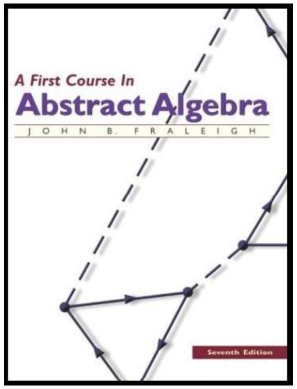
Introduction to Modern Algebra

Part I. Groups and Subgroups
I.6. Cyclic Groups



Theorem 6.1.

Theorem 6.1. Every cyclic group is abelian.

Proof. Let G be cyclic with generator $a \in G$, so $G = \langle a \rangle$. Let $g_1, g_2 \in G$. Then $g_1 = a^r$, and $g_2 = a^s$ for some $r, s \in \mathbb{Z}$. Then $g_1 g_2 = a^r a^s = a^{r+s} = a^{s+r} = a^s a^r = g_2 g_1$. Therefore $G = \langle a \rangle$ is abelian. □

Theorem 6.6.

Theorem 6.6. A subgroup of a cyclic group is cyclic.

Proof. Let G be a cyclic group generated by $a \in G$ and let H be a subgroup of G. If H is the trivial subgroup $H = \{e\}$, then $a^n \in H$ for some $n \in \mathbb{Z}$. Since $(a^n)^{-1} \in H$, then $a^{-n} \in H$ as well, and so W.L.O.G. $a^n \in H$ for some $n \in \mathbb{N}$. Let m be the smallest natural number such that $a^m \in H$ (every nonempty subset of $\mathbb{N}$ has a smallest element this is a property of $\mathbb{N}$).

We now show that $H = \langle a^m \rangle$. Let $b \in H$. Then $b = a^n$ for some $n \in \mathbb{Z}$ since $G = \langle a \rangle$. By the Division Algorithm, there exists $q, r \in \mathbb{Z}$ such that $n = mq + r$ and $0 \le r < m$. Then $a^n = a^{mq+r} = (a^m)^q a^r$, or $a^r = ((a^m)^q)^{-1} a^n = (a^m)^{-q} a^n$.

Theorem 6.6. (Continued)

Theorem 6.6. A subgroup of a cyclic group is cyclic.

Proof (Continued). Now since $a^n = b \in H$ (by hypothesis on b), $a^m \in H$ (since m is defined as the smallest natural number with this property), and since H is a group, then: $(a^m)^q \in H$ (closure under the binary operation), $(a^m)^{-q} \in H$ (inverse of $(a^m)^q$), and $(a^m)^{-q} a^n \in H$ (closure), or $a^r \in H$. But since m is the smallest natural number power such that $a^m \in H$ and since $0 \le r < m$, it must be that $r = 0$. Therefore $n = mq$ and $b = a^n = a^{mq} = (a^m)^q$. So each $b \in H$ is of the form $(a^m)^q$ for some $q \in \mathbb{Z}$. That is, $H = \langle a^m \rangle$ and so H is cyclic. □

Exercise 6.45.

Exercise 6.45. Let $r, s \in \mathbb{N}$. Then $\{nr + ms \mid n, m \in \mathbb{Z}\} = A$ is a subgroup of $\mathbb{Z}$.

Proof. Since $0 \in \mathbb{Z}$, then $(0)\,r + (0)\,s = 0 \in A$. If $a \in A$ then $a = nr + ms$ for some $n, m \in \mathbb{Z}$. Therefore $(-n)\,r + (-m)\,s = -\,(nr + ms) = -a \in A$. Associativity on A is inherited by associativity of addition on $\mathbb{Z}$. So by Theorem 4.15, A is a subgroup of $\mathbb{Z}$. □

Theorem 6.10.

Theorem 6.10. Let G be a cyclic group with generator a. If G is of infinite order then G is isomorphic to $\langle \mathbb{Z}, + \rangle$. If G has finite order n, then G is isomorphic to $\langle \mathbb{Z}_n, +_n \rangle$.

Proof. CASE 1: Suppose that for all natural numbers $m, a^m \neq e$. Suppose $a^h = a^k$ for some $h \neq k$, say $h > k$. Then $e = a^h a^{-h} = a^h a^{-k} = a^{h-k}$, but we have assumed in this case that no natural number power of 'a' yields the identity. Therefore if $h \neq k$ then $a^h \neq a^k$. So every element of G can be expressed as a^m for an unique $m \in \mathbb{Z}$. So the map $\varphi : G \to \mathbb{Z}$ defined as $\varphi\left(a^i\right) = i$ is therefore well defined (by the uniqueness of m comment above), one-to-one (different inputs a^i yield different outputs i), and onto $\mathbb{Z}$.

Now to show that φ preserves the binary operations:

$$\varphi\left(a^i a^j\right) = \varphi\left(a^{i+j}\right) = i + j = \varphi(i) + \varphi(j).$$

Therefore φ is an isomorphism and G is isomorphic to $\langle \mathbb{Z}, + \rangle$.

Theorem 6.10 (continued 1)

Theorem 6.10. Let G be a cyclic group with generator a. If G is of infinite order then G is isomorphic to $\langle \mathbb{Z}, + \rangle$. If G has finite order n, then G is isomorphic to $\langle \mathbb{Z}_n, +_n \rangle$.

Proof (continued). CASE 2: Suppose that $a^m = e$ for some natural number m. Let n be the smallest natural number such that $a^n = e$. If $s \in \mathbb{Z}$ and $s = nq + r$ for $0 \leq r < n$ (q and r given s and n by the Division Algorithm), then $a^s = a^{nq+r} = (a^n)^q\, a^r = e^q a^r = e a^r = a^r$. Similar to Case 1, if $0 < k < h < n$ and $a^h = a^k$, then $a^{h-k} = e$ and $0 < h - k < n$, contradicting the fact that n is the smallest positive exponent of 'a' yielding e. So the following powers of a are distinct: $a^0 = e, a, a^2, \ldots, a^{n-1}$. Now define the map $\psi : G \to \mathbb{Z}_n$ as $\psi\left(a^i\right) = i$ for $i = 0, 1, 2, \ldots, n-1$.

Theorem 6.10 (continued 2)

Theorem 6.10. Let G be a cyclic group with generator a. If G is of infinite order then G is isomorphic to $\langle \mathbb{Z}, + \rangle$. If G has finite order n, then G is isomorphic to $\langle \mathbb{Z}_n, +_n \rangle$.

Proof (continued). Then ψ is well defined, one-to-one, and onto $\mathbb{Z}_n$. Suppose $i +_n j = k$ (that is $i + j = k \pmod{n}$), so $i + j = k + ln$ for some $l \in \mathbb{Z}$). Then

$$\psi\left(a^i a^j\right) = \psi\left(a^{i+j}\right) = \psi\left(a^{k+ln}\right) = \psi\left(a^k a^{ln}\right)$$

$$= \psi\left(a^k (a^n)^l\right) = \psi\left(a^k e\right) = \psi\left(a^k\right) = k = i +_n j = \psi\left(a^i\right) +_n \psi(j).$$

Therefore ψ is an isomorphism and so G is isomorphic to $\mathbb{Z}_n$. □

Theorem 6.14.

Theorem. 6.14. Let G be a cyclic group with n elements and with generator a. Let $b \in G$ where $b = a^s$. Then b generates a cyclic subgroup H of G containing $\frac{n}{d}$ elements where $d = \gcd(n, s)$. Also, $\langle a^s \rangle = \langle a^t \rangle$ if and only if $\gcd(s, n) = \gcd(t, n)$.

Proof. By Theorem 5.17, b generates a cyclic subgroups of G; call it H. Now to show $|H| = \frac{n}{d}$. As in the proof of Case 2 of Theorem 6.10, the order of H is m where m is the smallest natural number such that $b^m = e$. Next, $b = a^s$ by hypothesis and so $b^m = e$ implies $(a^s)^m = e$.

Since (again by Theorem 6.10 Case 2) $\{G\} = \{e, a, a^2, \ldots, a^{n-1}\}$, then the only power of a which yields e are integer multiples of n. Therefore $a^{ms} = e$ implies that n divides ms. So

$$a^{ms} = e \text{ if and only if } \frac{n}{ms}. \qquad (*)$$

Let $d = \gcd(n, s)$. Then there exists integers (u) and (v) such that $d = (u)\,n + (v)\,s$ from the second paragraph of page 62.

Theorem 6.14 (continued 1)

Theorem. 6.14. Let G be a cyclic group with n elements and with generator a. Let $b \in G$ where $b = a^s$. Then b generates a cyclic subgroup H of G containing $\frac{n}{d}$ elements where $d = \gcd(n, s)$. Also, $\langle a^s \rangle = \langle a^t \rangle$ if and only if $\gcd(s, n) = \gcd(t, n)$.

Proof (continued). Since d is a division of both n and s (recall $d = \gcd(n, s)$), we may write $1 = \frac{d}{d} = \frac{un}{d} + \frac{vs}{d} \implies 1 = u\left(\frac{n}{d}\right) + v\left(\frac{s}{d}\right)$. Next, any integer which divides both $\frac{n}{d}$ and $\frac{s}{d}$, must divide $1 = u\left(\frac{n}{d}\right) + v\left(\frac{s}{d}\right)$. Therefore, such an integer must divide 1 and the integer must be 1. Hence, $\frac{n}{d}$ and $\frac{s}{d}$ must be relatively prime. Therefore $\left(\frac{n}{d}\right)\left(\frac{s}{d}\right) = \frac{n}{s}$ is some (positive) rational number. Hence, for some smallest positive $m \in \mathbb{N}$, we have $m\left(\frac{n}{s}\right) \in \mathbb{N}$.

Next $m\left(\frac{s}{n}\right) = m\frac{s/d}{n/d} \in \mathbb{N}$ and since $\frac{n}{d}$ and $\frac{s}{d}$ are relatively prime, then $\frac{n}{d}$ must divide m. So the smallest such value of m is $\frac{n}{d}$: $m = \frac{n}{d}$. $\qquad (**)$ Now, $(*)$ implies $a^{ms} = e$ iff $\frac{n}{ms}$. The smallest such m for which $\frac{n}{ms}$ is $m = \frac{n}{d}$ by $(**)$.

Theorem 6.14 (continued 2)

Theorem. 6.14. Let G be a cyclic group with n elements and with generator a. Let $b \in G$ where $b = a^s$. Then b generates a cyclic subgroup H of G containing $\frac{n}{d}$ elements where $d = \gcd(n, s)$. Also, $\langle a^s \rangle = \langle a^t \rangle$ if and only if $\gcd(s, n) = \gcd(t, n)$.

Proof (continued). So m is the smallest natural number such that $a^{ms} = (a^s)^m = b^m = e$ and by Case 2 of Theorem 6.10, the order of $H = \langle b \rangle$ is $m = \frac{n}{d}$. Next, by Theorem 6.10 we know that a cyclic group with n elements is isomorphic to $\mathbb{Z}_n$. In $\mathbb{Z}_n$, if d is a division of n, then $\langle d \rangle$ is a cyclic subgroup of $\mathbb{Z}_n$ with $\frac{n}{d}$ elements: $\langle d \rangle = \{0, d, 2d, 3d, \ldots, (n-1)\,d\}$. So $\langle d \rangle$ contans all $m \in \mathbb{Z}_n$ such that $\gcd(m, n) = d$. So $\langle d \rangle$ is the only subgroup of $\mathbb{Z}_n$ of order $\frac{n}{d}$ (since the only possible generators of a group of this order is an element for which $d = \gcd(m, n)$ by the first part of the theorem).

Theorem 6.14 (continued 3)

Theorem 6.14. Let G be a cyclic group with n elements and with generator a. Let $b \in G$ where $b = a^s$. Then b generates a cyclic subgroup H of G containing $\frac{n}{d}$ elements where $d = \gcd(n, s)$. Also, $\langle a^s \rangle = \langle a^t \rangle$ if and only if $\gcd(s, n) = \gcd(t, n)$.

Proof (Continued). So m is the smallest natural number such that $a^{ms} = (a^s)^m = b^m = e$ and by Case 2 of Theorem 6.10, the order of $H = \langle b \rangle$ is $m = \frac{n}{d}$.

Next, by Theorem 6.10 we know that a cyclic group with n elements is isomorphic to $\mathbb{Z}_n$. In $\mathbb{Z}_n$, if d is a division of n, then $\langle d \rangle$ is a cyclic subgroup of $\mathbb{Z}_n$ with $\frac{n}{d}$ elements: $\langle d \rangle = \{0, d, 2d, 3d, \ldots, (n-1)\,d\}$. So $\langle d \rangle$ contans all $m \in \mathbb{Z}_n$ such that $\gcd(m, n) = d$. So $\langle d \rangle$ is the only subgroup of $\mathbb{Z}_n$ of order $\frac{n}{d}$ (since the only possible generators of a group of this order is an element for which $d = \gcd(m, n)$ by the first point of the theorem).

Theorem 6.14 (continued 4)

Theorem 6.14. Let G be a cyclic group with n elements and with generator a. Let $b \in G$ where $b = a^s$. Then b generates a cyclic subgroup H of G containing $\frac{n}{d}$ elements where $d = \gcd(n, s)$. Also, $\langle a^s \rangle = \langle a^t \rangle$ if and only if $\gcd(s, n) = \gcd(t, n)$.

Proof (continued). By this uniqueness and the first part of this theorem, $\langle a^s \rangle$ has order $\gcd(s, n)$ and $\langle a^t \rangle$ has order $\gcd(t, n)$, so $\langle a^s \rangle = \langle a^t \rangle$ iff $\gcd(s, n) = \gcd(t, n)$. □