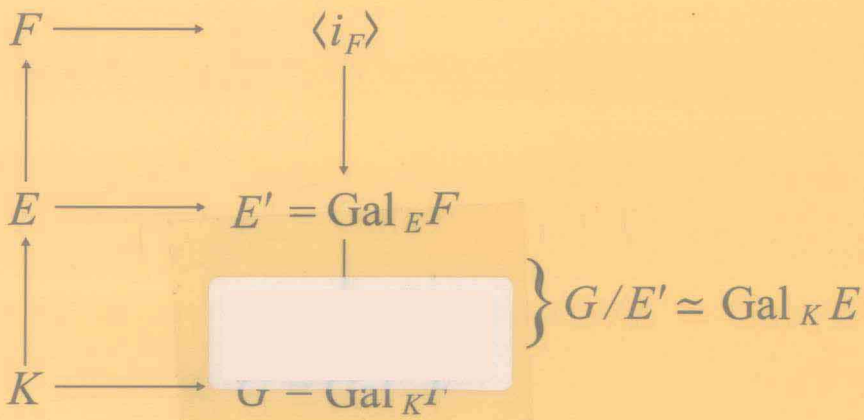
Maureen H. Fenrick

# Introduction to the Galois Correspondence

**Second Edition**

## 伽罗瓦对应导论 第2版




Birkhäuser

世界图书出版公司
www.wpcbj.com.cn

Maureen H. Fenrick

# *Introduction to the Galois Correspondence*

*Second Edition*

Birkhäuser
Boston • Basel • Berlin

**图书在版编目(CIP)数据**

伽罗瓦对应导论:第2版 = Introduction to the Galois Correspondence 2nd ed:英文/(美)芬威克(Fenrick,M. H.)著. —影印本. —北京:世界图书出版公司北京公司,2011.7
ISBN 978-7-5100-3760-3

Ⅰ.①伽… Ⅱ.①芬… Ⅲ.①伽罗瓦理论—英文 Ⅳ.①O153.4

中国版本图书馆CIP数据核字(2011)第139077号

---

**书　　名:** Introduction to the Galois Correspondence 2nd ed.
**作　　者:** Maureen H. Fenrick
**中 译 名:** 伽罗瓦对应导论 第2版
**责任编辑:** 高蓉　刘慧

---

**出 版 者:** 世界图书出版公司北京公司
**印 刷 者:** 三河市国英印务有限公司
**发　　行:** 世界图书出版公司北京公司(北京朝内大街137号　100010)
**联系电话:** 010-64021602,010-64015659
**电子信箱:** kjb@wpcbj.com.cn

---

**开　　本:** 24开
**印　　张:** 11
**版　　次:** 2011年07月
**版权登记:** 图字:01-2011-2543

---

**书　　号:** 978-7-5100-3760-3/O·884　　**定　　价:** 39.00元

# Preface

In this presentation of the Galois correspondence, modern theories of groups and fields are used to study problems, some of which date back to the ancient Greeks. The techniques used to solve these problems, rather than the solutions themselves, are of primary importance.

The ancient Greeks were concerned with *constructibility* problems. For example, they tried to determine if it was possible, using straightedge and compass alone, to perform any of the following tasks?

(1) Double an arbitrary cube; in particular, construct a cube with volume twice that of the unit cube.
(2) Trisect an arbitrary angle.
(3) Square an arbitrary circle; in particular, construct a square with area $\pi$.
(4) Construct a regular polygon with $n$ sides for $n > 2$.

If we define a real number $c$ to be constructible if, and only if, the point $(c, 0)$ can be constructed starting with the points (0,0) and (1,0), then we may show that the set of constructible numbers is a subfield of the field $\boldsymbol{R}$ of real numbers containing the field $\boldsymbol{Q}$ of rational numbers. Such a subfield is called an intermediate field of $\boldsymbol{R}$ over $\boldsymbol{Q}$. We may thus gain insight into the constructibility problems by studying intermediate fields of $\boldsymbol{R}$ over $\boldsymbol{Q}$. In chapter 4 we will show that (1) through (3) are not possible and we will determine necessary and sufficient conditions that the integer $n$ must satisfy in order that a regular polygon with $n$ sides be constructible.

Another problem of interest to mathematicians was the possibility of finding solutions of polynomial equations which use only rational operations and the extraction of roots. The student is no doubt familiar with the quadratic formula which gives the solutions to the general quadratic equation and was discovered by the Moslems around 900 A.D. The solutions to the general cubic were discovered by Tartaglia and Cardan in the mid 16th century and the general quartic equation was solved by Ferrari, also in the mid 16th century. The solution to the general fifth degree equation continued to elude mathematicians however, and it wasn't until 1828 that Abel, who died at the age of 27, produced a proof of the *unsolvability* of the general quintic.

Évariste Galois, who died in 1832 at the age of 21, in what some historians believe to be a politically motivated duel, determined *necessary and*

*sufficient* conditions that a polynomial equation be solvable by radicals. His unique approach led to the development of the modern theory of groups and fields. Galois died before achieving recognition and his work was not published until 14 years after his death. It is interesting to note that one of his teachers wrote the following about Galois: "Erratic, talkative. I believe that his ambition is to wear me out. He would be very bad for his classmates if he had any influence on them"(cf. reference [9], page 64).

The student should understand the difficulty of dealing with the types of questions just presented. How does one show that a solution *cannot* exist? This is quite different than just saying that one cannot find a solution! The Galois correspondence defines, for each field extension $F$ over $K$, a related group, called the Galois group of $F$ over $K$. One then studies field extensions by studying the related Galois group. It will be shown that a polynomial equation is solvable by radicals if, and only if, the Galois group of a certain related field extension is a solvable group. We will then be able to produce polynomials with Galois groups which are not solvable, and thereby produce polynomial equations which are not solvable by radicals.

In a similar manner, we will use our knowledge of group theory to classify those integers $n$ such that a regular polygon with $n$ sides is constructible. We use the Galois correspondence to replace field extensions, which are often infinite, with their related Galois group, which is often finite. We then study the groups and use this information, together with the Galois correspondence, to make conclusions about the field extensions.

It is my hope that the interested student who works through the problems and studies the applications presented in this book will come to understand and appreciate both the power and the elegance of the Galois correspondence in mathematics.

## To The Instructor

The theory of the Galois correspondence is perhaps one of the most elegant areas of mathematics. It can be presented to students of mathematics fairly early in their studies. One needs only a grasp of the elementary theory of groups, rings and vector spaces to begin.

It is one of the few areas of mathematics where major problems can be stated at the beginning of the course without first having to introduce new definitions and concepts. The students then have a goal in mind and an interest in the development.

Although it is recommended that the student have had a course in elementary abstract algebra, this book is self-contained. It is assumed only that the student has achieved a certain level of mathematical sophistication and is familiar with some elementary linear algebra (in particular, the concepts of vector spaces, bases and dimension).

The first chapter presents, in compact form, the necessary background in

groups and rings. The examples in this chapter are somewhat sparse and we concentrate on those examples which will be needed later. For most students, much of the material in this chapter will provide the necessary review of topics already studied and only those topics not previously covered need be studied in detail.

The intention in this chapter is to emphasize the procedure one uses to study algebraic structures. In groups, we study normal subgroups and quotient groups and we often try to ascertain information about a group $G$ given information about a normal subgroup $N$ of $G$ and the quotient group $G/N$. This is the method we will use to analyze Galois groups.

I have resisted the temptation to treat topics in a more general setting in this chapter; my goal is to provide a firm foundation for the study of the Galois correspondence. For example, we prove that if a prime $p$ divides the order of a group $G$, then $G$ contains a Sylow $p$-subgroup, but we do not discuss how many such subgroups may exist. Similarly, we discuss the decomposition of finite, abelian groups, rather than give the more general theorem on finitely generated abelian groups. We present the necessary theorems concerning polynomial rings over fields, without spending time discussing the more general concept of Euclidean domains and unique factorization domains. My experience has been that it is sometimes difficult to gather the necessary information from these more general theorems and still have time to adequately cover the Galois correspondence. We thus advance as needed on a straight and narrow path to the topic of interest.

This second edition includes appendices which provide more in-depth coverage of of some of the theory of groups and rings. Although the first chapter is presented independently of these appendices, the instructor might choose to include these topics at the appropriate time.

In Appendix A the concepts of group actions, orbits, stabilizers and fixed points are introduced and a generalization of the class equation is given. Various group action results are then used to prove the three Sylow theorems. A new section on free groups, generators and relations has been added to formalize the development of groups like the dihedral groups which are defined via generators and relations.

An appendix on factoring in integral domains had been added to generalize the concept of factoring in polynomial rings over fields. The instructor might wish to include this material after the presentation of polynomials rings given in section 5 of the first chapter.

We have also added an appendix on vector spaces covering the concepts of linearly independent and spanning sets, bases and dimension. This appendix provides a concise review of the vector space theory needed for our study of the Galois correspondence.

In the chapters on field extensions and the Galois corresondence, many examples have been provided. Most of the examples include exercises which involve verifying related facts. I feel that this is a good way for the student to test his or her understanding of the example and such a test should not

wait until the end of the section. The exercises presented at the end of the sections are more general and of varying degrees of difficulty. Many of these exercises include hints to get the student started.

Whenever possible, illustrations have been included as an aid to visualizing the Galois correspondence, and critical equations and isomorphisms have been displayed (rather than hidden within a paragraph).

The presentation of Galois theory concludes in chapter 4 with the discussion of some of the diverse applications of the Galois correspondence. These applications illustrate how the Galois correspondence might be used to study the related Galois group of a field extension and thus produce information concerning the field extension itself.

A preliminary version of this text has been class-tested at Mankato State University. The students had previously had the equivalence of a one semester course in elementary abstract algebra. We were able to cover, in a one quarter course, the material in the first chapter on Sylow subgroups, finite abelian groups and solvable groups, all of the second and third chapters, and the first section of the fourth chapter. The development led from solvable groups to solvable polynomials and concluded with the study of the use of the Galois correspondence in solving the classical constructibility problems.

It should be possible to cover the entire text in a one semester course (provided the students have had an elementary abstract algebra course), including whatever material may be necessary from the first chapter and any desirable topics from the appendices.

### Paths through the Second Edition

*Option One:* For those who wish to get to the Galois correspondence as quickly as possible, the first chapter covers, in very compact form, the necessary background in groups and rings. The students will probably have seen much of this theory and will receive the necessary review by reading this material and doing some of the exercises. Appendix C has been added for those who need a quick review of the necessary vector space theory.

*Option Two:* For a more in-depth course, it is suggested that Appendices A and B also be included.

In order to cover the first section of Appendix A on group actions and the Sylow theorems, the student should be familiar with the material from the first two sections of chapter 1 through Cauchy's Theorem for Abelian Groups. The instructor could cover through [2.23] in chapter 1 and include any of the exercises in section 2 except [2.20], [2.23] and [2.25]. A much more in-depth coverage of the Sylow theorems using group actions can then be presented using the first section of Appendix A.

The second section of Appendix A on free groups, generators and relations is quite independent of the first section and may be covered at the

instructor's discretion.

Appendix B on factoring in integral domains covers such concepts as Euclidean domains, principal ideal domains and unique factorization domains. It is suggested that this be included after covering all of section 5 in the first chapter. The student will then have the quite concrete example of polynomial rings over fields before approaching the more general concepts presented in Appendix B.

Finally, the student might be referred to Appendix C for the necessary review of vector spaces over fields at the beginning of chapter 2.

## Acknowledgements

I wish to express my appreciation to the department of Mathematics and Statistics at Mankato State University for their support during the writing of this manuscript. I am also grateful to the students who helped to eliminate many of the misprints and whose questions led to some rewriting and clarification. In addition, I would like to thank Joan Reinen in the computer services department at Mankato State University for her assistance above and beyond the call of duty in the printing of the preliminary version of this book. Finally, special thanks go to my parents and family members, and especially to Nancy and Michael, for their support and encouragement.

Maureen H. Fenrick
Department of Mathematics, Astronomy and Statistics
Mankato State University
Mankato, MN 56002-8400

**Library of Congress Cataloging-in-Publication Data**

Fenrick, Maureen H., 1946-
Introduction to the Galois correspondence / Maureen H. Fenrick. -- 2nd ed.
p. cm.
Includes bibliographical references (p. - ) and index.
ISBN 0-8176-4026-6 (acid-free paper).
1. Galois correspondence. I. Title.
QA248.F46 1998
512--dc21 97-30391
CIP

AMS Classification Codes: 20-01, 16-01, 12-01


First edition 1992

*Birkhäuser*



ISBN 0-8176-4026-6
ISBN 3-7643-4026-6

This reprint has been authorized by Springer-Verlag (Berlin/Heidelberg/New York) for sale in the Mainland China only and not for export therefrom.

# Contents

# Chapter I

## Preliminaries – Groups and Rings

In this chapter we present the background required in the study of the Galois correspondence. We give the basic definitions and theorems of the elementary theory of groups and rings, concentrating on examples that will be used in later chapters. Although some of the more straightforward proofs are left as exercises, the majority of the proofs in the first two sections are presented fully as we guide the student through the process of studying groups via their normal subgroups and quotient groups.

We conclude the second section with the proof of the existence of a Sylow $p$-subgroup in a general group whose order is a multiple of the prime $p$. This theorem is not only important in its own right, but provides a nice illustration of the technique of using normal subgroups and quotient groups in inductive arguments involving finite groups.

In Section 3, we show that finite, abelian groups can be completely classified as direct products of cyclic groups. A group $G$ is then said to be a solvable group if there is a finite chain of subgroups from $\{e\}$ to $G$ such that each subgroup is normal in the next, and each resulting quotient group is abelian. If $G$ is a finite, solvable group, then each of these quotient groups is a direct product of cyclic groups. We also show that, if $N$ is a normal subgroup of a group $G$, and the groups $N$ and $G/N$ are both solvable, then the group $G$ is also solvable. This fact will prove to be very useful in inductive arguments in Chapter 4.

In the fourth section we study rings via their ideals and quotient rings. We define integral domain and field and determine, in commutative rings with identity, which types of ideals produce quotient rings which are integral domains or fields. We conclude Section 4 with the construction of the field of fractions from an integral domain (a procedure which is similar to the construction of the field of rational numbers from the ring of integers).

In the last section of Chapter 1, we study polynomial rings $F[x]$ where $F$ is a field. In particular, we discuss methods for determining whether a given polynomial is irreducible over the field in question.

## 1. Introduction to Groups

**Definition [1.1].** *A group $\langle G, * \rangle$ is a nonempty set $G$, together with a binary operation $*$ on $G$ which satisfies the following properties.*

(1) *Associativity: For all $x, y, z \in G$, $(x * y) * z = x * (y * z)$.*
(2) *Existence of identity: There is an element $e \in G$ such that $e * x = x = x * e$ for all $x \in G$.*
(3) *Existence of inverses: For each $x \in G$, there is an element $y \in G$ such that $x * y = e = y * x$.*

If $\langle G, * \rangle$ is a group, we will often suppress the symbol $*$ for the binary operation and write $xy$ instead of $x * y$. In this case, we speak simply of the group $G$ rather than $\langle G, * \rangle$.

**Theorem [1.2].** *Let $G$ be a group. Then $G$ satisfies the following assertions.*

(1) *The identity of $G$ is unique.*
(2) *Every element $x \in G$ has a unique inverse (we generally denote the inverse of $x$ by $x^{-1}$).*
(3) *If $x, y \in G$, then $(xy)^{-1} = y^{-1}x^{-1}$.*

*Proof.* The proof is left to the reader. (See Exercise [1.1].) Q.E.D.

If $G$ is a group and $x \in G$, we define $x^0 = e$, and if $n \in \boldsymbol{N}$, $x^n$ is defined inductively by $x^n = xx^{n-1}$. We also define $x^{-n} = (x^{-1})^n$. It may be shown that $(x^n)^m = x^{mn} = (x^m)^n$ for all $x \in G$ and $n, m \in \boldsymbol{Z}$.

If $G$ is a finite group with $n$ elements, we say that $G$ is a group of *order* $n$ and we write $o(G) = n$.

A group $\langle G, * \rangle$ is said to be an *abelian* group if, and only if,

$$x * y = y * x \text{ for all } x, y \in G.$$

If $G$ is abelian, we will often use the additive notation $x + y$ for the group operation. We then call $G$ an *additive* group. In this case, we use the symbol 0 for the identity, $-x$ for the inverse of $x$, and $nx$ in place of $x^n$.

**Examples [1.3].**

**[1.3.1]** We will use the symbols $\boldsymbol{Z}$, $\boldsymbol{Q}$, $\boldsymbol{R}$ and $\boldsymbol{C}$ for the set of integers, rationals, reals, or complex numbers respectively. Each of these sets forms an infinite abelian group under addition.

If we denote the set of nonzero rationals, reals, complex numbers respectively by $\boldsymbol{Q}^*$, $\boldsymbol{R}^*$, $\boldsymbol{C}^*$ respectively, then each of these sets is an infinite abelian group under multiplication.

**[1.3.2]** *The group $\boldsymbol{Z}_n$:* If $n \in \boldsymbol{N}$ we define a relation $\equiv_n$ on the set $\boldsymbol{Z}$ by

$$a \equiv_n b \text{ if and only if } n \text{ divides } a - b.$$

We will sometimes use the notation $a \equiv b \pmod{n}$ instead of $a \equiv_n b$.

If $a \equiv_n b$, we say that $a$ is *congruent* to $b$ modulo $n$. The relation $\equiv_n$ is an equivalence relation on the set $\boldsymbol{Z}$.

If $a \in \boldsymbol{Z}$, we denote the equivalence class of $a$ under the relation $\equiv_n$ by $\widehat{a}$. The $n$ distinct equivalence classes $\widehat{0}, \widehat{1}, \ldots, \widehat{n-1}$ then partition the set $\boldsymbol{Z}$. Let

$$\boldsymbol{Z}_n = \{\widehat{0}, \widehat{1}, \ldots, \widehat{n-1}\}.$$

It may be verified that, if $a, b, c, d \in \boldsymbol{Z}$ and $a \equiv_n c$ and $b \equiv_n d$, then $a + b \equiv_n c + d$. Thus, if we define $+$ on $\boldsymbol{Z}_n$ by

$$\widehat{a} + \widehat{b} = \widehat{a+b},$$

then $+$ is independent of the choice of representatives for the equivalence classes, and hence is a well-defined binary operation on the set $\boldsymbol{Z}_n$. It may be verified that $\langle \boldsymbol{Z}_n, + \rangle$ is an abelian group of order $n$.

*Exercises.*

(a) Prove that $\equiv_n$ is an equivalence relation on $\boldsymbol{Z}$.

(b) Use the division algorithm on $\boldsymbol{Z}$ to prove that, for every $m \in \boldsymbol{Z}$, there is a unique $r \in \boldsymbol{Z}$ with $0 \leq r < n$ such that $m \equiv_n r$.

(c) Prove that, if $a, b, c, d \in \boldsymbol{Z}$ and $a \equiv_n c$ and $b \equiv_n d$, then $a + b \equiv_n c + d$. Explain why this implies that $+$ is a well-defined operation on the set $\boldsymbol{Z}_n$.

**[1.3.3]** *The group $\boldsymbol{Z}_n^\times$:* As in the preceding example, if $a, b, c, d \in \boldsymbol{Z}$ and $a \equiv_n c$ and $b \equiv_n d$, then it may be shown that $ab \equiv_n cd$. Hence if we define multiplication on $\boldsymbol{Z}_n$ by

$$\widehat{a}\widehat{b} = \widehat{ab},$$

then multiplication is a well-defined binary operation on $\boldsymbol{Z}_n$. The element $\widehat{1}$ is an identity for multiplication on $\boldsymbol{Z}_n$. We define

$$\boldsymbol{Z}_n^\times = \{\widehat{a} \in \boldsymbol{Z}_n : gcd(a, n) = 1\}.$$

Recall the following property of the set of integers: $(*)$ if $a \in \boldsymbol{Z}$, then $a$ and $n$ are relatively prime if, and only if, there are integers $x$ and $y$ such that $ax + ny = 1$.

It may then be verified that, if $a \equiv_n b$, then gcd $(a, n) = 1$ if, and only if, gcd $(b, n) = 1$, so that the definition of the set $\boldsymbol{Z}_n^\times$ is independent of the particular representative chosen from the equivalence class.

If $\widehat{a} \in \boldsymbol{Z}_n^\times$, then, by $(*)$, since $a$ and $n$ are relatively prime, there are integers $x$ and $y$ such that $ax + ny = 1$. But then, again by $(*)$, $x$ is also relatively prime to $n$ (so that $\widehat{x} \in \boldsymbol{Z}_n^\times$) and $ax \equiv_n 1$. Thus $\widehat{a}\widehat{x} = \widehat{1}$ and $\widehat{x}$ is an inverse for $\widehat{a}$.

In a similar manner one may show that, if $\hat{a}, \hat{b} \in Z_n^\times$, then $\widehat{ab}$ is also an element of $Z_n^\times$. Then $Z_n^\times$ is a group under multiplication and elements of $Z_n^\times$ are precisely those elements of $Z_n$ which have multiplicative inverses.

The order of the group $Z_n^\times$ is $\phi(n)$ where $\phi$ is the Euler function defined on $N$ by

$$\phi(n) = \text{ card } \{m \in N : m < n \text{ and } gcd(m,n) = 1\}.$$

*Exercises.*

(a) Prove that multiplication is a well-defined operation on the set $Z_n$.
(b) Prove that $\langle Z_n^\times, \cdot \rangle$ is a group.
(c) Write out a multiplication table for the group $Z_{12}^\times$.
(d) Prove that, for any prime $p$ and $k \in N$, $\phi(p^k) = p^{k-1}(p-1)$.

**[1.3.4]** *The group $S_n$:* If $n \in N$, let $I_n = \{1, 2, \ldots, n\}$ and let $S_n$ denote the set of bijections from $I_n$ to itself. The elements of $S_n$ are called permutations. For example,

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

denotes the element of $S_4$ defined by $\alpha(1) = 3$, $\alpha(2) = 4$, $\alpha(3) = 1$ and $\alpha(4) = 2$.

$S_n$ is a group of order $n!$ under composition of functions. Recall that composition of functions is read from right to left and thus, if $\alpha$ and $\beta$ are elements of $S_n$ for some $n$, $\alpha\beta$ is the permutation of $I_n$ whose action is determined by first applying $\beta$ and then applying $\alpha$.

If $A = \{a_1, a_2, \ldots, a_m\} \subseteq I_n$, we write

$$\alpha = (a_1 \quad a_2 \quad \ldots \quad a_m)$$

for the element of $S_n$ defined by $\alpha(a_i) = a_{i+1}$ for $1 \leq i < m$, $\alpha(a_m) = a_1$ and $\alpha$ fixes all elements of $I_n$ which are not in $A$. An element of this type is called an *m-cycle* and is said to have length $m$. The identity permutation is said to be a cycle of length 0. It may be shown that every element of $S_n$ can be written as a product of *disjoint* cycles. For example, if

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 5 & 3 & 6 \end{pmatrix} \in S_6,$$

then $\alpha(1) = 2$, and $\alpha(2) = 1$, producing the cycle $(1 \quad 2)$, and $\alpha(3) = 4$, $\alpha(4) = 5$ and $\alpha(5) = 3$, producing the cycle $(3 \quad 4 \quad 5)$. Since $\alpha$ fixes 6 we see that

$$\alpha = (1 \quad 2)(3 \quad 4 \quad 5).$$

A 2-cycle is called a *transposition*. If $\alpha = (a_1 \quad a_2 \quad \dots \quad a_m)$, then

$$\alpha = (a_m \quad a_{m-1})(a_m \quad a_{m-2}) \dots (a_m \quad a_1)$$

and it follows that every element of $S_n$ can be written as a product of transpositions.

*Exercises.*

(a) Prove that every nontrivial element of $S_n$ can be written as a product of disjoint cycles with the cycles appearing in the product unique.
(b) Prove that, if $\alpha$ and $\beta$ are disjoint cycles in $S_n$, then $\alpha\beta = \beta\alpha$.
(c) Give an example to show that cycles which are not disjoint do not generally commute.
(d) Write every element of $S_3$ as a product of transpositions.

**[1.3.5]** If $\langle G, * \rangle$ and $\langle G', \star \rangle$ are groups, then the cross product $G \times G'$ is a group (called the *direct product* of $G$ and $G'$) under the operation

$$(a, a')(b, b') = (a * b,\ a' \star b') \qquad (\text{for } a, b \in G, a', b' \in G').$$

If $G$ and $G'$ are finite groups of order $n$ and $m$ respectively, then $G \times G'$ is a finite group of order $nm$.

**Definition [1.4].** *Let $\langle G, * \rangle$ be a group. A subset $H$ of $G$ is a subgroup of $G$ if, and only if, $\langle H, * \rangle$ is also a group (that is, $H$ is a group using the same operation as that of $G$).*

The group $G$ itself and the *trivial* subgroup $\{e\}$ are always subgroups of a given group $G$. Any subgroup other than $\{e\}$ is referred to as a *nontrivial* subgroup of $G$.

The reader should verify that, if $H$ is a subgroup of $G$, then the identity of $H$ is the same as the identity of $G$. The following propositions are useful in identifying subgroups of a given group.

**Proposition [1.5].** *Let $G$ be a group and $H$ a nonempty subset of $G$. Then $H$ is a subgroup of $G$ if, and only if, the following two closure conditions are satisfied.*

(1) *If $x, y \in H$, then $xy \in H$.*
(2) *If $x \in H$, then $x^{-1} \in H$.*

*Moreover, if $H$ is finite, then (1) suffices.*

*Proof.* If $H$ is a subgroup of $G$, then the binary operation on $G$ restricts to a binary operation on $H$ and hence $H$ is closed under products. Since the identity of $H$ is the same as the identity of $G$, and every element of $H$ contains an inverse in $H$, $H$ is closed under inverses.

Now suppose that $H$ is a nonempty subset of $G$ satisfying (1) and (2). Then, by (1), the associative binary operation on $G$ restricts to an associative binary operation on $H$ and every element in $H$ has an inverse in $H$. Since $H \neq \emptyset$, there is an element $x \in H$. By (2), $x^{-1} \in H$ and hence, by (1), $xx^{-1} \in H$. Hence $e \in H$ and the result follows.

The proof of the final assertion is outlined in exercise [1.3]. Q.E.D.

Often the following proposition is a more efficient means of determining whether a given nonempty subset of a group is a subgroup.

**Proposition [1.6].** *Let $H$ be a nonempty subset of a group $G$. Then $H$ is a subgroup of $G$ if, and only if, whenever $x, y \in H$, then $xy^{-1} \in H$.*

*Proof.* The proof is left to the reader - cf. Exercise [1.2]. Q.E.D.

**Example.** Let $G$ be a group and $x \in G$. The reader should verify that the following sets are subgroups of $G$ (cf. Exercise [1.5]).

(1) $Z(G) = \{y \in G : yx = xy \text{ for all } x \in G\}$, called the *center* of the group $G$. Note that $G$ is abelian if, and only if, $Z(G) = G$.

(2) $C(x) = \{y \in G : yx = xy\} = \{y \in G : yxy^{-1} = x\}$, called the *centralizer* of $x$ in $G$.

**Definition [1.7].** *Let $X$ be a subset of a group $G$. The subgroup generated by $X$ is the set $\langle X \rangle$ defined by*

$$\langle X \rangle = \cap \{H : H \text{ is a subgroup of } G \text{ containing } X\}.$$

The reader should verify that $\langle X \rangle$ is a subgroup of $G$ containing $X$ and that, if $K$ is any other subgroup of $G$ containing $X$, then $\langle X \rangle \subseteq K$. The following proposition gives a more concrete description of $\langle X \rangle$.

**Proposition [1.8].** *Let $X$ be a subset of a group $G$. Then $\langle X \rangle$ consists of all finite products of the form*

$$x_1^{k_1} x_2^{k_2} \dots x_n^{k_n}$$

*where $n \in N$ and, for each $1 \leq i \leq n$, $x_i \in X$ and $k_i = \pm 1$. Moreover, if $G$ is finite, then we may take $k_i = 1$ for each $i$. (We interpret a product of length 0 as $e$ so that $\langle \emptyset \rangle = \{e\}$).*

*Proof.* Let $S$ be the set of all finite products of the given form. Each of the following facts may be verified.

(i) $X \subseteq S$.

(ii) $S$ is a subgroup of $G$.

(iii) If $H$ is a subgroup of $G$ containing $X$, then $S \subseteq H$.

See Exercise [1.6]. Q.E.D.

*Remark.* If $X$ consists of a single element $x \in G$, we write $\langle x \rangle$ instead of $\langle \{x\} \rangle$. Thus

$$\langle x \rangle = \{x^n : n \in Z\}$$

and, if $G$ is finite, then

$$\langle x \rangle = \{x^n : n \in \boldsymbol{N}\}.$$

Recall that, if $G$ is an additive group, then we write $nx$ instead of $x^n$ as above.

If $G = \langle x \rangle$, we say that $G$ is a *cyclic group with generator* $x$. If $\langle x \rangle$ has finite order $n$, we say that the element $x$ has order $n$ and write $o(x) = n$. Otherwise, we write $o(x) = \infty$. The following proposition shows that, if $x$ has finite order $n$, then $n$ is the smallest positive power of $x$ giving $e$.

**Proposition [1.9].** *Let $G$ be a group, $x \in G$ and suppose that $x$ has finite order $n$. Then the following assertions hold.*

(1) $\langle x \rangle = \{e, x, x^2, \ldots x^{n-1}\}$ *with these elements all distinct and* $x^n = e$.

(2) *If $m \in \boldsymbol{Z}$, then $x^m = e$ if, and only if, $n \mid m$. Hence, in particular, $n$ is the smallest positive power of $x$ giving $e$.*

(3) *If $k \in \boldsymbol{N}$, then $o(x^k) = n/gcd(k, n)$.*

*Proof.* (1) Since $\langle x \rangle$ is finite, and for all $k \in \boldsymbol{N}$, $x^k \in \langle x \rangle$, there must be $j < k \in \boldsymbol{N}$ such that $x^j = x^k$. Then $x^{k-j} = e$ and hence there is a positive integer power of $x$ producing $e$. Let $k$ be the smallest element of $\boldsymbol{N}$ such that $x^k = e$. Then, by the division algorithm, if $m \in \boldsymbol{Z}$, there are $q, r \in \boldsymbol{N}$ such that $m = qk + r$ and $0 \leq r < m$. Then

$$x^m = x^{qk+r} = (x^k)^q x^r = x^r$$

and hence

$$\langle x \rangle \subseteq \{e, x, x^2, \ldots x^{k-1}\}.$$

If $x^j = x^l$ with $0 \leq j < l \leq k - 1$, then $0 < l - j < k$ and $x^{l-j} = e$, contradicting the minimality of $k$. Hence the elements in the above mentioned set are distinct. Now, since $\langle x \rangle$ has $n$ elements, we see that, in fact $k = n$ and thus $n$ is the smallest positive integer power of $x$ producing $e$.

(2) As above, if $m \in \boldsymbol{Z}$, and $m = qn + r$ with $q, r \in \boldsymbol{Z}$ and $0 \leq r < n$, then

$$x^m = x^{qn+r} = (x^n)^q x^r = x^r.$$

Since $0 \leq r < n$, the minimality of $n$ gives us that $x^m = e$ if, and only if, $r = 0$; that is, if and only if $n \mid m$.

(3) We consider three cases.

Case (i): Suppose that $k \mid n$. Then $n = kr$ for some $r \in \boldsymbol{N}$. We must show that $o(x^k) = r$. Let $o(x^k) = m$. Since $(x^k)^r = x^n = e$, and $o(x^k) = m$, $m \leq r$. If $m < r$, then we would have $x^{km} = e$ with $km < kr = n$, contradicting $o(x) = n$.