Garrett

Chapter 9

Rings and Fields

Definition: A ring R is a set with two operations, $+$ and $\cdot$, and with a special element 0 (additive identity) with the following properties:

- the addition is associative - $a+(b+c)=(a+b)+c$ $\forall a,b,c \in R$
- the addition is commutative - $a+b=b+a$ $\forall a,b \in R$
- $\forall a \in R$ $\exists$ an additive inverse, $-a$, w/ $a+(-a)=0$
- Zero has the property that $0+a=a+0=a$, $\forall a \in R$
- the multiplication is associative - $(ab)c=a(bc)$ $\forall a,b,c \in R$
- the multiplication and addition have left and right distributive properties: $a(b+c)=ab+ac$ and $(b+c)a=ba+ca$ $\forall a,b,c \in R$

Often, a particular ring has some additional features/properties

- If there is an element 1 with the property $1 \cdot a = a \cdot 1$ $\forall a \in R$, then 1 is the multiplicative identity or unit in the ring.
- If $ab=ba$ for all $a,b \in R$, then the ring is a commutative ring, however not always true.
  eg. Matrix Multiplication
- If there exists $a^{-1} \in R$ such that $a \cdot a^{-1} = 1$ and $a^{-1} \cdot a = 1$, a^{-1} is a multiplicative inverse for a.
  if $a \in R$ has a mult. inverse, then a is called a unit in R.
  - the collection of all units in a ring R is denoted $R^\times$, called the group of units in R

* - A commutative ring in which every nonzero element is a unit is a Field

* - A not necessarily commutative ring in which every nonzero element is a unit is called a division ring

- In a ring R an element r such that $r \cdot s = 0$ or $s \cdot r = 0$ for some nonzero $s \in R$ is called a zero divisor. A comm. ring w/o nonzero zero-divisors is an integral domain
- A commutative ring R has the cancellation property if for any $r \neq 0 \in R$, if $rx = ry$ for $x, y \in R$, then $x = y$

Proof (of uniqueness of additive identity): If there is an element $z \in R$ and $r \in R$ s.t $r + z = r$, add $-r$ to both sides of the equation

$$(r+z) - r = r - r = 0$$

by definition of additive inverse. Using commutativity and associativity of addition, the left hand side of this is

$$(r+z) - r = (z+r) - r = z + (r-r) = z + 0 = z$$

also using the property of 0, i.e. $z = 0$, proving the uniqueness □

Proof (of uniqueness of additive inverse): Fix $r \in R$. If there is $r' \in R$ so that $r + r' = 0$, then add $-r$ to both sides,

$$(r + r') - r = -r + 0$$

Using comm. & assoc. of addition,

$$(r + r') - r = (r' + r) - r = r' + (r - r) = r' + 0 = r'$$

since the right hand side is $0 + (-r) = -r$, we have

$$r' = -r$$

□

Proof (of uniqueness of multiplicative identity)

Suppose that either u is a left identity or u is a right identity.

Suppose u is a left identity, in particular

$u \cdot 1 = 1$ then since $u \cdot 1 = u$ by the property of multiplicative identity 1 we have

$$u = u \cdot 1 = 1$$

□

Proof (of uniqueness of multiplicative inverses): Assume that $r \in R$ has a multiplicative inverse r^{-1}, and that $r' \in R$ is s.t. $r \cdot r' = 1$. Then multiplying the equation by r^{-1} on the left to obtain

$$r^{-1}(r \cdot r') = r^{-1} \cdot 1 = r^{-1}$$

by the property of 1. Using associativity of mult, the left hand side is

$$r^{-1}(r \cdot r') = (r^{-1} \cdot r) \cdot r' = 1 \cdot r' = r'$$

by prop. of mult inverses and of identity, Thus $r' = r^{-1}$ □

9.2 Ring Homomorphisms

~~Def:~~ ring homomorphisms are maps from one ring to another which preserve the ring structures.

Def: Ring homomorphism $f: R \to S$ from one ring R to another ring S is a map s.t $\forall r, r' \in R$ we have

$$f(r + r') = f(r) + f(r')$$
$$f(rr') = f(r)f(r')$$

That is, f preserves or respects both addition and multiplication. A ring homomorphism which is a bijection is an isomorphism. Two rings which are isomorphic are constructed as the same for all ring-theoretic purposes.

The kernal of a ring ~~isom~~ homomorphism $f: R \to S$ is

$$\ker f = \{r \in R : f(r) = 0\}$$

where (implicitly) the latter 0 is the ~~identit~~ additive identity in S.

Ex of a ring homomorphism

$f: \mathbb{Z} \to \mathbb{Z}/n$ given by

$f(x) = x \bmod n$

The assertion that this f is a ring homomorphism is the combination of the two assertions

$$x \bmod n + y \bmod n = (x+y) \bmod n$$

and $$(x \bmod n)(y \bmod n) = x \cdot y \bmod n$$

This homomorphism is called the reduction mod m homomorphism

Definition: A subset S of a commutative ring R is a subring if it contains 0, is closed under addition and the additive inverses, and is closed under multiplication

a subring is a ring in its own right, with the operations inherited from the ring inside which it ~~sis~~ sits

Definition: A subring I of a commutative ring R is ideal if

$$r \cdot i \in I$$

for all $r \in R$ and $i \in I$

Proposition: the kernal of any ring homomorphism $f: R \to S$ is an ideal in R

Proof. Let x be in the kernal, and $r \in R$ then

$$f(rx) = f(r) \cdot f(x) = f(r) \cdot 0 = 0$$

~~and~~ since we've proven that in any ring the product of anything w/ 0 is 0 by now. Thus rx is in the kernal of f. And for (x, y) both in the kernal

$$f(x+y) = f(x) + f(y) = 0 + 0 = 0$$

That is $x+y$ is also in the kernal and $f(0) = 0$, so 0 is also in the kernal. And for x in the kernal $f(-x)$,

$$f(-x) = -f(x) = -0 = 0,$$

so $-x$ is in the kernal

□

Evaluation and substitution homomorphisms - very important in applications

described as follows: Let R be a commutative ring, and $R[x]$ the polynomial ring in one variable with coefficients in R. Fix $r_0 \in R$ → talking about evaluating polynomials at r_0, or substituting r_0 for x in a polynomial

i.e.,

$\Rightarrow$ $P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_2 x^2 + a_1 x + a_0$

should be mapped to

$P(r_0) = a_n (r_0)^n + a_{n-1} (r_0)^{n-1} + \dots + a_2 (r_0)^2 + a_1 (r_0) + a_0$

Let $\boxed{e_{r_0}}$ denote this mapping, called the <u>evaluation map</u>

- the evaluation map $e_{r_0} : R[x] \to R$ is a ring homomorphism from the polynomial ring $R[x]$ to the ring R

Proof: Let $P(x) = \sum_{i=0}^{m} a_i x^i$

$Q(x) = \sum_{i=0}^{n} b_i x^i$

be two polynomials with coefficients in a comm. ring R.

First we show that the evaluation e_{r_0} at $r_0 \in R$ respects addition

$$e_{r_0}(P+Q) = e_{r_0}\left(\sum_j (a_j + b_j) x^j\right) = \sum_j (a_j + b_j) r_0^j$$

$$= \sum a_j r_0^j + \sum b_j r_0^j = e_{r_0}(P) + e_{r_0}(Q)$$

where $a_j = 0$ and $b_j = 0$ for any index outside the range for which coeff are defined

$\therefore$ the evaluation respects sums.

For products,

$$e_{r_0}(P \cdot Q) = e_{r_0}\left(\sum_{i,j} (a_i \cdot b_j) x^{i+j}\right) = \sum (a_i \cdot b_j) r_0^{i+j} =$$

$e_{r_0}(P) \cdot e_{r_0}(Q)$

$\therefore$ the evaluation respects products.

Thus, we can conclude that these evaluations really are ring isomorphisms

□

Proposition: Let $f : R \to S$ be a ring homomorphism. Let $0_R, 0_S$ be additive identities in R, S. respectively. Then $f(0_R) = 0_S$, i.e always the image of an additive identity under a ring homomorphism is the additive identity in the 'target' ring

→

Proof

First, $f(0_R) + f(0_R) = f(0_R + 0_R)$. Then

$0_R + 0_R = 0_R$ (property of additive identity in R)

so $f(0_R + 0_R) = f(0_R)$

together, we have

$$f(0_R) + f(0_R) = f(0_R + 0_R) = f(0_R)$$

Adding the additive inverse $-f(0_R)$ to both sides

$$(f(0_R) + f(0_R)) - f(0_R) = f(0_R) - f(0_R) = 0_S$$ (def of additive inverse)

using associativity of addition,

$$(f(0_R) + f(0_R)) - f(0_R) = f(0_R) + (f(0_R) - f(0_R))$$

$$= f(0_R) + 0_S = f(0_R)$$ (property of 0_S)

thus we can say

$$f(0_R) = (f(0_R) + \{f(0_R)) - f(0_R)\} =$$

$$f(0_R) - f(0_R) = 0_S$$

- Let $f: R \to S$ be a surjective ring homomorphism. Suppose that R has a multiplicative identity 1_R. Then S has a mult. iden. 1_S, and

$$f(1_R) = 1_S$$

Proof: Given $s \in S$, let $r \in R$ be such that $f(r) = s$. Then

$$f(1_R) \cdot s = f(1_R) \cdot f(r) = f(1_R \cdot r) = f(r) = s$$

Thus $f(1_R)$ behaves like the unit in S, by the uniqueness of units,

$$f(1_R) = 1_S$$

* important to note that the image of the multiplicative identity 1_R under a ring homomorphism $f: R \to S$ is not necessarily the multiplicative identity 1_S of S

Ask about Example in Book

9.3 Fields

A field is a subclass of commutative rings, eg. complex numbers, real numbers, rational numbers, and $\mathbb{Z}$ modulo primes. However integers are not

Definition (Field)

*A commutative ring R with unit 1 and such that any non-zero element of R has a multiplicative inverse (in R) is called a field

The commutative ring $\mathbb{Z}/p$ with p prime is a field.

Let $x \neq 0 \bmod p$ then p does not divide x.

Always $\gcd(x,p)$ is a divisor of p (and x), and since p is prime and does not divide x we have $\gcd(x,p) = 1$

Therefore there are integers r and s s.t. $rx + sy = 1$

Then $rx = 1 \bmod p$, so r is a multiplicative inverse of x in $\mathbb{Z}/p$

Exercises

X	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

9.05

Find the group of units in the rings:

$\mathbb{Z}/4$: $\{1, 3\}$

$\mathbb{Z}/5$: $\{1,2,3,4\}$

$\mathbb{Z}/6$: $\{1,5\}$

X	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	3	0	4	2
5	5	4	3	2	1

9.06

Find the group of units in the ring

$\mathbb{Z}/12$: $\{1, 5, 7, 11\}$

Chapter 10
Polynomials
10.1 Polynomials

The intuition we have for integers can be reused to a great extent in reasoning about polynomials with coefficients in a field.
Let k be a field, define the polynomial ring over k in one variable to be

$$k[x] = \{\text{polynomials with coefficients in } k\}$$

The ring $k[x]$ is a commutative ring, b/c polynomial multiplication is commutative.

We write a polynomial as a sum of 'constants' from k times non-negative integer powers of x:

$$f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_m x^m$$

The a_i's are the coefficients of the polynomial.
a_0 is the constant coefficient
If $a_n \neq 0$, then $a_n x^n$ is the highest-order term & a_m is the highest order coeff

summand $a_i x^i$ - degree i term
i is refered to as the order of the summand $a_i x^i$
The largest index i s.t the coeff a_i is non-zero is the degree of the polynomial

monic polynomial - highest order coeff is 1
two polynomials are equal $\iff$ coefficients of respective powers of x are all equal

Proposition: For polynomials P, Q with coefficients in a field k, the degree of the product is the sum of the degrees

$$\deg(P \cdot Q) = \deg P + \deg Q$$

Proof: The result is clear if either polynomial is the zero polynomial, so suppose that both are non-zero

Let

$$P(x) = a_m x^m + a_{m-1} x^{m-1} + \dots + a_2 x^2 + a_1 x + a_0$$
$$Q(x) = b_n x^n + b_{n-1} x^{n-1} + \dots + b_2 x^2 + b_1 x + b_0$$

where the highest-degree (a_m, b_n) coefficients are non-zero
Then in the product $P \cdot Q$ the highest degree ~~the~~ term is $a_m b_n x^{m+n}$, which only occurs once and has coeff $a_m \cdot b_n$. Since neither of these are 0 and since the product of non-zero elements of a field is non-zero, the coeff of x^{m+n} is non zero. □

Proposition:
(Cancellation Property)
Let $A \cdot P = B \cdot P$ for some non-zero polynomial P, where all of these polynomials have coefficients in a field k. Then $A = B$

Proof $A \cdot P = B \cdot P \Rightarrow (A - B) \cdot P = 0$.

Because the degree of the product is the sum of the degrees of the factors,

$$\deg(A - B) + \deg(P) = \deg 0 = -\infty \leftarrow \text{by convention}$$

since P is non-zero, $\deg P \geq 0$, then $\deg(A - B) = -\infty$

so $A - B = 0$, $A = B$ □

10.2 Divisibility

In a polynomial ring $K[x]$ with k a field

- Division algorithm exists and ∴ so ~~the~~ does the Euclidean Algorithm in nearly identical form
  - the degree of the remainder is less than the degree of the divisor

Proposition: Let K be a field and M a nonzero polynomial in $K[x]$
Let H be any other polynomial in $K[x]$

Then $H = \overbrace{Q}^{\text{quotient}} \cdot M + \overbrace{R}^{\text{remainder}}$

(notation: $R = H \,\%\, M$)

Ask about this proof

Proof: Let X be set of polynomials expressible in the form $H - S \cdot M$ for some polynomial S. Let $R = H - Q \cdot M$ be an element of X of minimal degree

Proposition:
A polynomial M divides another polynomial H iff $H \,\%\, M = 0$

Proof: If $H = Q \cdot M + R$ with $R = 0$, then clearly H is a multiple of M. Suppose $H = T \cdot M$ for some T. then by the uniqueness part of the reduction/division process, T would be the quotient and 0 is the remainder □

The gcd of two polynomials A, B is the monic (highest coef is 1) polynomial g of highest degree dividing both A and B

10.3 Factoring and irreducibility

we can factor polynomials just like we do with integers into a irreducible number (polynomial in our case)

naive method for this: trial division

Proper divisor D of F: $0 < \deg D < \deg F$,
moreover If F has a proper divisor, then it has a proper divisor D with

$$0 < \deg D \leq \frac{1}{2} \deg F$$

Low degree cases: Let k be a field

- Every linear polynomial in $k[x]$ is irreducible, since there is no value of "degree" b/t 1 and 0
- If a quadratic polynomial factors properly, then it must be the product of two linear factors
- " " cubic polynomial " ", then it must have at least one linear factor
- If a quartic or more polynomial factors properly, it may fail to have a linear factor

Prop: A polynomial $F(x)$ w/ coeff in a field k has a linear factor $x-a$ (w/ $a \in k$) iff $F(a) = 0$

Proof: $\Rightarrow$ $F(a) = (a-a)G(a) = 0 \cdot G(a)$ | $\Leftarrow$ division alg suppose $F(a)=0$: $F(x) = Q(x)\cdot(x-a) + R$, eval at a both sides

This gives to a slightly more economical way to test for linear factors

10.4 Euclidean Algorithm for polynomials

the Algorithm

Initialize $(F(x), G(x), R(x)) = (f(x), g(x), f(x) \,\%\, g(x))$

If $R(x) = 0$, then $\gcd(f(x), g(x)) = g(x)$

While $R(x) \neq 0$

replace $(F(x), G(x), R(x))$ with $(G(x), R(x), G(x) \,\%\, R(x))$

when $R(x) = 0$, the current value of $G(x)$ is the gcd

Ex. gcd of $x^5 + x + 1$ and $x^3 + x + 1$ considered as polynomials in $F_2[x]$

$$(x^5 + x + 1) - (x^2 + 1)(x^3 + x + 1) = x^2$$
$$(x^3 + x + 1) - (x)(x^2) = x + 1$$
$$(x^2) - (x+1)(x+1) = 1$$
$$(x+1) - (x+1)(1) = 0$$

relatively prime $\rightarrow$ gcd is 1

10.5 Unique Factorization of Polynomials

we can prove that the polynomial ring $k[x]$ has unique factorization into irreducible polynomials (prime)

Theorm: Given a non-zero polynomial P in $k[x]$, with a field k, P can be expressed as a product

$$P = c \cdot P_1^{e_1} \cdots P_n^{e_n}$$

where c is a non zero element of the field k, the P_i are irreducible monic polynomials, and e_i are positive integers

Proof: we need a peculiar characterization of the gcd of two polynomials, we showed earlier that for polynomials $f, g \in k[x]$ an element of the form $sf + tg$ (for some $s, t \in k[x]$) with the smallest degree is the gcd of f, g

Key Lemma: Let P be a irreducible polynomial. For two other polynomials A, B if $P \mid AB$ then $P \mid A$ or $P \mid B$

Proof: If $P \mid AB$ and $P \nmid A$ then $P \mid B$, then the gcd of P and A is just 1, therefore, we have $s, t \in k[x]$ s.t

$$1 = sA + tP$$

Then $B = B \cdot 1 = B \cdot (sA + tP) = s(AB) + (Bt)P$

Since $P \mid AB$, then P divides the right hand side, $\therefore P \mid B$