Graduate Texts in Mathematics

Steven Roman

Field Theory

Second Edition

域论 第2版

Springer

世界图书出版公司
www.wpcbj.com.cn

Steven Roman

Field Theory

Second Edition

With 18 Illustrations

Springer

图书在版编目(CIP)数据

域论:第2版 = Field Theory 2nd ed:英文/(美)罗曼(Roman,S.)著.—影印本.—北京:世界图书出版公司北京公司,2011.7
ISBN 978-7-5100-3763-4

Ⅰ.①域… Ⅱ.①罗… Ⅲ.①域(数学)—英文 Ⅳ.①O153.4

中国版本图书馆 CIP 数据核字(2011)第139089号

书　　名：Field Theory 2nd ed.
作　　者：Steven Roman
中 译 名：域论 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：14.5
版　　次：2011年07月
版权登记：图字:01-2011-2561

书　　号：978-7-5100-3763-4/O·902　　定　　价：39.00元

To Donna

Preface

This book presents the basic theory of fields, starting more or less from the beginning. It is suitable for a graduate course in field theory, or independent study. The reader is expected to have taken an undergraduate course in abstract algebra, not so much for the material it contains but in order to gain a certain level of mathematical maturity.

The book begins with a preliminary chapter (Chapter 0), which is designed to be quickly scanned or skipped and used as a reference if needed. The remainder of the book is divided into three parts.

Part 1, entitled *Field Extensions*, begins with a chapter on polynomials. Chapter 2 is devoted to various types of field extensions, including finite, finitely generated, algebraic and normal. Chapter 3 takes a close look at the issue of separability. In my classes, I generally cover only Sections 3.1 to 3.4 (on perfect fields). Chapter 4 is devoted to algebraic independence, starting with the general notion of a dependence relation and concluding with Luroth's theorem on intermediate fields of a simple transcendental extension.

Part 2 of the book is entitled *Galois Theory*. Chapter 5 examines Galois theory from an historical perspective, discussing the contributions from Lagrange, Vandermonde, Gauss, Newton, and others that led to the development of the theory. I have also included a very brief look at the very brief life of Galois himself.

Chapter 6 begins with the notion of a Galois correspondence between two partially ordered sets, and then specializes to the Galois correspondence of a field extension, concluding with a brief discussion of the Krull topology. In Chapter 7, we discuss the Galois theory of equations. In Chapter 8, we view a field extension E of F as a vector space over F.

Chapter 9 and Chapter 10 are devoted to finite fields, although this material can be omitted in order to reach the topic of solvability by radicals more quickly. Möbius inversion is used in a few places, so an appendix has been included on this subject.

Part 3 of the book is entitled *The Theory of Binomials*. Chapter 11 covers the roots of unity and Wedderburn's theorem on finite division rings. We also briefly discuss the question of whether a given group is the Galois group of a field extension. In Chapter 12, we characterize cyclic extensions and splitting fields of binomials when the base field contains appropriate roots of unity. Chapter 13 is devoted to the question of solvability of a polynomial equation by radicals. (This chapter might make a convenient ending place in a graduate course.) In Chapter 14, we determine conditions that characterize the irreducibility of a binomial and describe the Galois group of a binomial. Chapter 15 briefly describes the theory of families of binomials—the so-called *Kummer theory*.

Sections marked with an asterisk may be skipped without loss of continuity.

Changes for the Second Edition

Let me begin by thanking the readers of the first edition for their many helpful comments and suggestions.

For the second edition, I have gone over the entire book, and rewritten most of it, including the exercises. I believe the book has benefited significantly from a class testing at the beginning graduate level and at a more advanced graduate level.

I have also rearranged the chapters on separability and algebraic independence, feeling that the former is more important when time is of the essence. In my course, I generally touch only very lightly (or skip altogether) the chapter on algebraic independence, simply because of time constraints.

As mentioned earlier, as several readers have requested, I have added a chapter on Galois theory from an historical perspective.

A few additional topics are sprinkled throughout, such as a proof of the Fundamental Theorem of Algebra, a discussion of *casus irreducibilis*, Berlekamp's algorithm for factoring polynomials over $\mathbb{Z}_p$, and natural and accessory irrationalities.

Thanks

I would like to thank my students Phong Le, Sunil Chetty, Timothy Choi and Josh Chan, who attended lectures on essentially the entire book and offered many helpful suggestions. I would also like to thank my editor, Mark Spencer, who puts up with my many requests and is most amiable.

Contents

Chapter 0
Preliminaries

The purpose of this chapter is to review some basic facts that will be needed in the book. The discussion is not intended to be complete, nor are all proofs supplied. We suggest that the reader quickly skim this chapter (or skip it altogether) and use it as a reference if needed.

0.1 Lattices

Definition *A* **partially ordered set** (*or* **poset**) *is a nonempty set P, together with a binary relation* $\leq$ *on P satisfying the following properties. For all* α, β, $\gamma \in P$,

1) **(reflexivity)**

$$\alpha \leq \alpha$$

2) **(antisymmetry)**

$$\alpha \leq \beta,\ \beta \leq \alpha \Rightarrow \alpha = \beta$$

3) **(transitivity)**

$$\alpha \leq \beta,\ \beta \leq \gamma \Rightarrow \alpha \leq \gamma$$

If, in addition,

$$\alpha, \beta \in P \Rightarrow \alpha \leq \beta \text{ or } \beta \leq \alpha$$

then P is said to be **totally ordered.** □

Any subset of a poset P is also a poset under the restriction of the relation defined on P. A totally ordered subset of a poset is called a **chain.** If $S \subseteq P$ and $s \leq \alpha$ for all $s \in S$ then α is called an **upper bound** for S. A **least upper bound** for S, denoted by $\text{lub}(S)$ or $\bigvee S$, is an upper bound that is less than or equal to any other upper bound. Similar statements hold for lower bounds and greatest lower bounds, the latter denoted by $\text{glb}(S)$, or $\wedge S$. A **maximal element** in a poset P is an element $\alpha \in P$ such that $\alpha \leq \beta$ implies $\alpha = \beta$. A **minimal element** in a poset P is an element $\gamma \in P$ such that $\beta \leq \gamma$ implies

$\beta = \gamma$. A **top element** $1 \in P$ is an element with the property that $\alpha \leq 1$ for all $\alpha \in P$. Similarly, a **bottom element** $0 \in P$ is an element with the property that $0 \leq \alpha$ for all $\alpha \in P$. **Zorn's lemma** says that if every chain in a poset P has an upper bound in P then P has a maximal element.

Definition *A* **lattice** *is a poset L in which every pair of elements $\alpha, \beta \in L$ has a least upper bound, or* **join**, *denoted by $\alpha \vee \beta$ and a greatest lower bound, or* **meet**, *denoted by $\alpha \wedge \beta$. If every nonempty subset of L has a join and a meet then L is called a* **complete lattice**. □

Note that any nonempty complete lattice has a greatest element, denoted by 1 and a smallest element, denoted by 0.

Definition *A* **sublattice** *of a lattice L is a subset S of L that is closed under the meet and join operation of L.* □

It is important to note that a subset S of a lattice L can be a lattice under the same order relation and yet not be a sublattice of L. As an example, consider the coll

$\mathcal{S}$ of all subgroups of a group G, ordered by inclusion. Then $\mathcal{S}$ is a subset of the power set $\mathcal{P}(G)$, which is a lattice under union and intersection. But $\mathcal{S}$ is not a sublattice of $\mathcal{P}(G)$ since the union of two subgroups need not be a subgroup. On the other hand, $\mathcal{S}$ is a lattice in its own right under set inclusion, where the meet $H \wedge K$ of two subgroups is their intersection and the join $H \vee K$ is the smallest subgroup of G containing H and K.

In a complete lattice L, joins can be defined in terms of meets, since $\bigvee T$ is the meet of all upper bounds of T. The fact that $1 \in L$ ensures that T has at least one upper bound, so that the meet is not an empty one. The following theorem exploits this idea to give conditions under which a subset of a complete lattice is itself a complete lattice.

Theorem 0.1.1 *Let L be a complete lattice. If $S \subseteq L$ has the properties*
1) $1 \in S$
2) **(Closed under arbitrary meets)** $T \subseteq S,\ T \neq \emptyset \Rightarrow \bigwedge T \in S$
then S is a complete lattice under the same meet.

Proof. Let $T \subseteq S$. Then $\bigwedge T \in S$ by assumption. Let U be the set of all upper bounds of T that lie in S. Since $1 \in S$, we have $U \neq \emptyset$. Hence, $\bigwedge U \in S$ and is $\bigvee T$. Thus, S is a complete lattice. (Note that S need not be a sublattice of L since $\bigwedge U$ need not equal the meet of all upper bounds of T in L.) □

0.2 Groups

Definition *A* **group** *is a nonempty set G, together with a binary operation on G, that is, a map $G \times G \to G$, denoted by juxtaposition, with the following properties:*

1) **(Associativity)** $(\alpha\beta)\gamma = \alpha(\beta\gamma)$ *for all* $\alpha, \beta, \gamma \in G$
2) **(Identity)** *There exists an element* $\epsilon \in G$ *for which* $\epsilon\alpha = \alpha\epsilon = \alpha$ *for all* $\alpha \in G$
3) **(Inverses)** *For each* $\alpha \in G$, *there is an element* $\alpha^{-1} \in G$ *for which* $\alpha\alpha^{-1} = \alpha^{-1}\alpha = \epsilon$.

A group G is **abelian**, *or* **commutative**, *if* $\alpha\beta = \beta\alpha$, *for all* $\alpha, \beta \in G$.□

The identity element is often denoted by 1. When G is abelian, the group operation is often denoted by $+$ and the identity by 0.

Subgroups

Definition *A* **subgroup** S *of a group* G *is a subset of* G *that is a group in its own right, using the restriction of the operation defined on* G. *We denote the fact that* S *is a subgroup of* G *by writing* $S < G$.□

If G is a group and $\alpha \in G$, then the set of all powers of α

$$\langle\alpha\rangle = \{\alpha^n \mid n \in \mathbb{Z}\}$$

is a subgroup of G, called the **cyclic subgroup generated by** α. A group G is **cyclic** if it has the form $G = \langle\alpha\rangle$, for some $\alpha \in G$. In this case, we say that α **generates** G.

Let G be a group. Since G is a subgroup of itself and since the intersection of subgroups of G is a subgroup of G, Theorem 0.1.1 implies that the set of subgroups of G forms a complete lattice, where $H \wedge J = H \cap J$ and $H \vee J$ is the smallest subgroup of G containing both H and J.

If H and K are subgroups of G, it does not follow that the **set product**

$$HK = \{hk \mid h \in H, k \in K\}$$

is a subgroup of G. It is not hard to show that HK is a subgroup of G precisely when $HK = KH$.

The **center** of G is the set

$$Z(G) = \{\beta \in G \mid \alpha\beta = \beta\alpha \text{ for all } \alpha \in G\}$$

of all elements of G that commute with every element of G.

Orders and Exponents

A group G is **finite** if it contains only a finite number of elements. The cardinality of a finite group G is called its **order** and is denoted by $|G|$ or $o(G)$. If $\alpha \in G$, and if $\alpha^k = \epsilon$ for some integer k, we say that k is an **exponent** of α. The smallest positive exponent for $\alpha \in G$ is called the **order** of α and is denoted by $o(\alpha)$. An integer m for which $\alpha^m = 1$ for all $\alpha \in G$ is called an

exponent of G. (Note: Some authors use the term exponent of G to refer to the *smallest* positive exponent of G.)

Theorem 0.2.1 *Let G be a group and let $\alpha \in G$. Then k is an exponent of α if and only if k is a multiple of $o(\alpha)$. Similarly, the exponents of G are precisely the multiples of the smallest positive exponent of G.* □

We next characterize the smallest positive exponent for finite abelian groups.

Theorem 0.2.2 *Let G be a finite abelian group.*

1) **(Maximum order equals minimum exponent)** *If m is the maximum order of all elements in G then $\alpha^m = 1$ for all $\alpha \in G$. Thus, the smallest positive exponent of G is equal to the maximum order of all elements of G.*
2) *The smallest positive exponent of G is equal to $o(G)$ if and only if G is cyclic.* □

Cosets and Lagrange's Theorem

Let $H < G$. We may define an equivalence relation on G by saying that $\alpha \sim \beta$ if $\beta^{-1}\alpha \in H$ (or equivalently $\alpha^{-1}\beta \in H$). The equivalence classes are the **left cosets** $\alpha H = \{\alpha h \mid h \in H\}$ of H in G. Thus, the distinct left cosets of H form a partition of G. Similarly, the distinct **right cosets** $H\alpha$ form a partition of G. It is not hard to see that all cosets of H have the same cardinality and that there is the same number of left cosets of H in G as right cosets. (This is easy when G is finite. Otherwise, consider the map $\alpha H \mapsto H\alpha^{-1}$.)

Definition *The* **index** *of H in G, denoted by $(G : H)$, is the cardinality of the set G/H of all distinct left cosets of H in G. If G is finite then $(G : H) = |G|/|H|$.* □

Theorem 0.2.3 *Let G be a finite group.*

1) **(Lagrange)** *The order of any subgroup of G divides the order of G.*
2) *The order of any element of G divides the order of G.*
3) **(Converse of Lagrange's Theorem for Finite Abelian Groups)** *If A is a finite abelian group and if $k \mid o(A)$ then A has a subgroup of order k.* □

Normal Subgroups

If S and T are subsets of a group G, then the **set product** ST is defined by

$$ST = \{st \mid s \in S, t \in T\}$$

Theorem 0.2.4 *Let $H < G$. The following are equivalent*

1) *The set product of any two cosets is a coset.*
2) *If $\alpha, \beta \in G$, then*

$$\alpha H \beta H = \alpha\beta H$$

3) *Any right coset of H is also a left coset, that is, for any $\alpha \in G$ there is a $\beta \in G$ for which $H\alpha = \beta H$.*
4) *If $\alpha \in G$, then*

$$\alpha H = H\alpha$$

5) $\alpha\beta \in H \Rightarrow \beta\alpha \in H$ *for all* $\alpha, \beta \in G$.□

Definition A subgroup H of G is **normal** in G, written $H \lhd G$, if any of the equivalent conditions in Theorem 0.2.4 holds. □

Definition *A group G is* **simple** *if it has no normal subgroups other than $\{1\}$ and G.* □

Here are some normal subgroups.

Theorem 0.2.5
1) *The center $Z(G)$ is a normal subgroup of G.*
2) *Any subgroup H of a group G with $(G : H) = 2$ is normal.*
3) *If G is a finite group and if p is the smallest prime dividing $o(G)$, then any subgroup of index p is normal in G*□

With respect to the last statement in the previous theorem, it makes some intuitive sense that if a subgroup H of a finite group G is extremely large, then it may be normal, since there is not much room for conjugates. This is true in the most extreme case. Namely, the largest possible proper subgroup of G has index equal to the smallest prime number dividing $o(G)$. This subgroup, if it exists, is normal.

If $H \lhd G$, then we have the set product formula

$$\alpha H \beta H = \alpha\beta H$$

It is not hard to see that this makes the quotient G/H into a group, called the **quotient group** of H in G. The order of G/H is called the **index** of H in G and is denoted by $(G : H)$.

Theorem 0.2.6 *If G is a group and $\{H_i\}$ is a collection of normal subgroups of G then $\bigcap H_i$ and $\bigvee H_i$ are normal subgroups of G. Hence, the collection of normal subgroups of G is a complete sublattice of the complete lattice of all subgroups of G.* □

If $H < G$ then there is always an intermediate subgroup $H < K < G$ for which $H \lhd K$, in fact, H is such an intermediate subgroup. The largest such subgroup is called the **normalizer** of H in G. It is

$$N_G(H) = \{g \in G \mid gHg^{-1} = H\}$$

Euler's Formula

We will denote a greatest common divisor of α and β by (α, β) or $\gcd(\alpha, \beta)$.

If $(\alpha, \beta) = 1$, then α and β are **relatively prime**. The **Euler phi function** ϕ is defined by letting $\phi(n)$ be the number of positive integers less than or equal to n that are relatively prime to n.

Two integers α and β are **congruent modulo** n, written $\alpha \equiv \beta \bmod n$, if $\alpha - \beta$ is divisible by n. Let $\mathbb{Z}_n$ denote the ring of integers $\{0, \ldots, n-1\}$ under addition and multiplication modulo n.

Theorem 0.2.7 (Properties of Euler's phi function)
1) The Euler phi function is multiplicative, that is, if m and n are relatively prime, then

$$\phi(mn) = \phi(m)\phi(n)$$

2) If p is a prime and $n > 0$ then

$$\phi(p^n) = p^{n-1}(p-1)$$

These two properties completely determine ϕ.□

Since the set $G = \{\beta \in \mathbb{Z}_n \mid (\beta, n) = 1\}$ is a group of order $\phi(n)$ under multiplication modulo n, it follows that $\phi(n)$ is an exponent for G.

Theorem 0.2.8 (Euler's Theorem) *If $\alpha, n \in \mathbb{Z}$ and $(\alpha, n) = 1$, then*

$$\alpha^{\phi(n)} \equiv 1 \bmod n$$ □

Corollary 0.2.9 (Fermat's Theorem) *If p is a prime not dividing the integer α, then*

$$\alpha^p \equiv \alpha \bmod p$$ □

Cyclic Groups

Theorem 0.2.10
1) Every group of prime order is cyclic.
2) Every subgroup of a cyclic group is cyclic.
3) A finite abelian group G is cyclic if and only if its smallest positive exponent is equal to $o(G)$. □

The following theorem contains some key results about finite cyclic groups.

Theorem 0.2.11 *Let $G = \langle \alpha \rangle$ be a cyclic group of order n.*

1) *For* $1 \leq k < n$,

$$o(\alpha^k) = \frac{n}{(n,k)}$$

In particular, α^k *generates* $G = \langle\alpha\rangle$ *if and only if* $(n,k) = 1$.

2) *If* $d \mid n$, *then*

$$o(\alpha^k) = d \Leftrightarrow k = r\frac{n}{d}, \text{ where } (r,d) = 1$$

Thus the elements of G *of order* $d \mid n$ *are the elements of the form* $\alpha^{r(n/d)}$, *where* $0 \leq r < d$ *and* r *is relatively prime to* d.

3) *For each* $d \mid n$, *the group* G *has exactly one subgroup* H_d *of order* d *and* $\phi(d)$ *elements of order* d, *all of which lie in* H_d.

4) **(Subgroup structure charactertizes property of being cyclic)** *If a finite group* G *of order* n *has the property that it has at most one subgroup of each order* $d \mid n$, *then* G *is cyclic.* □

Counting the elements in a cyclic group of order n gives the following corollary.

Corollary 0.2.12 *For any positive integer* n,

$$n = \sum_{d \mid n} \phi(d)$$

□

Homomorphisms

Definition *Let* G *and* H *be groups. A map* $\psi: G \to H$ *is called a* **group homomorphism** *if*

$$\psi(\alpha\beta) = (\psi\alpha)(\psi\beta)$$

A surjective homomorphism is an **epimorphism**, *an injective homomorphism is a* **monomorphism** *and a bijective homomorphism is an* **isomorphism**. *If* $\psi: G \to H$ *is an isomorphism, we say that* G *and* H *are* **isomorphic** *and write* $G \approx H$. □

If ψ is a homomorphism then $\psi\epsilon = \epsilon$ and $\psi\alpha^{-1} = (\psi\alpha)^{-1}$. The **kernel** of a homomorphism $\psi: G \to H$,

$$\ker(\psi) = \{\alpha \in G \mid \psi\alpha = \epsilon\}$$

is a normal subgroup of G. Conversely, any normal subgroup H of G is the kernel of a homomorphism. For we may define the **natural projection** $\pi: G \to G/H$ by $\pi\alpha = \alpha H$. This is easily seen to be an epimorphism with kernel H.