January 21, 2013

1 Commutative rings

Rings will be assumed commutative with identity.

Our primary examples of commutative rings are

- The integers.
- The integers modulo some ideal.
- The rational numbers.
- The real numbers.
- The complex numbers.
- Polynomial rings $R[x_1, \ldots, x_n]$ where R is a commutative ring.

Suppose that $R \subset S$ is a subring, and let $s_1, \ldots, s_n$ be elements of S. We denote by

$$R[s_1, \ldots, s_n]$$

the smallest subring of S containing the subring R and the elements $s_1, \ldots, s_n$. $R \hookrightarrow R[s_1, \ldots, s_n] \hookrightarrow S$

Every element in $R[s_1, \ldots, s_n]$ can be written as a sum of elements of the form

$$rs_1^{l_1} \cdots s_n^{l_n}$$

where $l_i \geq 0$ are integers and r is an element in R.

An ideal I in a ring R is an additive subgroup I of R such that for any $a \in I$ and $r \in R$ we have

$$ra \in I.$$

If I is an ideal in R, we say that I is generated by $a_1, \ldots, a_n$ if

- $a_1, \ldots, a_n$ are all in I
- Any $a \in I$ can be written as

  $$a = ra_1 \cdots a_n$$

  for some $r \in R$.

In this case, we write

$$I = (a_1, \ldots, a_n).$$

If an ideal I is generated by one element, we say that I is principal.

If I is an ideal in R, we form the abelian group of left cosets R/I. It is a ring with multiplication given by

$$(r + I)(s + I) = rs + I.$$

This construction is called a quotient ring.

2 Solutions of polynomials

Let $R \subset S$ be a subring. Elements $f \in R[x]$ are of the form

$$f = a_0 + a_1x + \cdots + a_nx^n.$$

A solution/zero of f in S is an element $s \in S$ such that

$$f(s) = a_0 + a_1s + a_2s^2 + \cdots + a_ns^n.$$

Examples

- $1 - 2x$ in $\mathbb{Z}[x]$ has no solutions in $\mathbb{Z}$. Embedding $\mathbb{Z}$ in $\mathbb{Q}$, we see that $\frac{1}{2}$ is a solution in $\mathbb{Q}$.
- $2 - x^2$ in $\mathbb{Z}[x]$ has no solutions in $\mathbb{Z}$ or $\mathbb{Q}$. Embedding $\mathbb{Z}$ in $\mathbb{R}$, we see that $\sqrt{2}$ is a solution in $\mathbb{R}$.
- $1 + x^2$ in $\mathbb{Z}[x]$ has no solutions in $\mathbb{R}$, but two solutions in $\mathbb{C}$ (namely $\pm i$).
- $1 + x + x^2 + x^3$ in $\mathbb{Z}[x]$ can be factorized as $(1 + x)(1 + x^2)$, and has one solution in $\mathbb{R}$ (-1), but three solutions in $\mathbb{C}$ (-1, $\pm i$).
- $1 + x + x^2 + x^3$ in $\mathbb{Z}/2[x]$ can be factorized as $(1 + x)^3$, and has only one solution (-1 = 1).

Let R be a ring, and r an element of R.

Definition 1. *r is invertible if there is an s such that*

$$rs = 1.$$

If r is invertible, then s is unique and we denote it by r^{-1}.

Examples In $\mathbb{Z}$, only ± 1 are invertible. In $\mathbb{Q}$, all numbers are invertible.

Definition 2. *r is a zero divisor if $r \neq 0$ and there is an $s \neq 0$ such that*

$$rs = 0.$$

In $\mathbb{Z}$ there are no zero-divisors.

Definition 3. *r is reducible if there are non-invertible a, b in R such that*

$$r = ab.$$

Definition 4. *r is irreducible if it is not reducible; that is, if $r = ab$, then either a is invertible, or b is.*

Definition 5. *r divides $s \in R$ (written $r|s$??) if*

$$s = ra$$

for some $a \in R$.

Definition 6. *r is prime if r is not invertible, and*

$$r|ab?? \Rightarrow r|a \text{ or } r|b.$$

Definition 7.

- *R is called a domain if it has no zero divisors.*
- *R is called a field if all non-zero elements are invertible. (A field has no zero divisors. Prove this!)*
- *R is a PID (Principal Ideal Domain) if it is a domain and all ideals are principal (generated by one element).*

Examples of domains

$$\mathbb{Z}, \mathbb{Z}[x], \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Q}[x], \ldots$$

Examples of fields

$$\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/p$$

where p is prime.

Examples of PID's

- If k a field, and I is an ideal in k, then either $I = (0)$ or $I = (1)$. (Prove this!)
- $\mathbb{Z}$ is a PID, since $\mathbb{Z}$ is cyclic as a group.
- k a field, $k[x]$ is a PID. Let I be a non-zero ideal in $k[x]$. Choose a non-zero f in I of minimal degree. For any $g \in I$, we have

  $$g = fh + r$$

  where $\deg(r) < \deg(f)$. This means that $r = g - fh \in I$, so $r = 0$ by our assumption that f is of minimal degree in I. This essentially hinges on the fact that k is a field. Why? Well, write $g = b_0 + b_1 x + \cdots + b_m x^m$ and $f = a_0 + a_1 x + \cdots + a_n x^n$ ($n \leq m$, otherwise we are done). To lower the degree of g, subtract $\frac{b_m}{a_n} x^{m-n} f$. This presupposes that a_n is invertible.

Homework?? Show why $\mathbb{Z}[x]$ is not a PID.

Proposition 1. *Let R be a domain, then any non-zero prime element of R is irreducible.*

Proof. Suppose that r is prime, and that $r = ab$ ($r|ab$??). Then WLOG $a = rs$, that is

$$r = rsb \Rightarrow r(1 - sb) = 0.$$

Since R is a domain, $1 - sb = 0$, so b is invertible. By symmetry we are done. □

It is however not true in general that irreducible elements are prime (even if R is a domain). (Construct a counter-example!)

Consider $\mathbb{Z}[\sqrt{5}]$ (which is not a UFD), and the factorizations

$$(1 - \sqrt{5})(1 + \sqrt{5}) = -4 = (-2)(2).$$

The elements are irreducible, but not prime. (Show this!)

In $\mathbb{Z}$, being prime is equivalent to being irreducible. This actually holds true in all UFD's.

Proposition 2. *An element r in R is prime if and only if $R/(r)$ is a domain.*

Proof. Assume that r is prime. $[a], [b] \in R/(r)$. If $[a] \cdot [b] = 0$, then $ab \in (r)$, i.e. $r|ab$??. Now $r|a$ or $r|b$, so either $[a] = 0$ or $[b] = 0$.

To show the converse, suppose that $R/(r)$ is a domain. $r|ab$ means that $[a][b] = 0$, so $[a] = 0$ or $[b] = 0$. Hence $r|a$ or $r|b$, that is r is prime. □

Definition 8. *R is a UFD if it is a domain and every element in R can be written as a product of primes.*

Proposition 3. *Let R be a UFD. Then*

- *Irreducible elements are prime.*
- *Any two factorizations into primes are equivalent up to invertible elements. That is, if for some primes p_i, q_i we have*

$$p_1 \cdots p_m = q_1 \cdots q_n,$$

then $m = n$, and after an appropriate permutation we get

$$p_i = a_i q_i$$

for all $1 \leq i \leq n$ and some invertible elements a_i.