Modern Algebra Lecture Notes: Rings and Fields
Summary of Definitions and Theorems: Sets 1-9
Proofs which may be asked in the test or exam are marked ♣

Kevin Broughan

University of Waikato, Hamilton, New Zealand

June 1, 2010

Definition of a ring

A ring is a non-empty subset R with two binary operations, written $a.b$ or ab and $a + b$, such that for all $a, b, c \in R$ we have

- $a + b = b + a$,
- $(a + b) + c = a + (b + c)$,
- $\exists 0 \in R$ so $a + 0 = a$,
- $\exists -a \in R$ so $a + (-a) = 0$,
- $(ab)c = a(bc)$,
- $a(b + c) = ab + ac$,
- $(b + c)a = ba + ca$.

Extra defininitions

We say a ring R has an identity or unity if $\exists 1 \in R$ so $1a = a1 = a$.

If for all $a, b \in R$, $ab = ba$ we say R is commutative.

If $u \in R$ satisfies $uw = wu = 1$ for some $w \in R$ we say u is a unit of R.

If $a, b \in R$ and for some element $c \in R$, $ac = b$ we say a divides b and write $a \mid b$.

Consequences:

$(R, +, 0)$ is an abelian group.

$U = \{u \in R : u \text{ is a unit}\}$ is a multiplicative group $(U, ., 1)$, the group of units of R.

Theorem 1 ♣

(1) $a0 = 0a = 0$,

(2) $a(-b) = (-a)b = -(ab)$,

(3) $(-a)(-b) = ab$,

(4) $a(b - c) = ab - ac$,

(5) $(-1)a = -a$,

(6) $(-1)(-1) = 1$.

Definition of a Subring

If R is a ring and $S \subset R$ a subset which is a ring using the operations of R we say S is a subring of R.

Integral Domains

Definition

A zero-divisor a of a ring R is such that there is a nonzero element b in R with $ab = 0$. An integral domain is a commutative ring with a unity and with no zero-divisors.

Cancellation property

If R is an integral domain then if $a \neq 0$ and $ab = ac$ we have $b = c$.

Definition of a field

A field is a commutative ring with a unity in which every non-zero element has a multiplicative inverse, i.e. is a unit.

Theorem 2 ♣ Every finite integral domain is a field.

Ring characteristic

Let R be a ring with a unity 1. If for all $n \in \mathbb{N}$, $n.1 = 1 + \cdots + 1 \neq 0$ we say the characteristic of R, denoted $\mathrm{char}\ R$, is 0. Otherwise $\mathrm{char}\ R$ is the minimum value of n such that $n.1 = 0$.

Characteristic of an integral domain ♣

Theorem 3: If R is an integral domain then $\mathrm{char}\ R = 0$ or is a rational prime.

Definition of an ideal

Let $I \subset R$ be a subring. We say I is an ideal if for all $x \in R$ and $a \in I$, $x.a$ and $a.x$ are in I.

Factor Rings

Definition: we say the subset $[r] := r + A := \{r + a : a \in A\}$ is the coset with representative r with respect to the subring A in the ring R.

For a fixed subring A, the set of cosets forms an additive group with operation

$$(r + A) + (s + A) := (r + s) + A.$$

Factor Ring Theorem 4

The set of cosets forms a ring with operation $(x + A)(y + A) := xy + A$ if and only if A is an ideal. If so we call the ring R/A or R modulo A.

Maximal Ideals

Definition

An ideal $M \subset R$, where R is commutative, is called maximal if $M \neq \{0\}$, $M \neq R$ (so we say M is proper), and if B is any ideal with $M \subset B \subset R$ then $B = M$ or $B = R$.

Maximal Ideal Factor Theorem ♣

Theorem 5: If $A \subset R$ is an ideal in a commutative ring with unity, then A is maximal if and only if R/A is a field.

Definition of a prime ideal

An ideal $P \subset R$, where R is commutative, is called prime if P is proper and $ab \in P$ implies $a \in P$ or $b \in P$ or both.

Prime Ideal Factor Theorem ♣

Theorem 6: If $A \subset R$ is an ideal in a commutative ring with unity, then A is prime if and only if R/A is an integral domain.

Ring homomorphism

Let R and S be rings, not necessarily distinct. A ring homomorphism is a function $f : R \to S$ such that for all $a, b \in R$ we have

$$f(a+b) = f(a) + f(b), \quad f(ab) = f(a)f(b),$$

where the operations on the left are those of R and on the right those of S.

Ring isomorphism

If a ring homomorphism is both one-to-one (injective) and onto (surjective) then we say the function is a ring isomorphism and that R and S are isomorphic rings.

Definition of the kernel

Let $f : R \to S$ be a homomorphism of rings. Define

$$\text{Ker } f = \{x \in R : f(x) = 0\}.$$

Theorem 7 ♣

The kernel K of f is an **ideal** of R. Conversely if I is an ideal in R the natural map $f : R \to R/I$ is a **homomorphism** with kernel I

Isomorphism Theorem for rings

Theorem 8 ♣

Let $f : R \to S$ be any ring homomorphism. Then $f(R) \subset S$ is a subring. Let K be the kernel of f. Then the mapping

$$g : R/K \to f(R)$$

defined by $x + K \to f(x)$ is a ring isomorphism.

Theorem 9 ♣

Let R be a ring with identity 1. Then the function $f : \mathbb{Z} \to R$ defined by $n \to n.1$ (1 or -1 added to itself n times, or if $n = 0$, just the 0 of the ring) is a ring homomorphism.

Theorem 10 ♣

Let R be a ring with identity 1 and characteristic $n > 0$. Then R contains a subring isomorphic to $\mathbb{Z}/nZ$. If R has characteristic 0 it contains a subring isomorphic to $\mathbb{Z}$.

Theorem 11 ♣

Any field contains a copy of one of $\mathbb{Z}/p\mathbb{Z}$ (p a prime) or $\mathbb{Q}$.

Theorem 12

Let R be an integral domain, commutative with 1. then R is isomorphic to a subring of a field F, namely the so called field of quotients of R.

Definition

Let R be a commutative ring and x a "symbol" or "indeterminate". The by $R[x]$ we mean the set of formal sums

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x^1 + a_0$$

where the $a_i \in R$. We abbreviate these expressions by $f(x), g(x) etc$ and call them polynomials in x with coefficients in R.

Operations in the ring $R[x]$

$$\begin{aligned} f(x) &:= a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x^1 + a_0, \\ g(x) &:= b_n x^n + b_{n-1} x^{n-1} + \cdots + b_1 x^1 + b_0, \\ f(x) + g(x) &:= \sum_{j=0}^{n} (a_j + b_j) x^j, \\ f(x).g(x) &:= \sum_{j=0}^{n} c_j x^j \text{ where } c_j = \sum_{i=0}^{j} a_i b_{j-i}. \end{aligned}$$

$R[x]$ is a commutative ring

Definitions

The terms a_n are called coefficients and the coefficient which is non-zero with the highest value of n is called the leading coefficient, with the value of n being the degree of the polynomial. The zero polynomial has, by decree, no degree, and a constant non-zero polynomial degree 0. If the leading coefficient is 1, the polynomial is called monic.

Theorem 13: If R is an integral domain so is $R[x]$ ♣

Corollary ♣

$\deg f(x).g(x) = m + n = \deg f(x) + \deg g(x)$.

Theorem 14 The division identity

If $F[x]$ is the ring of polynomials with coefficients in a field F and $f(x),\ g(x) \in F[x]$ with $g(x) \neq 0$ then there are unique polynomials $q(x),\ r(x)$ in $F[x]$ with

$$f(x) = q(x).g(x) + r(x),\ r(x) = 0 \text{ or } \deg r(x) < \deg g(x).$$

Definition of factor

If $f(x) = g(x).h(x)$ in $R[x]$ we say $g(x)$ is a factor of $f(x)$ in $R[x]$.

Theorem 15 ♣

Let F be a field, $a \in F$ an element and $f(x) \in F[x]$ a polynomial. Then $f(x) = (x - a)q(x) + f(a)$, i.e. $f(a)$ is the remainder when we divide $f(x)$ by $x - a$. If $f(a) = 0$ then $(x - a)$ is a factor of $f(x)$.

Theorem 16: A poly over a field of degree n has at most n zeros in the field

Definition of a principal ideal domain

A principal ideal domain or PID, is an integral domain R where every ideal has the form $\langle a \rangle$ for some $a \in R$.

Theorem 17: $F[x]$ is a principal ideal domain ♣

Let $A \subset F[x]$ be an ideal. If $A = \{0\}$ we have $A = \langle 0 \rangle$.

Factoring polynomials

Definitions

If F is a field we say a polynomial $f(x) \in F[x]$ is irreducible over F if it cannot be expressed as the product of two polynomials over F with strictly lower degrees than that of $f(x)$.

If R is an integral domain we say a polynomial $f(x) \in R[x]$ is irreducible over R if whenever we write $f(x) = g(x).h(x)$ we must have either $g(x)$ or $h(x)$ a unit in $R[x]$.

Degree 1

If a non-zero polynomial over a field has degree 0 it is irreducible. For degree 1, $f(x) = ax + b$, then $f(-b/a) = 0$ and $f(x)$ is irreducible.

Degree 2 or 3

If $f(x) \in F[x]$ has a zero or root, $f(a) = 0$ then $f(x)$ is reducible since $f(x) = (x - a)g(x)$. If $f(x)$ has degree 2 or 3 then it is reducible if and only if it has a factor of degree 1 if and only if it has a zero/root.

Definition

Let $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$. The content of $f(x)$, denoted $c(f(x))$, is the gcd of the coefficients, i.e. $\gcd(a_0, \ldots, a_n)$. If $c(f(x)) = 1$ we say $f(x)$ is primitive.

Gauss' Lemma ♣

Let $f(x),\ g(x) \in \mathbb{Z}[x]$ be primitive. Then $f(x).g(x)$ is also primitive, i.e. the product of two primitive polynomials is primitive.

Reduction Modulo p

A useful operation on polynomials with integer coefficients is reduction modulo p where p is a fixed prime. This is a homomorphism of polynomial rings:

$$f(x) \in \mathbb{Z}[x] \to \theta(f(x)) \in \mathbb{Z}_p[x] : \quad a_n x^n + \cdots a_0 \to [a_n]x^n + \cdots + [a_0].$$

Theorem 18: ♣

If $f(x) \in \mathbb{Z}[x]$ and $f(x) = g(x).h(x)$ factors in $\mathbb{Q}(x)$ then $f(x) = g_1(x).h_1(x)$ in $\mathbb{Z}[x]$ and the degrees of $\deg g_1(x) = \deg g(x),\ \deg h_1(x) = \deg h(x)$.

Theorem 19: the Mod p irreducibility test ♣

Let p be a prime and $f(x) \in \mathbb{Z}[x]$ is such that $\theta_p(f(x))$ has the same degree and is irreducible in $\mathbb{Z}_p[x]$. Then $f(x)$ is irreducible over $\mathbb{Z}$.

Theorem 20: Eisenstein's irreducibility test

Let $f(x) = a_0 + a_1x + \cdots + a_nx^n$ have positive degree and suppose some prime $p \mid a_0, p \mid a_1, \ldots, p \mid a_{n-1}$ but $p \nmid a_n$ and $p^2 \nmid a_0$. Then $f(x)$ is irreducible over $\mathbb{Z}$.

Theorem 21: $f(x)$ irreducible implies $F[x]/\langle f(x)\rangle$ is a field ♣

Theorem 22: irreducible polynomials over a field are like prime numbers ♣

Let F be a field and let $f(x)$ in $F[x]$ be irreducible. Then if $f(x) \mid g(x).h(x)$ in $F[x]$ we must have $f(x) \mid g(x)$ or $f(x) \mid h(x)$.

Theorem 23: Unique factorization holds in $\mathbb{Z}[x]$

If $f(x) \in \mathbb{Z}[x]$ has positive degree then it can be factored, up to order, uniquely into the product of an integer and a set of polynomials of positive degree, irreducible over $\mathbb{Z}$.

Definitions

(1) An integral domain R is a commutative ring with a unity 1.
(2) Elements $a,\ b \in R$ are called associates if there is a unit $u \in R$ such that $a = ub$.
(3) An element $a \neq 0 \in R$ is called irreducible in R if whenever $a = bc$ in R, b or c is a unit.
(4) An element $a \neq 0 \in R$ is called a prime of R if whenever $a \mid bc$ in R, $a \mid b$ or $a \mid c$.
(5) If $m \in \mathbb{Z} \setminus \{0, 1\}$ is squarefree and $R = \mathbb{Z}[\sqrt{m}]$ then define the norm of an element $x = a + \sqrt{m}b$ by $N(x) = a^2 - mb^2$.

Theorem 24 ♣

(1) $N(x) = 0 \iff x = 0$,
(2) $N(xy) = N(x)N(y)$,
(3) x is a unit if and only if $N(x) = \pm 1$,
(4) If $N(x)$ is prime in $\mathbb{Z}$ then x is irreducible in $\mathbb{Z}[\sqrt{m}]$.

Primes vs irreducibles

Theorem 25 ♣

Let R be an integral domain. Then every prime p in R is irreducible.

Theorem 26: In a PID every irreducible is necessarily a prime

Definition

A unique factorization domain is an integral domain R in which every element which is not a unit can be written down as a product of irreducible elements of R, these factors being unique up to multiplication by associates and reordering.

Lemma ♣

In a PID R any increasing chain of distinct ideals $A_1 \subset A_2 \subset \cdots$ is necessarily finite in length.

Theorem 27: Each PID is a unique factorization domain ♣

Definition

An integral domain R is called Euclidean if there is a function $d : R \to \mathbb{Z}_{\geq 0}$ such that
(1) for all $a,\ b \neq 0 \in R$, $d(a) \leq d(ab)$, and
(2) if $a,\ b \neq 0 \in R$ there exist $q,\ r \in R$ such that $a = bq + r$ with $r = 0$ or $d(r) < d(b)$.

Examples of Euclidean rings with their mappings d:

(1) In $\mathbb{Z}$, $d(x) := |x|$.

(2) In $F[x]$, $d(f(x)) := \deg f(x)$.

(3) In $\mathbb{Z}[i]$, $d(a + ib) = a^2 + b^2 = N(a + ib)$.

Theorem 28: Statement

If R is a Euclidean domain then R is a principal ideal domain.

Units in $R[x]$ ♣

Let R be an integral domain. Units in $R[x]$ are constant polynomials with values which are units in R.

Representatives

Hence, if the degree of $f(x)$ is $n \geq 1$, elements of the quotient field look like $[r(x)]$ where $r(x) = a_0 + \cdots + a_{n-1}x^{n-1}$ where the a_i can be chosen arbitrarily from F giving in each case a unique element. That's what $F[x]/\langle f(x)\rangle$ looks like, namely $[r(x)]$'s. Later we will see a nice vector space description.

Addition

To add classes we, as usual add representatives:
$[r_1(x)] + [r_2(x)] = [r_1(x) + r_2(x)]$ and the sum on the right is just the polynomial with the coefficients of $r_1(x)$, $r_2(x)$ added in F.

Multiplication

To multiply classes we multiply the representatives and then take the remainder after division by $f(x)$: $[r_1(x)][r_2(x)] = [r_1(x).r_2(x)] = [r_1(x).r_2(x) \bmod f(x)]$.

Inverse

To get the inverse of a non-zero class represented by $r(x)$ we use the extended Euclidean algorithm in $F[x]$ to find polynomials $h(x),\ k(x)$ such that $h(x).r(x) + k(x).f(x) = \gcd(r(x), f(x)) = 1$, and then $[h(x)][r(x)] + 0 = [1]$ so $[h(x) \bmod f(x)]$ is the inverse for $[r(x)]$.

Definition

A vector space V over a field $\mathbb{K}$ has a binary operation "+" giving it an Abelian group structure, and a binary operation "." from $\mathbb{K} \times V \to V$, called scalar multiplication, which satisfies, for all $\alpha,\ \beta \in \mathbb{K}$ and $x, y \in V$:

$$\alpha.(x+y) = \alpha.x + \alpha.y,\ (\alpha+\beta).x = \alpha.x + \beta.x,\ \alpha.(\beta.x) = (\alpha\beta).x,\ 1.x = x.$$

Definitions

A set of vectors $\{x_1, \ldots, x_m\}$ in V is called linearly independent if whenever $\sum_{1 \le i \le m} \alpha_i.x_i = 0$ we must have $\alpha_i = 0,\ 1 \le i \le m$. These vectors are then all non-zero and distinct. No x_i can be expressed as a linear combination of the other x_j's.

A set of vectors $\{x_1, \ldots, x_m\}$ in V is said to span V if every element $v \in V$ can be expressed as a sum $v = \sum_{1 \le i \le m} \alpha_i.x_i$.

A set of vectors $\{x_1, \ldots, x_m\}$ in V is said to be a basis for V if it is both linearly independent and spans V.

A vector subspace of V is a subset W closed under the operations of V, i.e. if $x, y \in W \implies x + y \in W$ and $\alpha.x \in W$ for all $\alpha \in \mathbb{K}$.

If a vector space has a finite basis, its size is denoted by $[V : \mathbb{K}]$ or $\dim_{\mathbb{K}} V$ and called the dimension of the vector space.

Basis existence theorem

Every vector space has a basis. This is a deep fact and requires the logical axiom of choice or something equivalent like Zorn's lemma. It is only needed for infinite dimensional spaces.

Given a finite set of non-zero vectors $X = \{x_1, \ldots, x_m\}$ in V, the set of all linear combinations $\sum_{1 \leq i \leq m} \alpha_i . x_i$ forms a subspace W of V, and the set of vectors spans W.

We can replace X by a linearly independent set of vectors

Statement: Dimension Theorem 29 ♣

Let V over $\mathbb{K}$ have a basis of size $n \in \mathbb{N}$. Then every other basis has this same size, so $n = [V : \mathbb{K}]$.

Definitions

A field E is called an extension field of a field F if $F \subset E$ and F is a subfield of E.
If $F \subset E$ and E is an extension field of F and a polynomial $f(x) \in F[x]$ factors completely into linear factors in E (we say then that $f(x)$ **splits** in E), but does not split in any proper subfield of E, we say E is a splitting field for $f(x)$ over F.

Statement: Kronecker's Theorem 30 ♣

Let $f(x) \in F[x]$ be of $\deg f(x) > 0$. Then there is an extension E of F in which $f(x)$ has a root.

Definition

Let E be an extension of F and let $0 \neq a \in E$ be an element. We define $F(a)$ to be the smallest subfield of E containing a. Note that it must also contain $2a, 3a, -a, 1/a, a^2, g(a)/h(a), \ldots$ where $g(x), h(x) \in F[x]$ and $h(a) \neq 0$ in E.

Extended definitions

If $a, b, a_i \in E$, and extension of F, We can define $F(a, b)$ by $(F(a))(b)$ and inductively $F(a_1, \ldots, a_n) = (F(a_1, \ldots, a_{n-1}))(a_n)$, or simply as the smallest subfield of E containing all of the a, b, a_i.

Statement: Splitting fields exist: Theorem 31

Let $f(x) \in F[x]$ be of $\deg f(x) > 0$. Then there is an extension E of F which is a splitting field for $f(x)$. All splitting fields are isomorphic, so this field is essentially unique. The proof is omitted.

Fundamental Theorem of Algebra

The $\star$ Fundamental Theorem of Algebra $\star$, proved in Complex Calculus, shows that every polynomial with complex coefficients has a full set of roots in $\mathbb{C}$. Thus if $F = \mathbb{Q}$, there is at least one field extension of $\mathbb{Q}$ in which $f(x)$ splits completely. Later we will have an algebraic proof, which relies on the existence of a splitting field for each polynomial over a given field.

Dangerous curve!

Splitting fields can be of large dimension. There are examples of irreducible polynomials $f(x) \in \mathbb{Q}[x]$ with degree n and splitting fields of maximum dimension $n!$.

Differential algebra: derivative of a polynomial

Definition

Let $f(x) \in F[x]$ be a polynomial $f(x) = a_0 + \cdots a_n x^n$. Then if $n = 0$ set $f'(x) = 0$. Otherwise define

$$f'(x) := a_1 + 2a_2 x + 3a_3 x^2 \cdots + n a_n x^{n-1},$$

and call $f'(x)$ the derivative of $f(x)$. We sometimes write $(f(x))'$ for $f'(x)$.

Theorem 32: Properties of the derivative ♣

Let $f(x), g(x) \in F[x]$ and $a \in F$. Then
(1) $(f(x) + g(x))' = f'(x) + g'(x)$,
(2) $(af(x))' = af'(x)$,
(3) $(f(x).g(x))' = f(x).g'(x) + f'(x).g(x)$.

Multiple zero criterion

Theorem 33 ♣

The polynomial $f(x) \in F[x]$ has a multiple zero in some extension of F if and only if $f(x)$ and $f'(x))$ have a non-trivial common divisor of positive degree in $F[x]$, so the GCD $(f(x), f'(x))$ is non-trivial in $F[x]$

Theorem 34: Irreducibles have only simple zeros in characteristic zero ♣

Let $f(x) \in F[x]$ be irreducible, where F has characteristic zero. Then in any extension field, $f(x)$ has no multiple zeros.

Statement: Theorem 35 $F(a) \approx F[x]/\langle f(x) \rangle$ ♣

Let $f(x) \in F[x]$ be irreducible and $f(a) = 0$ in E. Then

(1) The field $F(a)$ is isomorphic to the field $F[x]/\langle f(x) \rangle$.

(2) If $\deg f(x) = n$ then $F(a)$ is a vector space over F with basis $\{1, a, a^2, \ldots, a^{n-1}\}$.

(3) If $a' \in E'$ is another zero of $f(x)$ then $F(a) \approx F(a')$.

Algebraic number

Let E be a field extension of F and let $a \in E$. We say a is algebraic over F if a is a root of some polynomial $f(x) \in F[x]$.

Minimum polynomial

If $a \in E$ is algebraic over F then the monic polynomial $f(x) \in F[x]$ of minimum degree having a as a root is called the minimum polynomial of a over F.

Transcendental number

We say a is transcendental over F if a is **not** the root of any polynomial in $F[x]$.

Definition

We say E is an algebraic extension of F if every element $a \in E$ is algebraic over F. If an extension is not algebraic it is called a transcendental extension.
An extension of the form $F(a)$ is called a simple extension of F.

Theorem 36: Description of simple algebraic extensions

If $a \in E$ is algebraic over F then $F(a) \approx F[x]/\langle f(x) \rangle$ where $f(x)$ is the unique minimum polynomial of a over F which is necessarily irreducible over F.

Definition

We have seen that E can be regarded as a vector space with scalars in F. We say the extension is finite if the dimension $[E : F] = n$ is finite.

Theorem 37: If $[E : F] = n < \infty$ then E is an algebraic extension of F ♣

Theorem 38: The set of algebraic numbers is a field ♣

Let F be a field and E a field extension of F. Let $A \subset E$ be the set of elements of E which are algebraic over F. Then A is a field.

Dimension Theorem 39 ♣

Let $F \subset E \subset K$ be field extensions with $[E : F] = m < \infty$, $[K : E] = n < \infty$. Then $[K : F] < \infty$ also and $[K : F] = [K : E][E : F] = mn$.

Statement

Let F have characteristic zero and let $a, b \in E$ be algebraic over F. Then there is an element $c \in E$ such that $F(a, b) = F(c)$. Consequently any finite algebraic extension is simple.