

This is another way to look at the Klein four-group.

It has 6 automorphisms i.e. isomorphisms from the group to itself.

The group G (Klein four-group) has 16 endomorphisms (homomorphisms $G \to G$)

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

$ab = c$

$|a| = |b| = |c| = 2$

Why? To define an endomorphism T of $G = \{1, a, b, c\} = \langle a, b \rangle$

think of T as a linear transformation $T: G \to G$

there are four choices of $T(a) \in G$ i.e. $T(a) \in \{1, a, b, c\}$

" " " " $T(b) \in G$

Then $T(c) = T(ab) = T(a)T(b)$

Only 6 of these 16 homomorphisms are invertible.

How many endomorphisms does a finite cyclic group have?

Take $G = C_n = \{1, g, g^2, \dots, g^{n-1}\}$, $|g| = n$.

How many homomorphisms are there from this group to itself? Exactly n.

They are the maps $\phi_0, \phi_1, \dots, \phi_{n-1}$ where $\phi_j : G \to G$, $\phi_j(g^i) = g^{ij}$.

Note that $\phi_j(xy) = (xy)^j = x^j y^j = \phi_j(x)\phi_j(y)$ so ϕ_j is a homomorphism.

Note that $\phi_j \neq \phi_k$ for $j \neq k$ in $\{0, 1, \dots, n-1\}$ —

since $\phi_j(g) = g^j \neq \phi_k(g) = g^k$ so we have at least n different homomorphisms $C_n \to C_n$.

Conversely, suppose $\phi: C_n \to C_n$ is any homomorphism.
Then $\phi(g) = g^i \in G$, $0 \le i \le n-1$. In this case we claim $\phi = \phi_i$.

$$\phi(g^2) = \phi(gg) = \phi(g)\phi(g) = g^i g^i = g^{2i} = (g^2)^i = \phi_i(g^2)$$
$$\phi(g^3) = \phi(g^2 g) = \phi(g^2)\phi(g) = g^{2i} g^i = g^{3i} = (g^3)^i = \phi_i(g^3)$$

Inductively we get $\phi(x) = \phi_i(x)$ for all $x \in G$ i.e. $\phi = \phi_i$. □

---

eg. $G = C_4 = \{1, g, g^2, g^3\}$ has four endomorphisms $\phi_0, \phi_1, \phi_2, \phi_3$ defined by

$$\phi_j(g^i) = g^{ij}$$

x	$\phi_0(x)$	$\phi_1(x)$	$\phi_2(x)$	$\phi_3(x)$
1	1	1	1	1
g	1	g	g^2	g^3
g^2	1	g^2	1	g^2
g^3	1	g^3	g^2	g

$\phi_0(g^i) = g^{0i} = g^0 = 1$
trivial homomorphism
$\phi_0(ab) = \phi_0(a)\phi_0(b)$
$1 \quad 1 \quad 1$

$\phi_1(g^i) = g^{1i} = g^i$ is the identity

$\phi_2(g^i) = g^{2i}$, $\phi_2(x) = x^2$

$\phi_3(x) = x^3$

$\phi_j(xy) = (xy)^j = x^j y^j = \phi_j(x)\phi_j(y)$

If $\psi(g^i) = g$ then $g = \psi(g^2) = \psi(gg) \neq \underbrace{\psi(g)}_{g}\underbrace{\psi(g)}_{g} = g^2$

$G = \{1, g, g^2, \dots, g^{n-1}\}$ has n homomorphisms $G \to G$, namely $\phi_k(x) = x^k$, $0 \le k \le n-1$ or $1 \le k \le n$.

How many of these are isomorphisms? (bijective)

$\phi_k : G \to G$, $x \mapsto x^k$ is one-to-one iff it's onto iff it's bijective iff $\gcd(k,n) = 1$ (k is relatively prime to n).

For $n = 12$, $\phi_k : C_{12} \to C_{12}$ is bijective iff $k \in \{1, 5, 7, 11\}$.

$\phi_3 : C_{12} \to C_{12}$ has image $\phi_3(C_{12}) = \{1, g^3, g^6, g^9\}$ ϕ_3 is neither one-to-one nor onto.

$\phi_3(1) = \phi_3(g^4) = 1$

$g \notin \phi_3(C_{12})$ $\quad g^2 = g^7$

The image of $f : G \to H$ is $f(G) = \{f(g) : g \in G\}$.

$\phi_5 : C_{12} \to C_{12}$ is onto; its image is $\{1, g^5, g^{10}, g^{15}, g^{20}, g^{25}, g^{30}, g^{35}, g^{40}, g^{45}, g^{50}, g^{55}\}$

$\qquad\qquad = g^3 \qquad = g^8 \qquad = g \qquad = g^6 \qquad = g \qquad = g^4 \qquad = g^9$

$\phi_9 : C_{12} \to C_{12}$ is not onto; $\phi_9(C_{12}) = \{1, g^9, g^6, g^3\}$ $\quad g^{60} = (g^{12})^5 = 1^5 = 1$

Euclid's Algorithm (extended form):

Let $a, b \in \mathbb{Z}$, not both zero, and let $d = \gcd(a,b)$. Then there exist integers $r, s \in \mathbb{Z}$ such that $d = ra + sb$. (That is, d is an integer linear combination of a, b).

Eg. $a = 369$, $b = 126$. We will compute $d = \gcd(a,b)$ and write d as an integer linear combination of a, b.

$369 = 2 \times 126 + 117$

$126 = 1 \times 117 + \boxed{9}$ ← $d = 9 = \gcd(a,b)$

$117 = 13 \times 9 + 0$

$369 \;\; 252 \;\; 117$

$9 = 126 - 117$

$= 126 - (369 - 2 \times 126)$

$= 3 \times 126 - 369$

$12 = 2 \times 5 + 2$

$5 = 2 \times 2 + \boxed{1} = \gcd(12,5) =$

$2 = 2 \times 1 + 0$

$1 = 5 - 2 \times 2$

$= 5 - 2(12 - 2 \times 5)$

$= 5 \times 5 - 2 \times 12$

$k = 5k \times 5 - 2k \times 12$

We want to show every element of C_{12} is the 5^{th} power of some element.

$g^k = g^{5k \times 5 - 2k \times 12} = (g^{5k})^5 (g^{12})^{-2k} = (g^{5k})^5$

$(k \in \mathbb{Z})$ ($g^{12} = 1$)

$a = 369 = 3 \times 123 = 3^2 \times 41$

$b = 126 = 3 \times 42 = 2 \times 3 \times 21 = 2 \times 3 \times 3 \times 7 = 2 \times 3^2 \times 7$.

There are n homomorphisms $\phi_k : C_n \to C_n$, $k \in \{1, 2, \dots, n\}$ $\phi_k(x) = x^k$.

There are $\phi(n)$ isomorphisms $C_n \to C_n$, namely ϕ_k, $1 \le k \le n$, $\gcd(k, n) = 1$.

Euler's totient function $\phi(k)$ = number of integers $k \in \{1, \dots, n\}$ such that $\gcd(k, n) = 1$.

$\phi(12) = 4$.

Sorry I'm using "ϕ" more than once.