Modern Algebra

Chapter I. Groups

I.3. Cyclic Groups—Proofs of Theorems

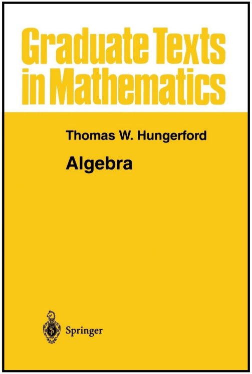

Table of contents

Theorem I.3.1

Theorem I.3.1. Every subgroup H of the additive group $\mathbb{Z}$ is cyclic. Either $H = \langle 0 \rangle$ or $H = \langle m \rangle$ where m is the least positive integer in H. If $H \neq \langle 0 \rangle$, then H is infinite.

Proof. Either $H = \langle 0 \rangle$ or H contains a least positive integer m (this property is part of the formal definition of $\mathbb{N}$, the Law of Well Ordering on page 10). Since H is closed under the binary operation (addition here) then $\langle m \rangle = \{km \mid k \in \mathbb{Z}\} \subset H$.

Theorem I.3.1

Theorem I.3.1. Every subgroup H of the additive group $\mathbb{Z}$ is cyclic. Either $H = \langle 0 \rangle$ or $H = \langle m \rangle$ where m is the least positive integer in H. If $H \neq \langle 0 \rangle$, then H is infinite.

Proof. Either $H = \langle 0 \rangle$ or H contains a least positive integer m (this property is part of the formal definition of $\mathbb{N}$, the Law of Well Ordering on page 10). Since H is closed under the binary operation (addition here) then $\langle m \rangle = \{km \mid k \in \mathbb{Z}\} \subset H$. Conversely if $h \in H$, then $h = qm + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r < m$ by the Division Algorithm (Theorem 0.6.3). Since $r = h - qm \in H$ (because $h, qm \in H$), the minimality of positive integer m implies that $r = 0$ (since $0 \leq r < m$ and $r \in H$) and so $h = qm$. Hence $H \subset \langle m \rangle$. If $H \neq \langle 0 \rangle$, then for $k_1, k_2 \in \mathbb{Z}$ with $k_1 \neq k_2$, we have $k_1 m \neq k_2 m$ and hence $\langle m \rangle$ is infinite. □

Theorem I.3.1

Theorem I.3.1. Every subgroup H of the additive group $\mathbb{Z}$ is cyclic. Either $H = \langle 0 \rangle$ or $H = \langle m \rangle$ where m is the least positive integer in H. If $H \neq \langle 0 \rangle$, then H is infinite.

Proof. Either $H = \langle 0 \rangle$ or H contains a least positive integer m (this property is part of the formal definition of $\mathbb{N}$, the Law of Well Ordering on page 10). Since H is closed under the binary operation (addition here) then $\langle m \rangle = \{km \mid k \in \mathbb{Z}\} \subset H$. Conversely if $h \in H$, then $h = qm + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r < m$ by the Division Algorithm (Theorem 0.6.3). Since $r = h - qm \in H$ (because $h, qm \in H$), the minimality of positive integer m implies that $r = 0$ (since $0 \leq r < m$ and $r \in H$) and so $h = qm$. Hence $H \subset \langle m \rangle$. If $H \neq \langle 0 \rangle$, then for $k_1, k_2 \in \mathbb{Z}$ with $k_1 \neq k_2$, we have $k_1 m \neq k_2 m$ and hence $\langle m \rangle$ is infinite. □

Theorem I.3.2

Theorem I.3.2. Every infinite cyclic group is isomorphic to the additive group $\mathbb{Z}$ and every finite cyclic group of order m is isomorphic to the additive group $\mathbb{Z}_m$.

Proof. For $G = \langle a \rangle$ a cyclic group, define $\alpha : \mathbb{Z} \to G$ as $\alpha(k) = a^k$. By Theorem I.1.9, α is a homomorphism. Since a is a generator of G, then (by Theorem I.2.8) α is onto and so α is an epimorphism.

Theorem I.3.2

Theorem I.3.2. Every infinite cyclic group is isomorphic to the additive group $\mathbb{Z}$ and every finite cyclic group of order m is isomorphic to the additive group $\mathbb{Z}_m$.

Proof. For $G = \langle a \rangle$ a cyclic group, define $\alpha : \mathbb{Z} \to G$ as $\alpha(k) = a^k$. By Theorem I.1.9, α is a homomorphism. Since a is a generator of G, then (by Theorem I.2.8) α is onto and so α is an epimorphism. If $\text{Ker}(\alpha) = \{0\}$ then α is one to one by Theorem I.2.3(i), α is an isomorphism, and hence $\mathbb{Z} \cong G$. Otherwise if $\text{Ker}(\alpha) \neq \{0\}$ and $\text{Ker}(\alpha)$ is a nontrivial subgroup of $\mathbb{Z}$ (by Exercise I.2.9 $\text{Ker}(\alpha)$ is a subgroup of $\mathbb{Z}$) then $\text{Ker}(\alpha) = \langle m \rangle$ for some least positive m in $\text{Ker}(\alpha)$ by Theorem I.3.1.

Theorem I.3.2

Theorem I.3.2. Every infinite cyclic group is isomorphic to the additive group $\mathbb{Z}$ and every finite cyclic group of order m is isomorphic to the additive group $\mathbb{Z}_m$.

Proof. For $G = \langle a \rangle$ a cyclic group, define $\alpha : \mathbb{Z} \to G$ as $\alpha(k) = a^k$. By Theorem I.1.9, α is a homomorphism. Since a is a generator of G, then (by Theorem I.2.8) α is onto and so α is an epimorphism. If $\text{Ker}(\alpha) = \{0\}$ then α is one to one by Theorem I.2.3(i), α is an isomorphism, and hence $\mathbb{Z} \cong G$. Otherwise if $\text{Ker}(\alpha) \neq \{0\}$ and $\text{Ker}(\alpha)$ is a nontrivial subgroup of $\mathbb{Z}$ (by Exercise I.2.9 $\text{Ker}(\alpha)$ is a subgroup of $\mathbb{Z}$) then $\text{Ker}(\alpha) = \langle m \rangle$ for some least positive m in $\text{Ker}(\alpha)$ by Theorem I.3.1.

Theorem I.3.2 (continued)

Theorem I.3.2. Every infinite cyclic group is isomorphic to the additive group $\mathbb{Z}$ and every finite cyclic group of order m is isomorphic to the additive group $\mathbb{Z}_m$.

Proof (continued). Now to show that $\mathbb{Z}_m \cong G$. For $r, s \in \mathbb{Z}$, then $a^r = a^s$ if and only if $a^{r-s} = e$ if and only if $r - s \in \text{Ker}(\alpha) = \langle m \rangle$ if and only if $m \mid (r - s)$ if and only if $\overline{r} = \overline{s}$ in $\mathbb{Z}_m$ (where $\overline{k}$ is the congruence class of $\mathbb{Z}_m$ containing $k \in \mathbb{Z}$). So the map $\beta : \mathbb{Z}_m \to G$ given by $\overline{k} \mapsto a^k$ is well defined. Also, β is a homomorphism because

$$\beta(\overline{r} + \overline{s}) = a^{r+s} = a^r a^s = \beta(\overline{r})\beta(\overline{s})$$

and so is onto since a is a generator of G. That is, β is an epimorphism.

Theorem I.3.2 (continued)

Theorem I.3.2. Every infinite cyclic group is isomorphic to the additive group $\mathbb{Z}$ and every finite cyclic group of order m is isomorphic to the additive group $\mathbb{Z}_m$.

Proof (continued). Now to show that $\mathbb{Z}_m \cong G$. For $r, s \in \mathbb{Z}$, then $a^r = a^s$ if and only if $a^{r-s} = e$ if and only if $r - s \in \mathrm{Ker}(\alpha) = \langle m \rangle$ if and only if $m \mid (r - s)$ if and only if $\overline{r} = \overline{s}$ in $\mathbb{Z}_m$ (where $\overline{k}$ is the congruence class of $\mathbb{Z}_m$ containing $k \in \mathbb{Z}$). So the map $\beta : \mathbb{Z}_m \to G$ given by $\overline{k} \mapsto a^k$ is well defined. Also, β is a homomorphism because

$$\beta(\overline{r} + \overline{s}) = a^{r+s} = a^r a^s = \beta(\overline{r})\beta(\overline{s})$$

and so is onto since a is a generator of G. That is, β is an epimorphism. Since $\beta(\overline{k}) = e$ if and only if $a^k = e = a^0$ if and only if $\overline{k} = \overline{0} \in \mathbb{Z}_m$, then $\mathrm{Ker}(\beta) = \{\overline{0}\}$ and by Theorem I.2.3(i) β is one to one and is hence a monomorphism. So β is one to one and onto (i.e., is an isomorphism) and $\mathbb{Z}_m \cong G$. □

Theorem I.3.2 (continued)

Theorem I.3.2. Every infinite cyclic group is isomorphic to the additive group $\mathbb{Z}$ and every finite cyclic group of order m is isomorphic to the additive group $\mathbb{Z}_m$.

Proof (continued). Now to show that $\mathbb{Z}_m \cong G$. For $r, s \in \mathbb{Z}$, then $a^r = a^s$ if and only if $a^{r-s} = e$ if and only if $r - s \in \text{Ker}(\alpha) = \langle m \rangle$ if and only if $m \mid (r-s)$ if and only if $\overline{r} = \overline{s}$ in $\mathbb{Z}_m$ (where $\overline{k}$ is the congruence class of $\mathbb{Z}_m$ containing $k \in \mathbb{Z}$). So the map $\beta : \mathbb{Z}_m \to G$ given by $\overline{k} \mapsto a^k$ is well defined. Also, β is a homomorphism because

$$\beta(\overline{r} + \overline{s}) = a^{r+s} = a^r a^s = \beta(\overline{r})\beta(\overline{s})$$

and so is onto since a is a generator of G. That is, β is an epimorphism. Since $\beta(\overline{k}) = e$ if and only if $a^k = e = a^0$ if and only if $\overline{k} = \overline{0} \in \mathbb{Z}_m$, then $\text{Ker}(\beta) = \{\overline{0}\}$ and by Theorem I.2.3(i) β is one to one and is hence a monomorphism. So β is one to one and onto (i.e., is an isomorphism) and $\mathbb{Z}_m \cong G$. □

Theorem I.3.4

Theorem I.3.4. Let G be a group and $a \in G$. If a has infinite order then

(*i*) $a^k = e$ if and only if $k = 0$;

(*ii*) the elements a^k are all distinct as the values of k range over $\mathbb{Z}$.

If a has finite order $m > 0$ then

(*iii*) m is the least positive integer such that $a^m = e$;

(*iv*) $a^k = e$ if and only if $m \mid k$;

(*v*) $a^r = a^s$ if and only if $r \equiv s \pmod{m}$;

(*vi*) $\langle a \rangle$ consists of the distinct elements $a, a^2, \ldots, a^{m-1}, a^m = e$.

(*vii*) for each k such that $k \mid m$, $|a^k| = m/k$.

Proof. **(vii)** We have $(a^k)^{m/k} = a^m = e$ by Theorem I.1.9(ii) and (iii). ASSUME $(a^k)^r = e$ for some $0 < r < m/k$. Then $a^{kr} = e$ (Theorem I.1.9(ii)) where $kr < k(m/k) = m$, CONTRADICTING (iii). So the order of a^k is $|a^k| = m/k$ by (iii). □

Theorem I.3.4

Theorem I.3.4. Let G be a group and $a \in G$. If a has infinite order then

(*i*) $a^k = e$ if and only if $k = 0$;

(*ii*) the elements a^k are all distinct as the values of k range over $\mathbb{Z}$.

If a has finite order $m > 0$ then

(*iii*) m is the least positive integer such that $a^m = e$;

(*iv*) $a^k = e$ if and only if $m \mid k$;

(*v*) $a^r = a^s$ if and only if $r \equiv s \pmod{m}$;

(*vi*) $\langle a \rangle$ consists of the distinct elements $a, a^2, \ldots, a^{m-1}, a^m = e$.

(*vii*) for each k such that $k \mid m$, $|a^k| = m/k$.

Proof. **(vii)** We have $(a^k)^{m/k} = a^m = e$ by Theorem I.1.9(ii) and (iii). ASSUME $(a^k)^r = e$ for some $0 < r < m/k$. Then $a^{kr} = e$ (Theorem I.1.9(ii)) where $kr < k(m/k) = m$, CONTRADICTING (iii). So the order of a^k is $|a^k| = m/k$ by (iii). □

Theorem I.3.5

Theorem I.3.5. Every homomorphic image and every subgroup of a cyclic group G is cyclic. In particular, if H is a nontrivial subgroup of $G = \langle a \rangle$ and m is the least positive integer such that $a^m \in H$, then $H = \langle a^m \rangle$.

Proof. Let $f : G \to K$ be a group homomorphism. Then for any $a^k \in G$ we have $f(a^k) = (f(a))^k$, so the image of f is $\mathrm{Im}(f) = \langle f(a) \rangle$. Now suppose H is a subgroup of G. Let m be the least positive integer such that $a^m \in H$. Then $\langle a^m \rangle \subset H$.

Theorem I.3.5

Theorem I.3.5. Every homomorphic image and every subgroup of a cyclic group G is cyclic. In particular, if H is a nontrivial subgroup of $G = \langle a \rangle$ and m is the least positive integer such that $a^m \in H$, then $H = \langle a^m \rangle$.

Proof. Let $f : G \to K$ be a group homomorphism. Then for any $a^k \in G$ we have $f(a^k) = (f(a))^k$, so the image of f is $\text{Im}(f) = \langle f(a) \rangle$. Now suppose H is a subgroup of G. Let m be the least positive integer such that $a^m \in H$. Then $\langle a^m \rangle \subset H$. Now for $h \in H \subset G$ we have $h = a^{qm+r}$ for some $q, r \in \mathbb{Z}$ and $0 \le r < m$ by the Division Algorithm (Theorem 0.6.3). But $a^m \in H$, so $(a^m)^q = a^{qm} \in H$ and $(a^{qm})^{-1} = a^{-qm} \in H$. Therefore $a^{-qm}h = a^{-qm}a^{qm+r} = a^r \in H$. But since m is the least positive integer for which $a^m \in H$ and $0 \le r < m$, then it must be that $r = 0$. That is, if $h = a^{qm+r} \in H$ (as above) then $r = 0$ and so $h = a^{qm}$ where $q \in \mathbb{Z}$. That is, $h \in \langle a^m \rangle$. So $H \subset \langle a^m \rangle$ and hence $H = \langle a^m \rangle$. □

Theorem I.3.5

Theorem I.3.5. Every homomorphic image and every subgroup of a cyclic group G is cyclic. In particular, if H is a nontrivial subgroup of $G = \langle a \rangle$ and m is the least positive integer such that $a^m \in H$, then $H = \langle a^m \rangle$.

Proof. Let $f : G \to K$ be a group homomorphism. Then for any $a^k \in G$ we have $f(a^k) = (f(a))^k$, so the image of f is $\mathrm{Im}(f) = \langle f(a) \rangle$. Now suppose H is a subgroup of G. Let m be the least positive integer such that $a^m \in H$. Then $\langle a^m \rangle \subset H$. Now for $h \in H \subset G$ we have $h = a^{qm+r}$ for some $q, r \in \mathbb{Z}$ and $0 \le r < m$ by the Division Algorithm (Theorem 0.6.3). But $a^m \in H$, so $(a^m)^q = a^{qm} \in H$ and $(a^{qm})^{-1} = a^{-qm} \in H$. Therefore $a^{-qm}h = a^{-qm}a^{qm+r} = a^r \in H$. But since m is the least positive integer for which $a^m \in H$ and $0 \le r < m$, then it must be that $r = 0$. That is, if $h = a^{qm+r} \in H$ (as above) then $r = 0$ and so $h = a^{qm}$ where $q \in \mathbb{Z}$. That is, $h \in \langle a^m \rangle$. So $H \subset \langle a^m \rangle$ and hence $H = \langle a^m \rangle$. □

Theorem I.3.6

Theorem I.3.6. Let $G = \langle a \rangle$ be a cyclic group. If G is infinite, then a and a^{-1} are the only generators of G. If G is finite of order m, then a^k is a generator of G if and only if $(k, m) = 1$ (i.e., the greatest common divisor of k and m is 1; k and m are relatively prime).

Proof. Let G be infinite. By Theorem I.3.2, $G \cong \mathbb{Z}$. "Clearly" $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$. Let $m \in \mathbb{Z}$, $m \notin \{-1, 0, 1\}$, and consider $\langle m \rangle$. Now $\langle m \rangle = \langle -m \rangle$ and $|m|$ is the smallest positive integer in $\langle m \rangle = \langle -m \rangle$ (see Theorem I.3.1). So $1 \notin \langle m \rangle$ and $\langle m \rangle$ is a proper subgroup of $\mathbb{Z}$.

Theorem I.3.6

Theorem I.3.6. Let $G = \langle a \rangle$ be a cyclic group. If G is infinite, then a and a^{-1} are the only generators of G. If G is finite of order m, then a^k is a generator of G if and only if $(k, m) = 1$ (i.e., the greatest common divisor of k and m is 1; k and m are relatively prime).

Proof. Let G be infinite. By Theorem I.3.2, $G \cong \mathbb{Z}$. "Clearly" $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$. Let $m \in \mathbb{Z}$, $m \notin \{-1, 0, 1\}$, and consider $\langle m \rangle$. Now $\langle m \rangle = \langle -m \rangle$ and $|m|$ is the smallest positive integer in $\langle m \rangle = \langle -m \rangle$ (see Theorem I.3.1). So $1 \notin \langle m \rangle$ and $\langle m \rangle$ is a proper subgroup of $\mathbb{Z}$. Hence m does not generate $\mathbb{Z}$ and the only generators of $\mathbb{Z}$ are -1 and 1. Equivalently, the only generators of G are a^{-1} and a.

Theorem I.3.6

Theorem I.3.6. Let $G = \langle a \rangle$ be a cyclic group. If G is infinite, then a and a^{-1} are the only generators of G. If G is finite of order m, then a^k is a generator of G if and only if $(k, m) = 1$ (i.e., the greatest common divisor of k and m is 1; k and m are relatively prime).

Proof. Let G be infinite. By Theorem I.3.2, $G \cong \mathbb{Z}$. "Clearly" $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$. Let $m \in \mathbb{Z}$, $m \notin \{-1, 0, 1\}$, and consider $\langle m \rangle$. Now $\langle m \rangle = \langle -m \rangle$ and $|m|$ is the smallest positive integer in $\langle m \rangle = \langle -m \rangle$ (see Theorem I.3.1). So $1 \notin \langle m \rangle$ and $\langle m \rangle$ is a proper subgroup of $\mathbb{Z}$. Hence m does not generate $\mathbb{Z}$ and the only generators of $\mathbb{Z}$ are -1 and 1. Equivalently, the only generators of G are a^{-1} and a.

Theorem I.3.6 (continued)

Proof (continued). Let G be finite. By Theorem I.3.2, $G \cong \mathbb{Z}_m$ where m is the order of G. If $(k, m) = 1$ then there are $c, d \in \mathbb{Z}$ such that $ck + dm = 1$ (by Theorem 0.6.5 in Section I.3. Cyclic Groups). Then $\underbrace{\overline{k} + \overline{k} + \cdots + \overline{k}}_{c \text{ times}} = \overline{1}$. So for any $\overline{n} \in \mathbb{Z}_m$, we have $\underbrace{\overline{k} + \overline{k} + \cdots + \overline{k}}_{nc \text{ times}} = \overline{n}$ and hence $\overline{k}$ generates $\mathbb{Z}_m$. Next, if $(k, m) = r > 1$ then consider $n = m/r < m$. We then have $\underbrace{\overline{k} + \overline{k} + \cdots + \overline{k}}_{n \text{ times}} = \overline{nk} = \overline{km/r} = \overline{(k/r)m} = (k/r)\overline{m} = \overline{0}$ and so $\overline{k}$ does not generate $\mathbb{Z}_m$ (it generates a subgroup of order at most $n = m/r$).

Theorem I.3.6 (continued)

Proof (continued). Let G be finite. By Theorem I.3.2, $G \cong \mathbb{Z}_m$ where m is the order of G. If $(k, m) = 1$ then there are $c, d \in \mathbb{Z}$ such that $ck + dm = 1$ (by Theorem 0.6.5 in Section I.3. Cyclic Groups). Then $\underbrace{\overline{k} + \overline{k} + \cdots + \overline{k}}_{c \text{ times}} = \overline{1}$. So for any $\overline{n} \in \mathbb{Z}_m$, we have $\underbrace{\overline{k} + \overline{k} + \cdots + \overline{k}}_{nc \text{ times}} = \overline{n}$ and hence $\overline{k}$ generates $\mathbb{Z}_m$. Next, if $(k, m) = r > 1$ then consider $n = m/r < m$. We then have $\underbrace{\overline{k} + \overline{k} + \cdots + \overline{k}}_{n \text{ times}} = \overline{nk} = \overline{km/r} = \overline{(k/r)m} = (k/r)\overline{m} = \overline{0}$ and so $\overline{k}$ does not generate $\mathbb{Z}_m$ (it generates a subgroup of order at most $n = m/r$). So $\overline{k}$ is a generator of $\mathbb{Z}_m$ if and only if $(k, m) = 1$. Equivalently, a^k is a generator of finite order cyclic group $G = \langle a \rangle$ if and only if $(k, m) = 1$. □

Theorem I.3.6 (continued)

Proof (continued). Let G be finite. By Theorem I.3.2, $G \cong \mathbb{Z}_m$ where m is the order of G. If $(k, m) = 1$ then there are $c, d \in \mathbb{Z}$ such that $ck + dm = 1$ (by Theorem 0.6.5 in Section I.3. Cyclic Groups). Then $\underbrace{\overline{k} + \overline{k} + \cdots + \overline{k}}_{c \text{ times}} = \overline{1}$. So for any $\overline{n} \in \mathbb{Z}_m$, we have $\underbrace{\overline{k} + \overline{k} + \cdots + \overline{k}}_{nc \text{ times}} = \overline{n}$ and hence $\overline{k}$ generates $\mathbb{Z}_m$. Next, if $(k, m) = r > 1$ then consider $n = m/r < m$. We then have $\underbrace{\overline{k} + \overline{k} + \cdots + \overline{k}}_{n \text{ times}} = \overline{nk} = \overline{km/r} = \overline{(k/r)m} = (k/r)\overline{m} = \overline{0}$ and so $\overline{k}$ does not generate $\mathbb{Z}_m$ (it generates a subgroup of order at most $n = m/r$). So $\overline{k}$ is a generator of $\mathbb{Z}_m$ if and only if $(k, m) = 1$. Equivalently, a^k is a generator of finite order cyclic group $G = \langle a \rangle$ if and only if $(k, m) = 1$. $\square$