School of Mathematical Sciences
PURE MTH 3007
Groups and Rings III, Semester 1, 2009

Week 9 Summary

8. Rings

8.1. Definitions.

Definition 8.1. A *ring* is a set R with two binary operations $+, \cdot$ such that

(i) $(R,+)$ is an abelian group
(ii) $a(bc) = (ab)c$ for all $a,b,c \in R$ *(Associative law for multiplication)*
(iii) $a(b+c) = ab + ac$ and $(a+b)c = ac + bc$ for all $a,b,c \in R$ *(Distributive laws)*.

Notes:
(1) As usual, we often omit $\cdot$ and write ab instead of $a \cdot b$.
(2) $(R,\cdot)$ is not necessarily a group – why?
(3) The additive identity of $(R,+)$ is denoted 0. Thus $a + 0 = 0 + a = a$ for all $a \in R$.
(4) The additive inverse of $(R,+)$ is denoted $-a$. Thus $a + (-a) = (-a) + a = 0$ for all $a \in R$.
(5) R is called *a commutative ring* if $ab = ba$ for all $a,b \in R$.
(6) R is called *a ring with identity* if there is an element $1 \neq 0$ in R such that $1.a = a.1 = a$ for all $a \in R$.

8.2. Examples of rings.

(1) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are rings (commutative rings with identity).
(2) For any integer $n \geq 1$, $\mathbb{Z}_n$ is a ring under addition and multiplication $\pmod n$.
(3) For any integer $n \geq 1$, if R is a ring, then the set of $n \times n$ matrices $M_n(R)$ is a ring under the usual operations.
(4) The *Gaussian integers* $\mathbb{Z}[i] = \{a + bi \mid a,b \in \mathbb{Z}\}$.
(5) The set $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a,b \in \mathbb{Q}\}$.
(6) The ring of real quaternions

$$\mathbb{R}(\mathbb{H}) = \{a + bi + cj + dk \mid a,b,c,d \in \mathbb{R}, i^2 = j^2 = k^2 = -1, ij = k, jk = i, ki = j\}.$$

The definitions and examples above were given in the Friday lecture of Week 8.

Week 8 — Lecture 18 — Tuesday 12th May .

8.3. Properties of rings.

(1) $0.a = a.0 = 0$ for all $a \in R$.
(2) $a(-b) = (-a)b = -ab$ for all $a,b \in R$.
(3) $(-a)(-b) = ab$ for all $a,b \in R$.

8.4. Homomorphisms.

Definition 8.2. Let R and R' be rings. A function $\phi : R \to R'$ is a *ring homomorphism* if

(i) $\phi(a+b) = \phi(a) + \phi(b)$
(ii) $\phi(ab) = \phi(a)\phi(b)$

for all $a,b \in R$.

The homomorphism ϕ is called an *isomorphism* if it is $1-1$ and onto.

The *kernel* of ϕ is $ker\,\phi = \{a \in R \mid \phi(a) = 0\}$.

Note: The homomorphism ϕ is $1-1$ if and only if $\ker \phi = \{0\}$.

8.5. Subrings.

Definition 8.3. A *subring* S of a ring R is a subset of R that is itself a ring.

Thus S is a subring of R if $(S,+) < (R,+)$ and if S is closed under multiplication.

In particular, if $\phi : R \to R'$ is a ring homomorphism then $\phi(R)$ and $\ker \phi$ are subrings of R' and R respectively.

Week 8 — Lecture 19 — Wednesday 13th May.

---

9. Integral Domains and Fields

9.1. Definitions.

Definition 9.1. Let R be a ring with identity 1. A *unit* of R is an element u that has a multiplicative inverse u^{-1}. So, $uu^{-1} = u^{-1}u = 1$.

If every non-zero element of R is a unit then R is called a *field* when R is commutative, or a *skewfield* or *division ring* when R is not commutative.

Thus when R is a field, $(R,+)$ and $(R \setminus \{0\}, \cdot)$ are both abelian groups.

Definition 9.2. Let R be a ring. A non-zero element $a \in R$ is a called a *zero-divisor* if there exists a non-zero $b \in R$ such that $ab = 0$ or $ba = 0$.

The ring $\mathbb{Z}_n$ ($n > 1$) has no zero-divisors if and only if n is prime.

Definition 9.3. An *integral domain* is a commutative ring with identity which has no zero-divisors.

Examples:
1. $\mathbb{Z}$ is an integral domain.
2. If p is prime, $\mathbb{Z}_p$ is an integral domain.
3. If n is composite, Z_n is not an integral domain.
4. Every field is an integral domain.

Theorem 9.4. *Every finite integral domain is a field.*

Corollary 9.5. *If p is a prime, then $\mathbb{Z}_p$ is a field.*

9.2. The field of quotients of an integral domain.

Let D be an integral domain. Then we can construct a field F containing D as follows:

Let
$$S = \{(a,b) \in D \times D \mid b \neq 0\}.$$

Define an equivalence relation on S by
$$(a,b) \sim (c,d) \text{ if } ad = bc.$$
Let F be the set of equivalence classes under this relation:
$$F = \{[(a,b)] \mid a,b \in D, b \neq 0\}.$$

Define operations of addition and multiplication on F by
$$[(a,b)] + [(c,d)] = [(ad+bc, bd)]$$

and

$$[(a,b)] \cdot [(c,d)] = [(ac,bd)].$$

Then F is a field under these operations and F contains an integral domain

$$\overline{D} = \{[(a,1)] \mid a \in D\}$$

which is isomorphic to D. We usually say that $D \subset F$.

The field F is called the *field of quotients* of D. This field is the smallest field containing D, and is unique up to isomorphism.

Week 8 — Lecture 20 — Friday 15th May.

---

10. Polynomials

10.1. **Basic operations.** Let R be a ring. We denote by $R[x]$ the set of all *polynomials* in x with coefficients in R. Here x is an 'indeterminate', not a variable or element of R.

Thus

$$R[x] = \left\{ \sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + a_2 x^2 + \ldots \;\middle|\; a_i \in R, \text{ only a finite number of } a_i \text{ non-zero} \right\}.$$

The *degree* of the polynomial $f(x)$ is the largest i such that $a_i \neq 0$. It is conventional to say that the zero polynomial 0 has degree $-\infty$.

10.1.1. *Addition and multiplication of polynomials.* If

$$\begin{aligned} f(x) &= a_0 + a_1 x + a_2 x^2 + \ldots \\ g(x) &= b_0 + b_1 x + b_2 x^2 + \ldots \end{aligned}$$

then

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \ldots$$

and

$$f(x)g(x) = d_0 + d_1 x + d_2 x^2 + \ldots$$

where $d_i = \sum_{j=0}^{i} a_j b_{i-j}$. Note that with these definitions,

$$\deg f(x)g(x) \leq \deg f(x) + \deg g(x)$$

and

$$\deg(f(x) + g(x)) \leq \max\{\deg f(x), \deg g(x)\}.$$

Under these operations, $R[x]$ is a ring.

If R is commutative, so is $R[x]$. If R has an identity 1, so has $R[x]$.

More generally, we can define the polynomial ring $R[x_1, x_2, \ldots, x_n]$ in n indeterminates $x_1, x_2, \ldots, x_n$ by

$$R[x_1, x_2, \ldots, x_n] = (R[x_1, x_2, \ldots, x_{n-1}])[x_n].$$

10.2. **Polynomials over an integral domain and field.** If D is an integral domain, so is $D[x]$ and hence so is $D[x_1, x_2, \ldots, x_n]$. In this case

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

If F is a field, then $F[x]$ is an integral domain but *not* a field.

10.2.1. *The division algorithm.*

Lemma 10.1 (Division algorithm for $\mathbb{Z}$)**.** *Let m and n be integers with $m \neq 0$. Then there are unique integers q and r such that*

$$n = qm + r$$

and $0 \leq r < m$.

Lemma 10.2 (Division algorithm for $F[x]$)**.** *Let F be a field and $f(x), g(x)$ be polynomials in $F[x]$ with $g(x) \neq 0$. Then there are unique polynomials $q(x)$ and $r(x)$ in $F[x]$ such that*

$$f(x) = g(x)q(x) + r(x)$$

and $\deg r(x) < \deg g(x)$.

Note that $g(x) \mid f(x)$ if and only if $r(x) = 0$.