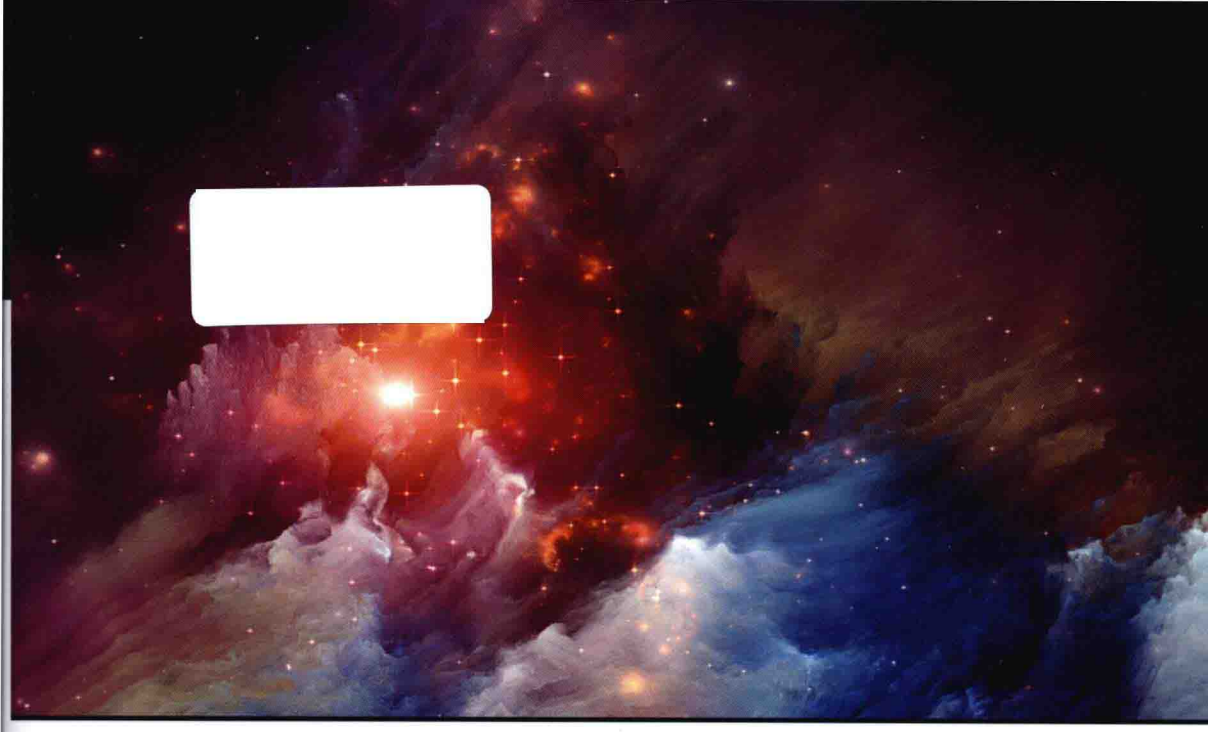

Algebraic Number Theory

Second Edition

ZHANG Xianke

Higher Education Press

Alpha Science

Algebraic Number Theory

SECOND EDITION

ZHANG Xianke

Algebraic Number Theory provides concisely both the fundamental and profound theory, starting from the succinct ideal theory (Chapters 1-3), turning then to valuation theory and local completion field (Chapters 4-5) which is the base of modern approach. After specific discussions on class numbers, units, quadratic and cyclotomic fields, and analytical theory (Chapters 6-8), the important Class Field Theory (Chapter 9) is expounded, and algebraic function field (Chapter 10) is sketched. This book is based on the study and lectures of the author at several universities.

Alpha Science International Ltd.
www.alphasci.com

ISBN 978-1-78332-208-4

Alpha Science

Algebraic Number Theory

2/e

ZHANG Xianke

Algebraic Number Theory
Second Edition

ZHANG Xianke

常州大学山书馆
藏书章

Higher Education Press

Alpha Science International Ltd.
Oxford, U.K.

Algebraic Number Theory
Second Edition
416 pgs. | 33 figs. | 5 tbls.

Copyright © 2016, Higher Education Press, China

ZHANG Xianke
Tsinghua University
Department of Mathematical Sciences
Beijing 100084
Email: xianke@tsinghua.edu.cn; xzhang@math.tsinghua.edu.cn

ISBN 978-1-78332-208-4

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without prior written permission of the publisher.

此为试读,需要完整PDF请访问: www.ertongbook.com

Algebraic Number Theory

Second Edition

Preface

The purpose of the book is to lead the readers quickly arrive at the area of algebraic number theory; striving to clearly and briefly interpret both the fundamental and deepgoing theory from a relatively modern mathematical angle of view.

The book begins with concise ideal-theory in the first three chapters, which is relatively easy to understand, classical and fundamental, and which draws the outline of the classical algebraic number theory.

Then in Chapters 4–5, valuation-completion theory and local fields are developed, which form the basic language and tool of modern approach.

In Chapters 6–8, the regular materials are treated concisely such as class numbers, units, quadratic and cyclotomic fields, and brief analytical theory.

In Chapter 9, the important class field theory and idele groups are expounded.

Finally, algebraic function fields are briefly sketched in Chapter 10.

This book originally grew out of the lectures given at "The National Summer School of Mathematical Graduates" (Beijing, 1996), and lectures given at Tsinghua University and University of Science and Technology of China to graduates for a long term. This is translated from the second and enriched edition.

Though some impressions of researching and teaching are assimilated into the book, but only a few of the contents are my independent original innovation (e.g., part of statements and proofs of the general valuations), most are compiled and written consulting to literatures (as in the Bibliography), especially [A1], [A-T], [Deur], [Eich], [Goss], [La], [Lo], [Ma], [Ne], [Rosen], [Sa], [Si], [Sticht], [Wash], [We], and [Zar]; I am grateful to the authors.

Here, I want to express my special gratitude to Professors Don B. Zagier and Lawrence C. Washington for their many helps during my studying and researching on number theory, both in the time in University of Maryland, USA and in China. Professor Zagier firstly went to our university giving series of lectures in the spring of 1982, and Professors Washington, K. Rubin, and

Wen-Ching Winnie Li visited us in 1990, both times I wrote poems. The poem in 1982 in English is:

Welcome Prof. Zagier

How gorgeous peach flowers
Blossom at the willow's verdant hair!
Warblers dance swallows sing
To welcome Professor Don Zagier.
So profound and splendid,
Number Theory expounded is without limit;
Ever-lasting and never-ending,
Will Friendship planted grow up just as it.

And the poem in 1990 is :

To Prof. Washington, Rubin, and W. Li

You our best friends landed
near the Forbidden Palace in the May season,
Then lectured with flower petals
raining and dancing in riotous profusion;
Circled around Emperor Lake,
wavering Cyclotomic shadow or reflection,
Zigzagged along the Great Wall,
winding Elliptic curves' spirit and reason.
Thousand arms of Goddess Guanyin,
almighty, which does Number Theory?
Inexorable doom of Stone Stick and Fermat,
coming, who knows Fates Three?
From ancient times, mathematicians
have much more dreams worry,
Ever afterwards, there will add
you in each of my parting reverie !

The poem records a "bet" of Rubin and Washington on the precedence of fall of Fermat's Last Conjecture and the Stone Stick of Chengde, which is famous and like a hug baseball bar standing upside down dangerously on top of a hill at the city Chengde. The poem also records the sightseeing accompanied by number theory lectures and discusses.

Thanks to professors ZENG Kencheng, FENG Keqin, and LU Hongwen for their helps.

I also thank Doctors WANG Kunpeng, LIU Tong, DI Yanming, QIU Derong, MA Lianrong, LI Wei, YANG Dong, TIAN Yichao, LI Yan, ZHAO Jia, ZHAO Yusheng, and HU Su, they very carefully read this book (both the first and second editions) and contributed many significant corrections and suggestions.

Thanks are also given to Mr. ZHAO Tianfu, the editor of the book, who helped to bring about the second edition and this English version completed.

ZHANG Xianke
Tsinghua University

此为试读,需要完整PDF请访问: www.ertongbook.com

Preliminaries
— Groups, Rings, Fields, and Modules

Some simple knowledge of abstract algebra and elementary number theory are needed for reading this book. Here we sketch the most basic part of it, wherewith to assume notations too. Essential preparatory knowledge will be given in the text when needed.

(I) For a **set** A, let $|A|$ or $\# A$ denote its cardinality (the number of its elements). Let $\varnothing$ denote the empty set. For sets A and B, let $A \subset B$ mean A is contained in B but may be equal to B; similarly for $A \supset B$; let $A - B$ or $A \backslash B$ denote the complement of set B in set A, and $A \times B = \{(a, b) | a \in A, b \in B\}$ be the Cartesian product of A and B. For a **map** (or **mapping**, or function) $f: A \to B$, we say $f(a)$ is the image of a, the set

$$\text{Im } f = f(A) = \{f(a) | a \in A\}$$

is the **image** of f, the set $f^{-1}(b) = \{a \in A | f(a) = b\}$ is the **inverse image** of $b \in B$. We say f is **injective** (or an **injection**) if $f(a_1) = f(a_2)$ implies $a_1 = a_2$; f is **surjective** (or a **surjection**) if $\text{Im } f = B$, i.e., for each $b \in B$ there exists $a \in A$ such that $f(a) = b$. If f is both injective and surjective, then we say f is bijective (or a bijection, or a 1:1 correspondence). The composite $g \circ f$ (or product gf) of two maps $f: A \to B$ and $g: B \to C$ is defined by $(g \circ f)(a) = (gf)(a) = g(f(a))$. If S is a subset of A, then a map $f: A \to B$ determines another map $g: S \to B$ by $g(s) = f(s)$; then we say g is a **restriction** of f to S, denoted by $g = f|_S$, and say f is an **extension** of g over A, or g is extended to f.

(II) A **group** is a set having one operation with inverse operation. Strictly speaking, a group $(G, *)$ is a set G together with a binary operation "$*$" on G satisfying the following (4 axioms) for any $a, b, c \in G$:

(g1) (closeness) $a*b \in G$;

(g2) (associative law) $a*(b*c) = (a*b)*c$;

(g3) (existing identity) There exists $e \in G$ such that $e*a = a*e = a$;

(g4) (existing inverses) For each $a \in G$ there exists $a' \in G$ such that $a' * a = a * a' = e$ (We call a' the inverse of a; call e the identity element or unit element).

We often refer to the group $(G, *)$ as group G, refer to the operation "$*$" as a multiplication, denote $a*b$ as $a\cdot b$ or ab. In that case we call $(G, *)$ a multiplicative group, write the identity as 1 (instead of e), write the inverse of a as a^{-1}.

For a group $(G, *)$, if the operation "$*$" further satisfies the commutative law, i.e., $a*b = b*a$ for any $a, b \in G$, then $(G, *)$ is called **abelian group** (or commutative group). For an abelian group $(G, *)$, some times, the operation "$*$" is written as "+" and is called addition, denote $a*b$ as $a+b$. In that case we call $(G, +)$ an **additive group**, write the identity as 0 (instead of e) called zero element, write the inverse of a as $-a$ called minus element. For example, the set μ_m of all mth complex roots of unity is a multiplicative abelian group. The set $\mathbb{Z}$ of integers is an additive (abelian) group. The set $\mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}, \cdots, \overline{m-1}\}$ of congruent classes modulo m is an additive group, where $\overline{a} = a + m\mathbb{Z} = \{a + mk \mid k \in \mathbb{Z}\}$ is a congruent class modulo m, and $\overline{a} + \overline{b} = \overline{a+b}$.

Informally speaking, a multiplicative group is a set within which we can multiply and divide (via $a/b = ab^{-1}$); an additive group is a set within which we can add and subtract (via $a - b = a + (-b)$).

A group G generated by one element is called **cyclic group**.

If H is a subgroup of group $(G, *)$ (i.e., $H \subset G$ and $(H, *)$ is a group), then $(G:H) = |G|/|H|$ is called the index of H in G. For additive groups A, B, their (external) direct sum is $A \oplus B = \{(a, b) \mid a \in a, b \in B\}$ with addition $(a, b) + (a', b') = (a + a', b + b')$. If A, B are subgroups of an additive group G, their sum is $A + B = \{a + b \mid a \in A, b \in B\}$; when $A \cap B = \{0\}$ (or $a + b = a' + b'$ implies $a = a', b = b'$), then $A + B$ is called (internal) direct sum, denoted by $A \oplus B$. For multiplication groups A, B, there is similar definition about direct product.

The cardinality $|G|$ (the number of elements) of G is called the order of G. For a (multiplicative) group and any $g \in G$, the smallest integer $n (\geq 1)$ such that $g^n = 1$ is called the order of g (if n exists), if never $g^n = 1$ then we say g has order ∞. The orders of any subgroup or any element are divisors of $|G|$.

Assume the (multiplicative) group G has a subgroup H. If for any $g \in G$ we have $gH = Hg$ (i.e., $gHg^{-1} = H$, or $ghg^{-1} \in H$ for any $h \in H$), then we say H is a **normal subgroup** of G. In that case we may classify G by H: a, b belong to the same class if and only if $ab^{-1} \in H$, denoted by $a \equiv b \pmod{H}$. Each class is called **residue (or congruent) class** modulo H. The class represented by a (i.e., the class containing a) is just $\overline{a} = aH = \{ah \mid h \in H\}$. Let

$$G/H = \{\overline{e}, \overline{a}, \overline{b}, \cdots\}$$

be the set of all the congruent classes. Then G/H is a group, called the **quotient group**, or **congruent (residue) class group** of G modulo H, by the operation $\overline{a}\ \overline{b} = \overline{ab}$ or $(aH)\ (bH) = (ab)H$. Of course, for an additive group G, each

subgroup is naturally normal, so we always may get quotient group G/H, and the congruent class represented by a is $\overline{a} = a + H$, and $\overline{a} + \overline{b} = \overline{a+b}$. For example, $\mathbb{Z}/7\mathbb{Z} = \{\overline{0}, \overline{1}, ..., \overline{6}\}$ is a quotient group.

Suppose that $\varphi: G \to G'$ is a map from group to group. If φ "preserves" operation, i.e., $\varphi(ab) = \varphi(a)\,\varphi(b)$ for any $a, b \in G$, then φ is called **homomorphism**. And $\ker\varphi = \{a \in G | \varphi(a) = 1\}$ is called the kernel of φ, which is a normal subgroup of G. The inverse image of any $b \in G'$ is $\varphi^{-1}(b) = a_0 \ker\varphi$, where $a_0 \in G$ and $\varphi(a_0) = b$. So a homomorphism φ is an injection (called embedding) if and only if $\ker\varphi = \{1\}$. A bijective homomorphism $\varphi: G \to G'$ is called isomorphism, and then G, G' are said to be isomorphic, denoted by $G \cong G'$. For a homomorphism $\varphi: G \to G'$, here is the fundamental theorem:

$$G/\ker\varphi \cong \mathrm{Im}\,\varphi.$$

Let H, K be subgroups of group G, K is normal in G, then we have naturally the isomorphism

$$(HK)/K \cong H/(K \cap H).$$

where $HK = \{hk | h \in H, k \in K\}$ is a group, $H \cap K$ is a normal subgroup of H. Now assume $H \supset K$ are normal subgroups of G, then there is naturally an isomorphism

$$\frac{G}{H} \cong \frac{G/K}{H/K}.$$

(III) A **ring** is a set within which we can add, subtract, and multiply. Strictly speaking, a ring A is a set, together with two binary operations called addition and multiplication (and denoted by "+" and "•". Often write $a \bullet b$ as ab) respectively; and satisfy conditions:

($r1$) $(A, +)$ is an abelian group (whose identity is 0);

($r2$) $(A, \bullet)$ is a semi-group (i.e., the multiplication satisfies ($g1$) closeness and (g2) associative law);

($r3$) Distributive law are satisfied (i.e., $a(b + c) = ab + ac$, $(b + c)\,a = ba + ca$ for any $a, b, c, \in A$).

If a ring A has an element e such that $ea = ae = a$ for all $a \in A$, then e is called identity (element) of A and is denoted by 1 usually. A ring A is said to be **commutative** if $ab = ba$ for all $a, b \in A$. In this book, **"ring" will mean "commutative ring with identity"** unless otherwise remarking. If $a, b \in A$ are nonzero but $ab = 0$, then a and b are called **zero divisors**. A commutative ring with identity $1 \neq 0$ which contains no zero-divisor is called **domain** (or **integral ring**, or entire ring, or integral domain). Let A be a ring with identity, and $a \in A$, if there is $a' \in A$ such that $aa' = a'a = 1$, then we say a is **invertible** (or a **unit** of A), a' is the **inverse** of a. The set A^* of all units (invertible elements) of A is

a multiplicative group (**unit group**). If $A^* = A - \{0\}$ then A is called **division ring** (with itdentity). A commutative division ring is called **field**.

For ring A, let $A[X]$ denote the set of polynomials (formal) over A with indeterminate X, which is a domain. Similarly, $A[X_1, ..., X_n]$ denotes the domain of all polynomials with n indeterminate. $A[[X]]$ denotes the domain of all formal power series over A. Let $A \subset B$ be rings and $x \in B$, then $A[x]$ denotes the subring of B generated by x over A, i.e., the set of all polynomials of x with coefficients in A. Similarly, $A[x_1, ..., x_n]$ denotes the subring generated by $x_1, ..., x_n \in B$ over A.

We assume our rings are **commutative rings with identity** in the following. An **ideal** I of a ring A is an additive subgroup of A(as an additive group) which satisfies the **absorbing law**: $ax \in I$ for all $x \in I$ and $a \in A$. For exmple A and $\{0\}$ are ideals, called trivial ideals. A field F has only trivial ideals (since for $0 \neq x \in I \subset F$ we have $x^{-1} \in F$, $1 = x^{-1} x \in I$, so $a \cdot 1 \in I$ for all $a \in F$). For any subset $S = \{x_i\}$ of a ring A, the set of all $\sum_i a_i x_i$ (finite sums, $a_i \in A$) is an ideal, we say it is **generated** by $\{x_i\}$, and denoted by AS (or SA, or $(\{x_i\})$. In particular, an ideal generated by one element (say x) is called **principal ideal** (denoted by Ax, xA or (x)). Two elements $x, y \in A$ generate the ideal $(x, y) = Ax + Ay$. And $(1) = A$. For two ideals I, J of ring A, the **sum** $I + J$ is the ideal generated by (elements of) I, J, i.e., $I + J = \{a + b | a \in I, b \in J\}$, which is just the minimal ideal containing I, J. The product IJ is the set of all the finite sums $\sum a_i b_i$ ($a_i \in I$, $b_i \in J$).

A **principal ideal domain (PID)** is a domain in which every ideal is principal. For any $a, b \in A$ (a PID), the ideal $(a, b) = (d)$, where d is the greatest common divisor of a, b. Consequently, there exist $u, v \in A$ such that

$$ua + vb = d \quad \text{(Bezout equality)}.$$

Examples of PID: $\mathbb{Z}$(integers), $F[X]$ (polynomials over field F), and $F[[X]]$ (formal power series domain, whose ideals are (X^n), $n \geq 0$). Note that $(3) \supset (6)$ in $\mathbb{Z}$. So in any ring, we denote ideals $I \supset J$ also by $I|J$, and say I is a factor of J.

An ideal I of ring A is apriori a subgroup of A(as an additive group), so we have the quotient group A/I. Now we can define multiplication in A/I by $\overline{a}\,\overline{b} = \overline{ab}$, thus A/I becomes a ring, called the **quotient ring**, or **congruent (residue) class ring** of A modulo I. The ideals of the quotient ring A/I are just J/I, where J runs over ideals of A containing I. A/I is a field if and only if I is a **maximal ideal** (i.e., A has no ideal J between A and I). A/I is a domain if and only if I is a **prime ideal** (i.e., $xy \in I$ implies $x \in I$ or $y \in I$). For example, $m\mathbb{Z} = \{mk | k \in \mathbb{Z}\}$ is an ideal of $\mathbb{Z}$ for any integer m, and

$$\mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}, \cdots, \overline{m-1}\}$$

is a quotient ring of $\mathbb{Z}$ modulo $m\mathbb{Z}$. When $m = p$ is a prime number, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is a field with p elements.

A map $f:A \to B$ between rings is called **homomorphism** if it "preserves" all operations, i.e., $f(a + b) = f(a) + f(b)$, $f(ab) = f(a)\,f(b)$, $f(1) = 1$ (for any $a, b \in A$). We call a bijective homomorphism $f:A \to B$ an **isomorphism**, and say then A an B are isomorphic, denote by $A \cong B$. For example, if I is an ideal of A, then $f:A \to A/I$, $a \mapsto \bar{a}$, is a (canonical) homomorphism.

Similar to additive groups, we have (1) For a homomorphism $f:A \to B$, the kernel $\ker f = \{a \in A \mid f(a) = 0\}$ is an ideal, and

$$A/\ker f \cong \operatorname{Im} f, \qquad a + \ker f \mapsto f(a).$$

(2) Let $A \supset S$ be rings, I an ideal of A. Then

$$(S + I)/I \cong S/(S \cap I), \qquad s + I \mapsto s + (S \cap I)$$

where $S + I = \{s + x \mid s \in S, x \in I\}$ is a ring containing I as an ideal, $S \cap I$ is an ideal of S.

(3) Assume now $I \supset J$ are ideals of ring A. Then

$$\frac{A}{I} \cong \frac{A/J}{I/J}, \quad a + I \mapsto (a + J) + I/J$$

Let A be a domain. We say $K = \{a/b \mid a, b \in A, b \neq 0\}$ is the **quotient field**, or the **field of fractions** of A. For example, $\mathbb{Q}$ is the field of fractions of $\mathbb{Z}$. And let $F[X]$ be the domain of polynomials of indeterminate X over field F, then the field of fractions of $F[X]$, denoted by $F(X)$, is called **rational function field** (or rational form field) over F. For $x, y \in K$ the field of fractions of A, if there exists $a \in A$ such that $y = ax$, we say x **divides** y, or x is a factor (divisor) of y, and y is a **multiple** of x, denoted by $x \mid y$. The set of multiples of x, denoted by Ax, is a **(fractional) ideal** generated by x. Obviously, $x \mid y$ is equivalent to $y \in Ax$ or $Ay \subset Ax$. If $x \mid y$ and $y \mid x$, then we say y is an **associate** of x, which is equivalent to $Ay = Ax$ or $y = ux$ with u a unit. A proper factor of a means factor of a being not an associate of 1 and a itself. Let $p \in A$ be not zero or a unit, if p has no proper factor, then we call p **irreducible**; which means that if $p = ab$ then a or b is a unit.

If each element (not being zero or a unit) of A could be uniquely (up to units and factor order) written as a finite product of irreducible elements, then A is said to be a **unique factorization domain** (**UFD**). A PID is a UFD.

(IV) A **Field** is a set within which we can add, subtract, multiply and divide. Strictly speaking, a field F is a ring whose non-zero elements form a multiplicative abelian group. For a field, the additive identity is denoted by 0, the multiplicative identity is denoted by 1 (or e some times). And for convenience of writing we assume $2 \cdot e = e + e = 2 \cdot 1 = 1 + 1 = 2 \in F$, etc.

Examples of fields: the rational number field $\mathbb{Q}$, the real number fields $\mathbb{R}$, the complex number field $\mathbb{C}$, and the finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ with p elements. Two fields are isomorphism if they are so as rings.

If k is a subfield of field F(i.e., k is a subset of F and is a field with the addition and multiplication in F), then we say F is an **extension** (field) of k and denoted by F/k. In that case, F is naturally a vector (linear) space over k, the dimension of the space is called the **degree** of the extension F/k, denoted by $[F:k]$; the basis of F as a vector space over k is called its k-**basis**. Extension with finite degree is called **finite extension**.

For a field F, if there exists a positive integer p such that $p \cdot 1 = 1 + 1 + ... + 1 \in F$ is equal to zero, then the least such positive integer p (which is a prime) is called the **characteristic** of F (denoted by $\mathrm{Chara}(F) = p$); otherwise (i.e., $n \cdot 1 = 1 + 1 + ... + 1$ never be zero for any integer $n > 0$) we say F has characteristic 0 (denoted by $\mathrm{chara}(F) = 0$). The map $\sigma: n \mapsto ne$ sends $\mathbb{Z}$ to F, its image $\sigma(\mathbb{Z})$ is isomorphic to $\mathbb{Z}$ or $\mathbb{F}_p$ according to $\mathrm{chara}(F) = 0$ or p respectively. So up to an isomorphism we may say F is an extension of $\mathbb{Q}$ or $\mathbb{F}_p$ in these two cases. In a field F with characteristic p, the most peculiarity is $pa = 0$, and $(a + b)^p = a^p + b^p$ for any $a, b \in F$. For any prime number p and integer $n \geq 1$, there is a unique (up to isomorphism) field with $q = p^n$ elements, which is the extension of degree n over $\mathbb{F}_p$, denoted by $\mathbb{F}_q$. The set $\mathbb{F}_q^*$ (non-zero elements of $\mathbb{F}_q$) is a cyclic group of order $q - 1$. So $\mathbb{F}_p$ consists of the q roots of $XP - X$.

(V) **Modules** are natural generalizations of additive groups and vector (linear) spaces. The definition for a vector space over a field F where "field F" is replace by "ring A" becomes a definition for a module over ring A. Strictly speaking, a module M over a ring A is an additive (abelian) group, together with a **scalar multiplication**, i.e., a map $A \times M \to M$, $(a, x) \mapsto ax$, satisfying

$$a(x + y) = ax + ay, \qquad (a + b)x = ax + bx,$$
$$(ab)x = a(bx), \qquad 1x = x$$

(for $a, b \in A$, $x, y \in M$). We also say M is an A-module.

For example, an additive abelian group is a $\mathbb{Z}$-module. A vector space over a field F is an F-module. Vector space V over F with a transformation σ is an $F[X]$-module by the "scalar multiplication" $g(X)\alpha = g(\sigma)\alpha$ for $g(X) \in F[X]$ and $\alpha \in V$.

Many terms for vector spaces are similarly used also to modules, e.g., submodules, linear generate, annihilator, sum, direct sum. For any subset $S = \{x_i\} \subset M$, all the finite sums $\sum a_i x_i$ $(a_i \in A)$ (A-**linear combinations**) make an A-module, called submodule[i] generated by S, denoted by $N = AS$, which is the smallest A-module containing $\{x_i\}$; and $\{x_i\}$ is a generator system of it.

此为试读,需要完整PDF请访问: www.ertongbook.com