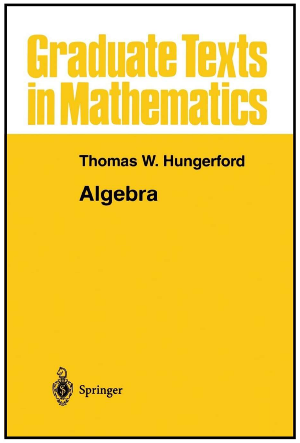
# Modern Algebra

**Chapter I. Groups**

I.2. Homomorphisms and Subgroups—Proofs of Theorems








## Theorem I.2.3

**Theorem I.2.3.** Let $f : G \to H$ be a homomorphism of groups. Then:

(*i*) $f$ is a monomorphism if and only if $\text{Ker}(f) = \{e_G\}$;

(*ii*) $f$ is an isomorphism if and only if there is a homomorphism $f^{-1} : H \to G$ such that $ff^{-1} = 1_H$ and $f^{-1}f = 1_G$.

**Proof. (i)** If $f$ is a monomorphism then $f$ is one to one (by definition) and if $a \in \text{Ker}(f)$ then $f(a) = e_H$. But $f(e_G) = e_H$ by Exercise I.2.1 (since $f$ is a homomorphism), and so $f(a) = e_H = f(e_G)$ and the one to one-ness of $f$ implies that $a = e_G$. That is, $\text{Ker}(f) = \{e_G\}$. Next, if $\text{Ker}(f) = \{e_G\}$ and $f(a) = f(b)$, then

$$\begin{aligned} e_H &= f(a)f(b)^{-1} \\ &= f(a)f(b^{-1}) \text{ by Exercise I.2.1} \\ &= f(ab^{-1}) \text{ since } f \text{ is a homomorphism} \end{aligned}$$

and so $ab^{-1} \in \text{Ker}(f)$. But then $ab^{-1} = e_G$ and $(ab^{-1})b = e_G b$ or $a = b$. That is, $f$ is one to one. □





## Theorem I.2.3 (continued)

**Theorem I.2.3.** Let $f : G \to H$ be a homomorphism of groups. Then:

(*ii*) $f$ is an isomorphism if and only if there is a homomorphism $f^{-1} : H \to G$ such that $ff^{-1} = 1_H$ and $f^{-1}f = 1_G$.

**Proof (continued) (ii)** First, suppose that $f : G \to H$ is an isomorphism. Then $f^{-1} : H \to G$ defined as $f^{-1}(h) = g$ if and only if $f(g) = h$ is an isomorphism of $H$ with $G$ (see Note 1 parts (a) and (b); also Fraleigh's Exercise 3.26). Then, of course, $f^{-1}$ is a homomorphism. Also, $ff^{-1} = 1_H$ and $f^{-1}f = 1_G$.

Second, suppose that there is a homomorphism $f^{-1} : H \to G$ such that $ff^{-1} = 1_H$ and $f^{-1}f = 1_G$. Then by Note 1 part (c), $f^{-1}$ and $f$ are one to one; by Note 1 part (d), $f^{-1}$ and $f$ are onto. So $f^{-1}$ is a one to one and onto homomorphism, and so is $f$. That is, $f$ is an isomorphism. □





## Theorem I.2.5

**Theorem I.2.5.** Let $H$ be a nonempty subset of a group $G$. Then $H$ is a subgroup of $G$ if and only if $ab^{-1} \in H$ for all $a, b \in H$.

**Proof.** Suppose that $ab^{-1} \in H$ for all $a, b \in H$. Since $H \neq \varnothing$ then there is $a \in H$ and so $aa^{-1} = e \in H$ (the identity in $G$ is also the identity in $H$). So for $b \in H$, we have $eb^{-1} = b^{-1} \in H$. So if $a, b \in H$ we have $b^{-1} \in H$ and hence $a(b^{-1})^{-1} = ab \in H$ and $H$ is closed under the binary operation. Associativity in $H$ is "inherited" from $G$. So $H$ has an associative binary operation ($H$ is a semigroup), $H$ has an identity ($H$ is a monoid) and each element of $H$ has an inverse in $H$ ($H$ is a group). Therefore $H$ is a subgroup of $G$.

If $H$ is a subgroup of $G$, then for all $a, b \in H$ we must have $b^{-1} \in H$ and so $ab^{-1} \in H$. □

## Theorem I.2.8

**Theorem I.2.8.** If $G$ is a group and $X$ is a nonempty subset of $G$, then the subgroup $\langle X\rangle$ generated by $X$ consists of all finite products $a_1^{n_1}a_2^{n_2}\cdots a_t^{n_t}$ (where $a_i \in X$ and $n_i \in \mathbb{Z}$ for $i = 1, 2, \ldots, t$). In particular, for every $a \in G$, $\langle a\rangle = \{a^n \mid n \in \mathbb{Z}\}$.

**Proof.** Let $H = \{a_1^{n_1}a_2^{n_2}\cdots a_t^{n_t} \mid t \in \mathbb{N}, a_i \in X, n_i \in \mathbb{Z}\}$. Let $x \in X$. With $t = 1$, $a_1 = x$, and $n_1 = 1$ we see that $x \in H$, so $X \subseteq H$. Now $H \subseteq G$ and $H$ is "clearly" closed under the binary operation, so $H$ is a semigroup (associativity in $H$ is inherited from $G$). For any $x \in X$, with $t = 1$, $a_1 = x$, and $n_1 = 0$, we have that $x^0 = e \in H$, so $H$ is a monoid. For any $a_1^{n_1}a_2^{n_2}\cdots a_t^{n_t} \in H$, we also have $a_t^{-n_t}a_{t-1}^{-n_{t-1}}\cdots a_1^{-n_1} \in H$ and $(a_1^{n_1}a_2^{n_2}\cdots a_t^{n_t})(a_t^{-n_t}a_{t-1}^{-n_{t-1}}\cdots a_1^{-n_1}) = e$. Hence, $H$ is a subgroup of $G$ that contains $X$. That is, $\langle X\rangle < H$.





## Theorem I.2.8 (continued)

**Theorem I.2.8.** If $G$ is a group and $X$ is a nonempty subset of $G$, then the subgroup $\langle X\rangle$ generated by $X$ consists of all finite products $a_1^{n_1}a_2^{n_2}\cdots a_t^{n_t}$ (where $a_i \in X$ and $n_i \in \mathbb{Z}$ for $i = 1, 2, \ldots, t$). In particular, for every $a \in G$, $\langle a\rangle = \{a^n \mid n \in \mathbb{Z}\}$.

**Proof (continued).** Let $H_i$ be a subgroup of $G$ containing $X$. Then for $a_1^{n_1}a_2^{n_2}\cdots a_t^{n_t} \in H$ we have $a_1, a_2, \ldots, a_t \in X \subseteq H_i$. Since $H_i$ is a group then (see Definition I.1.8) $a_1^{n_1}, a_2^{n_2}, \ldots, a_t^{n_t} \in H_i$. Since $H_i$ is a group, it is closed under the binary operation and so $a_1^{n_1}a_2^{n_2}\cdots a_t^{n_t} \in H_i$. So $H < H_i$ for all such $H_i$. Therefore $H < \cap_{i\in I} H_i = \langle X\rangle$. Hence $H < \langle X\rangle < H$ and it must be that $H = \langle X\rangle$ and the result follows. □