Intro to Modern Algebra II

Robert Friedman

Transcribed by Ron Wu

This is an advanced undergraduate course, offered in spring 2013 at Columbia University. Recommended books are Michael Artin, *Algebra*; Dummit, Foote, *Abstract Algebra*; Fraleigh, *A First Course in Abstract Algebra*, Gallian, *Contemporary Abstract Algebra*, Hungerford, *Abstract Algebra: An Introduction*, I. Herstein, *Abstract Algebra*, S. Lang, *Undergraduate Algebra*. Office hours: M 8:30-9:30, Th 2-3.

Contents

1 Rings

Lecture 1 (1/23/13)

Last semester, we studied groups, and studying (finite) group is really studying symmetry. This course we study rings, and study rings is to study factorization.

1.1 Rings

Definition 1. a *ring* $\mathcal{R} = (\mathcal{R}, +, \cdot)$ with two binary operators $+$, $\cdot$, such that

(i) $(\mathcal{R}, +)$ is an abelian group; (ii) $(\mathcal{R}, \cdot)$ is an associative binary structure; (iii) left, right distribution law hold, namely $\forall\, r, s, t \in \mathcal{R}$, $r(s+t) = rs + rt$ and $(s+t)r = st + tr$.

Of course the mathematical word "ring" makes no reference to circle. And in the definition (ii) binary means take $x, y \in \mathcal{R}$ sending to $z \in \mathcal{R}$, so by definition it is a closed operation. Notice (iii) links (i) and (ii).

Definition 2. $\mathcal{R}$ is *commutative* if $\cdot$ is commutative.

Definition 3. If $\mathcal{R}$ has a *unity* 1 (multiplicative identity) i.e. $\exists\, 1 \in \mathcal{R}$, $1r = r1 = r\ \forall\, r$, we say $\mathcal{R}$ is unital.

As usual, a unity is unique if it exists.

Definition 4. Suppose $\mathcal{R}$ is a ring with unity, a *unit* $r \in \mathcal{R}$ is an element which has a multiplicative inverse, i.e. $\exists\, r'$, $rr' = r'r = 1$.

Since such inverse is unique, we denote it r^{-1}.

Definition 5. $\mathcal{R}^* = \{r \in \mathcal{R} : r \text{ is a unit}\}$. (we assume $\mathcal{R}$ has a unity, so we don't want $\mathcal{R}^* = \varnothing$).

Exercise 6. check $(\mathcal{R}^*, \cdot)$ is a group.

Use definition of a ring, one can show

$$0r = r0 = 0$$

Proof. $0 + 0 = 0 \implies r0 + r0 = r(0+0) = r0 \implies r0 = 0$. ($\because (\mathcal{R}, +)$ is group, $0\ \exists$) □

One can also show

$$(-r)s = -(rs) = r(-s)$$

Proof. $(-r)s + rs = (-r + r)s = 0s = 0 \implies (-r)s = -(rs)$. ($\because (\mathcal{R}, +)$ is group, $-r\ \exists$) $\square$

Definition 7. If $\mathcal{R}^* = \mathcal{R}\backslash\{0\}$, we call $\mathcal{R}$ is a *division ring*. (as before assume $\mathcal{R} \neq \{0\}$)

Definition 8. We call a commutative division ring a *field*.

Example 9. (of rings of numbers) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Notice $\mathbb{N}$ is not a ring, because $(\mathbb{N}, +)$ not a group.

$\mathbb{Z}$ is commutative ring with unity, and $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are fields.

Also $n\mathbb{Z} = \langle n \rangle = \{nk : k \in \mathbb{Z}\}$ is a ring (if $n \neq \pm 1$, it has no unity. cf example 24), check $\mathbb{Z}^* = \{\pm 1\}$, $\mathbb{Q}^* = \mathbb{Q} - \{0\}$.

$(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ a commutative ring with unity. $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)^* = \{[a] : qcd(a, n) = 1\}$ i.e. a relative prime to n. The addition and multiplication are inherited from $\mathbb{Z}$.

When is $\mathbb{Z}/n\mathbb{Z}$ a field?

$\iff n = p$ a prime.

Definition 10. We denote $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ "the" field with p elements.

Example 11. (of rings of matrix) We call $M_n(\mathbb{R}) = n \times n$ matrices with real coefficients. One can add, multiply and $\exists$ unity $= I$. If $n > 1$, $M_n(\mathbb{R})$ not commutative.

Because it is possible $\exists\, A, B$ both non-zero, but $AB = 0$, $\implies$ either A or B is not invertible $\implies M_n(\mathbb{R})$ is not a division ring.

One can also take $M_n(\mathbb{Q})$, $M_n(\mathbb{C})$, $M_n(\mathbb{Z})$, and $M_n^*(\mathbb{R}) = GL_n(\mathbb{R})\{A : \det A \neq 0\}$, $M_n(\mathbb{Z}) = \{A : \det A = \pm 1\}$.

More general if $\mathcal{R}$ any ring, we have $M_n(\mathcal{R})$ a ring.

If $\mathcal{R}$ has a unity, $M_n(\mathcal{R})$ has a unity, and $M_n^*(\mathcal{R}) = \{A : \det A \in \mathcal{R}^*\}$.

Example 12. (of trivial rings) $\mathcal{R} = \{0\}$ commutative with unity $1 = 0$, which is the only ring has $1 = 0$.

Take $(A, +)$ any abelian group define $ab = 0\ \forall\, a, b \in A$, then it is also a ring, but not interesting either.

Example 13. (of ring of functions) Recall $\mathbb{R}^{\mathbb{R}}$ = set of all functions $f : \mathbb{R} \to \mathbb{R}$.

We have pointwise addition and pointwise multiplication. $f(x)+g(x) = (f+g)(x)$ etc. Notice it is not composition, because normally composition is not distributive.

Also $C(\mathbb{R})$ continuous function from $\mathbb{R}$ to $\mathbb{R}$ is a ring.

Check replace continuous be differentiable, also gives a ring.

More general let X be any set, $\mathcal{R}$ be a ring

$$\mathcal{R}^X = \text{set of all funtions } f : X \to \mathcal{R}$$

again is a ring under pointwise addition and multiplication.

Example 14. (of product rings) $\mathcal{R}_1$, $\mathcal{R}_2$ 2 rings, then define

$$\mathcal{R}_1 \times \mathcal{R}_2 = \{(r_1, r_2), r_1 \in \mathcal{R}_1, r_2 \in \mathcal{R}_2\}$$

is a ring under component addition and multiplication.

Example 15. (of polynomial rings) Recall

$$\mathbb{R}[x] = \text{set of all polynomials}$$

product is given by

$$(a_n x^n + ... + a_0)(b_m x^m + ... + b_0) = \sum c_i x^i$$

where $c_i = \sum_{j+k=i} a_j b_k$

One can define $\mathcal{R}[x]$ for any $\mathcal{R}$ that has unity ($\because$ one wants to have x to mean $1 \cdot x$.), and $\mathcal{R}$ is commutative.

Example 16. (Exotic)

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$$

notice the square bracket used here, will be explained later.

$$\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$$

$$\mathbb{R} \subseteq \mathbb{C} = \mathbb{R}(i) = \{a + bi : a, b \in \mathbb{R}\}$$

$$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$$

$$\mathbb{Z}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 : a, b, c \in \mathbb{Z}\}$$
$$\mathbb{Q}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 : a, b, c \in \mathbb{Q}\}$$

Check they are rings. Particular what to do

$$\frac{1}{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2} =?$$

Example 17. (of ring of quaternion) $\mathbb{H} = \{a+bi+cj+dk : a, b, c, d \in \mathbb{R}\}$ with $i^2 = j^2 = k^2 = 1$ and $ij = \epsilon_{ijk}k$, etc.

Exercise 18. Check this is a division ring.

Definition 19. If $\mathcal{R}$, $\mathcal{S}$ are 2 rings, f is a *homomorphism* $\mathcal{R} \to \mathcal{S}$ if $\forall\, r, s \in \mathcal{R}$

$$f(r + s) = f(r) + f(s)$$
$$f(rs) = f(r)f(s)$$

Definition 20. If f is also homomorphism + bijection, we says f is an *isomorphism*.

Example 21. By Chinese reminder theorem, if $gcd(n, m) = 1$, then

$$\mathbb{Z}/nm\mathbb{Z} \cong (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$$

Definition 22. $\mathcal{R}$ is a subring of $\mathcal{S}$, denoted $\mathcal{R} \leq \mathcal{S}$, if $(\mathcal{R}+)$ is a subgroup of $(\mathcal{S}+)$ and $\mathcal{R}$ is closed under multiplication.

Proposition 23. $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$.

Important modifications to the definition of homomorphism.

If $\mathcal{R}, \mathcal{S}$ both have unity 1, we will require any homomorphism $f : \mathcal{R} \to \mathcal{S}$ satisfy $f(1) = 1$. Also for $\mathcal{R}$ to be a subring of $\mathcal{S}$, $\mathcal{R}$ has to contain the same 1 from $\mathcal{S}$.

Example 24. $n\mathbb{Z} \subseteq \mathbb{Z}$ but if $n > 1 \implies 1 \notin n\mathbb{Z}$. We will not call $n\mathbb{Z}$ a subring of $\mathbb{Z}$.

Example 25. $\mathbb{Z} \times \mathbb{Z}$, it has unity (1,1), subgroup $\mathbb{Z} \times \{0\}$ has unity $(1, 0)$, so we will not call $\mathbb{Z} \times \{0\}$ a subring of $\mathbb{Z} \times \mathbb{Z}$.

Lecture 2 (1/28/13)

Proposition 26. *If $f : \mathcal{R} \to \mathcal{S}$ is homomorphism, then*

$$Imf = f(\mathcal{R})$$

is a subring of $\mathcal{S}$.

Proof. All to check.

1) $f(\mathcal{R})$ is a subgroup under addition

2) closed under multiplication. Given $f(r), f(s) \in f(\mathcal{R})$, then $f(r) \cdot f(s) = f(rs) \in f(\mathcal{R})$.

3) Is $1 \in f(\mathcal{R})$? Yes, because we assume $f(1) = 1$. □

Example 27. $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is a ring homomorphism.

Example 28. $\mathcal{R}_1 \times \mathcal{R}_2 \to \mathcal{R}_1$ is a ring homomorphism. note $\pi_1(1,1) = 1$

Example 29. $\mathcal{R}_1 \to \mathcal{R}_1 \times \mathcal{R}_2$, $r \mapsto (r, 0)$ not a ring homomorphism, if $\mathcal{R}_2 \neq \{0\}$.

1.2 Polynomial Ring

It is easy to see that one can generalize from the definition of a ring to get

1) Generalized distributive law

$$(r_1 + ... + r_n)(s_1 + ... + s_m) = \sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} r_i s_j$$

2) one can define for $n \in \mathbb{N}$,

$$r^n = \underbrace{r \cdot r \cdot ... \cdot r}_{n \text{ times}}$$

do this inductively

$$r^1 = r$$

$$r^{n+1} = r^n \cdot r$$

then one gets some properties

$$r^n \cdot r^m = r^{n+m}$$

$$(r^n)^m = r^{nm}$$

there is a convention:

$$r^0 = 1$$

if $1 \in \mathcal{R}$. Recall last time if $r =$unit, r^{-1} exist. One can then say

$$r^{-n} = (r^{-1})^n$$

Theorem 30. *(Binomial Theorem) if $\mathcal{R}$ commutative ring*

$$(r+s)^n = \sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) r^k s^{n-k}$$

where $\left(\begin{array}{c} n \\ k \end{array} \right) = \frac{n!}{k!(n-k)!}$.

Proof.

$$(r+s)^n = (r+s)...(r+s)$$

expand the product, one gets each term has total degree n, selecting similar terms. How many terms are $r^k s^{n-k}$, that is n choose k, so

$$\left(\begin{array}{c} n \\ k \end{array} \right) r^k s^{n-k}$$

□

An alternative proof by induction

Proof. if $n = 1$, okay

$$\begin{aligned}
(r+s)^{n+1} &= (r+s)^n (r+s) \\
&= \sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) r^k s^{n-k} (r+s) \\
&= \sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) r^{k+1} s^{n-k} + \sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) r^k s^{n+1-k} \\
&= r^{n+1} + s^{n+1} + \sum_{k=1}^{n} \left[\left(\begin{array}{c} n \\ k-1 \end{array} \right) + \left(\begin{array}{c} n \\ k \end{array} \right) \right] r^k s^{n+1-k} \\
&= r^{n+1} + s^{n+1} + \sum_{k=1}^{n} \left(\begin{array}{c} n+1 \\ k \end{array} \right) r^k s^{n+1-k} \\
&= \sum_{k=0}^{n+1} \left(\begin{array}{c} n+1 \\ k \end{array} \right) r^k s^{n+1-k}
\end{aligned}$$

we used $\left(\begin{array}{c} n \\ k-1 \end{array} \right) + \left(\begin{array}{c} n \\ k \end{array} \right) = \left(\begin{array}{c} n+1 \\ k \end{array} \right)$ from Pascal triangle. □

Definition 31. $\mathcal{R}[x]$ set of all polynomials with coefficients in $\mathcal{R}$, where $\mathcal{R}$ is a commutative ring with unity, i.e.

$$\mathcal{R}[x] \ni f(x) = \sum_{i=0}^{n} a_i x^i \tag{1.1}$$

Note: here n must be finite, for $n = \infty$, power series, will come later. But we are not going to talk about negative power. That is because

(1) they are not polynomials in ordinary sense (2) Use composition will get thing like

$$\frac{1}{x^2 - 4}$$

bad for evaluation. (3) they make bad factors.

In order to make (1.1) well defined, we need to handle the case that two polynomials are equal.

Three ways to do that, all of them are to make sure the following are equal, e.g

$$3x + x^3 = 0 + 3x + 0x^2 + x^3 + 0x^{13}$$

way 1)

$$\sum_{i=0}^{n} a_i x^i = \sum_{i=0}^{m} b_i x^i$$

if $n \geq m$ and $a_i = b_i$ $i \leq m$, $a_i = 0$ for $i > m$.

way 2)

$$f(x) = \sum_{i=0}^{\infty} a_i x^i$$

$a_i \in \mathcal{R}$ $\exists N$ $a_i = 0$ for $i \geq N$.

way 3)

$$f(x) \leftrightarrow (a_0, a_1, ..., a_i, ...)$$

a sequence in $\mathcal{R}$ such that $\exists N$ $a_i = 0$ for $i \geq N$. e.g

$$x \leftrightarrow (0, 1, 0, ...)$$

Notice

$$\mathcal{R} \leq \mathcal{R}[x]$$

now $\mathcal{R}$ has the meaning of constant polynomials. In way 3)'s notation

$$r \in \mathcal{R} \leftrightarrow rx^0 \leftrightarrow (r, 0, 0, ...)$$

Definition 32. If $f(x) = \sum_{i=1}^{n} a_i x^i \in \mathcal{R}[x]$, the largest i s.t.

$$a_i \neq 0$$

is called *degree* of $f(x)$, denoted as $deg(f)$.

Notice $0 \in \mathcal{R} \leq \mathcal{R}[x]$, by convention

$$deg(0) = \text{undefined}$$

but for $r \in \mathcal{R} \leq \mathcal{R}[x]$,

$$deg(r) = 0$$

The reason for that will become clear soon.

Definition 33. If $d = deg(f)$, a_d =leading coefficient.

Definition 34. If the leading coefficient is 1, we say f is *monic*.

Definition 35. We called a_0 the constant term.

Let us define the operations on $\mathcal{R}[x]$ to make it a ring.
If $f(x) = \sum_{i=1}^{n} a_i x^i$, $g(x) = \sum_{i=1}^{m} b_i x^i$,

$$f(x) + g(x) = \sum (a_i + b_i) x^i$$

for addition, sequence notation (way 3) is easier to manipulate.

$$f(x) \cdot g(x) = \sum_{k=0}^{n+m} \sum_{i+j=k} a_i b_j x^k$$

Claim 36. $(\mathcal{R}[x], +, \cdot)$ is a commutative ring with unity.

Proof. commutative is clear. The product of the three polynomials are same regardless the order

$$\left(\sum_{i=0}^{n} a_i x^i \right) \left(\sum_{i=0}^{m} b_i x^i \right) \left(\sum_{i=0}^{p} c_i x^i \right) = \sum_{t=0}^{n+m+p} \sum_{i+j+k=t} a_i b_j c_k x^t$$

multiplication is associative and distributive over addition is also clear. □

In following two theorems, we assume $f, g \neq 0$.

Theorem 37.

$$deg(f+g) \leq Max(\deg(f), \deg(g))$$

One should expect the equality to hold in most situation, unless there is some cancellation in the leading coefficients, e.g.

$$(x+2)+(-x+1)$$

Theorem 38.

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

The reason we don't have strict equality, because e.g in $\mathbb{Z}/6\mathbb{Z}[x]$

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

One reason for no one defines

$$\deg 0 = 0$$

that is because of the following proposition

Proposition 39. *If $f(x)$ is monic,*

$$\deg fg = \deg f + \deg g$$

But some people define

$$\deg 0 = -\infty$$

this will even take care of theorems 37, 38.

Definition 40. For polynomials in several variables, one can first define

$$\mathcal{R}[x_1, x_2] \ni f(x_1, x_2) = \sum_{0 \leq i,j \leq N} a_{ij} x_1^i x_2^j$$

$a_{ij} \in \mathcal{R}$. Then inductively define

$$\mathcal{R}[x_1, ..., x_n] = \mathcal{R}[x_1, ..., x_{n-1}][x_n]$$

Since people normally think polynomials not as rings but functions, we would like to evaluate $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathcal{R}[x]$ for some given $r \in \mathcal{R}$, we of course want

$$f(r) = \sum_{i=0}^{n} a_i r^i \in \mathcal{R}$$

so let's formulate this.

Definition 41. Given $r \in \mathcal{R}$, we let

$$ev_r : \mathcal{R}[x] \to \mathcal{R}$$

$$ev_r(f(x)) = f(r)$$

In the notation, find a zero of $f(x) \iff$ find r s.t. $ev_r(f(x)) = 0$.

Claim 42. $ev_r : \mathcal{R}[x] \to \mathcal{R}$ is a ring homomorphism.

Proof. one will have to check multiplication and addition i.e.

$$ev_r(fg) = ev_r f \cdot ev_r g$$

and

$$ev_r(f + g) = ev_r f + ev_r g$$

and

$$ev_r(1) = 1$$

□

There is another way of thinking polynomial rings as functions, more direct way.

Recall $\mathcal{R}^{\mathcal{R}}$ = set of functions $\mathcal{R} \to \mathcal{R}$, we studied last time, it is a ring under pointwise multiplication and addition.

Definition 43. let

$$E : \mathcal{R}[x] \to \mathcal{R}^{\mathcal{R}}$$

then given $f(x) \in \mathcal{R}[x]$,

$$E(f(x))(r) = f(r) = ev_r f(x)$$

which is the usual way of think, polynomials as functions.

Claim 44. E is a ring homomorphism from $\mathcal{R}[x] \to \mathcal{R}^{\mathcal{R}}$.

Proposition 45. *For $\mathcal{R} = \mathbb{R}$,*

$$E : \mathbb{R}[x] \to \mathbb{R}^{\mathbb{R}}$$

is injective.

Hence the real polynomials as algebraic objects are specified by polynomials as functions i.e. its value at each point. But the proposition is not true for an arbitrary $\mathcal{R}$.

Example 46. take finite $\mathcal{R}$ e.g. $\mathcal{R} = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, $\mathcal{R}^{\mathcal{R}}$ is finite, but $\mathcal{R}[x]$ is always infinite. so cannot find injection $\mathcal{R}[x] \to \mathcal{R}^{\mathcal{R}}$.

This is the reason for us, we should think polynomials as algebraic object. If we need to treat it as functions, just do an evaluate at some points

Lecture 3 (1/30/13)

Before we finish ring polynomials, there are some variants of evaluation to mention

1st variance

Suppose $\mathcal{R} \leq \mathcal{S}$, $s \in \mathcal{S}$, then

$$ev_s\mathcal{R}[x] \to \mathcal{S} \tag{1.2}$$

$$ev_s f(x) = f(s)$$

Clearly $\mathcal{R}[x] \leq \mathcal{S}[x]$, so (1.2) is just composition

$$\mathcal{R}[x] \to \mathcal{S}[x] \overset{ev}{\to} \mathcal{S}$$

Proposition 47. *$ev_s(\mathcal{R}[x])$ is a subring of $\mathcal{S}$.*

We write $ev_s(\mathcal{R}[x]) = \mathcal{R}[s] = \left\{\sum a_i s^i | a_i \in \mathcal{R}\right\} \leq S$.

Example 48. $\mathbb{R} \leq \mathbb{C}$, $f(x) \in \mathbb{R}[x]$, then

$$ev_i f(x) = f(i) \in \mathbb{C}$$

$$ev_i(x^2 + 1) = 0$$

this shows we can get 0 which cannot be achieved before.

Example 49. $ev_{\sqrt{2}} : \mathbb{Z}[x] \to \mathbb{R}$, we write

$$\mathbb{Z}[\sqrt{2}] = \{n + m\sqrt{2} : n.m \in \mathbb{Z}\}$$

also from lecture one

$$\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\} \leq \mathbb{C}$$

$$\mathbb{Q}(i) = \{a + bi | a, b \in \mathbb{Q}\} \leq \mathbb{C}$$

notice () is used for field, and [] for not a field, hence $\mathbb{Q}(i)$ is a field.

2nd variance

Given

$$\rho : \mathcal{R} \to \mathcal{S}$$

ρ a ring homomorphism $\mathcal{R} \to \mathcal{S}$, one can get

$$\rho : \mathcal{R}[x] \to \mathcal{S}[x]$$

with

$$\rho\left(\sum a_i x^i\right) = \sum \rho(a_i) x^i$$

Example 50. $\rho : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ (reduce mod n), then $\rho : \mathbb{Z}[x] \to \mathbb{Z}/n\mathbb{Z}[x]$, that is meaning reduce first then do the product or reduce the coefficient then do the product.

3rd variance

Given $\rho : \mathcal{R} \to \mathcal{S}$ and $s \in \mathcal{S}$

$$ev_{\rho,s} : \mathcal{R}[x] \to \mathcal{S}$$

by

$$\mathcal{R}[x] \xrightarrow{\rho} \rho[x] \to \mathcal{S}$$

4th variance

Several variables. Given $\mathcal{R} \leq \mathcal{S}$, given s_1, s_2, ... , $s_n \in \mathcal{S}$

$$ev_{s_1,s_2,...,s_n} : \mathcal{R}[s_1, s_2, ..., s_n] \to \mathcal{S}$$

by

$$ev_{s_1,s_2,...,s_n} f(x_1, x_2, ..., x_n) = f(s_1, s_2, ..., s_n)$$

this gives a subring. In fact this is the smallest subring that contains both $\mathcal{R}$ and $[s_1, s_2, ..., s_n]$.

Example 51. $\mathbb{Z}[\sqrt[3]{2}, i, \pi] \leq \mathbb{C}$.

1.3 Integral Domain

Our biggest interest of the course is factorization.

Definition 52. Let $\mathcal{R}$ be a ring, then $r \in \mathcal{R}$ is a *divisor* of 0 if $r \neq 0$, and $\exists\, s \in \mathcal{R}$ s.t.

$$s \neq 0 \text{ and } rs = 0$$

Example 53. In $\mathbb{Z}/6\mathbb{Z}$, 2, 3 are divisors of 0.

Definition 54. An element $r \in \mathcal{R}$ is *nilpotent* if $\exists\, n \in \mathbb{N}$

$$r^n = 0$$

note: 0 is nilpotent.

Example 55. In $\mathbb{Z}/4\mathbb{Z}$, 2 is nilpotent since $2^2 = 0$.

Lemma 56. *If $r \in \mathcal{R}$ a nilpotent, and $r \neq 0$, then*

r is a divisor of 0.

Proof. Know $r^n = 0$ some $n \in \mathbb{N}$, choose the smallest such n

Note $n > 1$, since $r^1 = r \neq 0$, so

$$r^n = r^{n-1} r$$

$r^{n-1} \in \mathcal{R}$, and $r^{n-1} \neq 0$ because n is the smallest. □

Remark 57. The converse is not true. In $\mathbb{Z}/6\mathbb{Z}$, 2 is a divisor of 0 but 2 is not nilpotent.

Definition 58. $\mathcal{R}$ is an *integral domain* if $\mathcal{R} \neq \{0\}$,(i.e. $1 \neq 0$) and there are no zero divisor in $\mathcal{R}$, i.e. if $r, s \in \mathcal{R}$

$$r \neq 0,\ s \neq 0 \implies rs \neq 0.$$

Example 59. $\mathbb{Z}$ is an integral domain.

Proposition 60. *Any field is an integral domain.*

Proof. F is a field, suppose $r, s \in F$, $r \neq 0$, $s \neq 0$ but $rs = 0$. Since $\exists\, r^{-1} \in F$

$$0 = r^{-1}0 = r^{-1}(rs) = 1s = s$$

we used the fact that $1 \neq 0$. □

Clearly any subring of an integral domain is an integral domain.

Example 61. take a subring of a field

$$\mathbb{Z} \leq \mathbb{Q} \qquad \mathbb{Z}[\sqrt[3]{2}] \leq \mathbb{R}$$

Proposition 62. *If $\mathcal{R}$ is an integral domain, then $\mathcal{R}[x]$ is an integral domain.*

In particular if F is a field, then $F[x]$ is an integral domain, but clearly $F[x]$ is not a field.

Proof. If $f(x) \neq 0$, $g(x) \neq 0 \in \mathcal{R}[x]$, $\mathcal{R}$ an integral domain. Then the leading coefficient of fg is

$$a_n b_m$$

$\mathcal{R}$ an integral domain $\implies a_n b_m \neq 0$, so $fg \neq 0$. □

Corollary 63. *If $\mathcal{R}$ is an integral domain*

$$(\mathcal{R}[x])^* = \mathcal{R}^*.$$

Example 64. If F a field,

$$(F[x])^* = F^* = F - \{0\}$$

non-zero constant polynomials.

$$(\mathbb{Z}[x])^* = \mathbb{Z}^* = \{\pm 1\}$$

Proof. say $f(x) \in (\mathcal{R}[x])^*$, so $f(x) \neq 0$, and $\exists\, g(x) \neq 0$ s.t.

$$\begin{aligned} f(x)g(x) = 1 &\implies \deg f + \deg g = \deg fg = \deg 1 = 0 \\ &\implies \deg f = \deg g = 0 \end{aligned}$$

so $f(x) = r \in \mathcal{R}$, and $g(x) = s \in \mathcal{R}$, s.t. $rs = 1 \implies \mathcal{R}^*$. □

Example 65. In $\mathbb{Z}/4\mathbb{Z}[x]$,

$$(1 + 2x)$$

is a unit, and it's nilpotent.

$$(1 + 2x)(1 + 2x) = 1$$

Definition 66. If $\mathcal{R}$ is a ring, the *cancellation law* holds in $\mathcal{R}$ if $\forall\, r, s, t \in \mathcal{R}$ with $r \neq 0$,

$$rs = rt \implies s = t$$

Proposition 67. *If $\mathcal{R} \neq \{0\}$, $\mathcal{R}$ is an integral domain $\iff$ cancellation law holds.*

Proof. ($\implies$) suppose $rs = rt$, $r \neq 0$

$$\begin{aligned} &\implies && rs - rt = 0 \\ &\implies && r(s-r) = 0 \\ &\implies && s - r = 0 \\ &\implies && s = r \end{aligned}$$

($\impliedby$) say $rs = 0$, $r \neq 0$

$$rs = 0 = r0 \implies s = 0$$

□

Let $\mathcal{R}$ be an integral domain (often a field), we take $1 \in \mathcal{R}$ as a generator

$$\langle 1 \rangle = \{n \cdot 1 | n \in \mathbb{Z}\} \leq (\mathcal{R}, +)$$

This is also a subring: closed under multiplication

$$(n \cdot 1)(m \cdot 1) = nm \cdot 1$$

of course $1 \in \langle 1 \rangle$.

If we think this as a group

$$\langle 1 \rangle \text{ is cyclic} \cong \begin{cases} \mathbb{Z} & \text{if 1 is infinite order} \\ \mathbb{Z}/d\mathbb{Z} & \text{if the smallest } d \in \mathbb{N} \text{ s.t. } d \cdot 1 = 0 \end{cases}$$

Definition 68. For an integral domain $\mathcal{R}$ we call such d the characteristic of $\mathcal{R}$. Denoted as char$\mathcal{R}$. If 1 has ∞ order, we say char$\mathcal{R} = 0$.

Notice we only define char for integral domains, if one tries to do this for general ring, some strange things will happen.

Example 69. For $\mathcal{R} = \mathbb{Z}$,$\mathbb{Q}$,$\mathbb{R}$, $\mathbb{C}$. char$\mathcal{R} = 0$. For $\mathcal{R} = \mathbb{Z}/p\mathbb{Z}$, char$\mathcal{R} = p$.

Proposition 70. *$\mathcal{R} \leq \mathcal{S}$, then char$\mathcal{R}$ =char$\mathcal{S}$.*

Proposition 71. *$\mathcal{R}$ an integral domain, then either char$\mathcal{R} = 0$, or char$\mathcal{R} = p$, p a prime.*

Proof. Say $\exists$ smallest d s.t.

$$d1 = 0$$

suppose d can be factored $d = mn$, $m, n \in \mathbb{N}$, so

$$\begin{aligned} 0 &= d1 \\ &= (m1)(n1) \end{aligned}$$

so $m1 = 0$ or $n1 = 0$, but d is the smallest so $m = d$ or $n = d$, so d is a prime. □

Suppose $r \in \mathcal{R}$, $r \neq 0$. suppose $d \in \mathbb{N}$, $d \cdot r = 0$, then $0 = (d \cdot 1)(r) \implies d \cdot 1 = 0 \implies \text{char}\mathcal{R}|d$. Conversely if $\text{char}\mathcal{R}|d \implies d \cdot r = (d \cdot 1)r = 0$. Therefore we have proved the following

Corollary 72. *$\mathcal{R}$ an integral domain, if $\text{char}\mathcal{R} = p \neq 0$, then every nonzero element of $\mathcal{R}$ has order p in $(\mathcal{R}, +)$. If $\text{char}\mathcal{R} = 0$, then every nonzero element of $\mathcal{R}$ has order ∞ in $(\mathcal{R}, +)$.*

Lecture 4 (2/4/13)

As from now on, we always work with $\mathcal{R}$ that is commutative and has unity.

Proposition 73. *If $\mathcal{R}$ is a finite integral domain, then $\mathcal{R}$ is a field.*

Proof. Let $r \in \mathcal{R}$, $r \neq 0$, consider $r, r^2, .., r^n$, then exists $n < m$ with $r^n = r^m$ say $m = n + k$ then

$$r^n = r^m = r^{n+k} = r^n \cdot r^k$$

knowing $r \neq 0 \implies r^n \neq 0$, ($\because$ R is an integral domain if $r^n = 0$ then either $r = 0$ or if not then $r^{n-1} = 0$ use reduction gives $r = 0$.)

So $1 = r^k$ or

$$r^{k-1} = r^{-1}$$

which says r has a multiplicative inverse. □

1.4 Quotient Field

Recall from last lecture, $\mathcal{R} \leq \mathcal{S} \implies \text{char}\mathcal{R} = \text{char}\mathcal{S}$. We learned also if F a field, $\mathcal{R} \leq F \implies \mathcal{R}$ is an integral domain.

Now we ask given an integral domain $\mathcal{R}$, is it contained in a field of $\mathcal{S}$ as a subring?

Example we have in mind, $\mathbb{Z} \leq \mathbb{Q} = \{a/b | a, b \in \mathbb{Z}, b \neq 0$ with relation $a/b = c/d \iff ad = bc\}$. This suggests to relate

$$a/b \leftrightarrow (a, b) \in \mathbb{Z} \times (\mathbb{Z} - \{0\})$$

with

$$(a, b) \sim (c, d) \iff ad = bc \tag{1.3}$$

Claim 74. (1.3) is an equivalence relation.

So we understand $\mathbb{Z} \times (\mathbb{Z} - \{0\})/\sim$ are equivalence class (a, b), but we will still use the notation a/b.

One can then define operations in $\mathbb{Q}$ as usual

$$a/b + c/d = \frac{ad + bc}{bd}$$

$$(a/b)(c/d) = ad/bd$$

Note 75. These are well defined. (i.e. check they are independent of the representations)

Note 76. With these operations, $(\mathbb{Q}, +\cdot)$ is a ring.

Note 77. $\mathbb{Z} \leq \mathbb{Q}$ The notion of subring here is loosely defined. Since pedantically elements in $\mathbb{Z}$ are not the elements in $\mathbb{Q}$, but with the following injective homomorphism

$$\rho : \mathbb{Z} \to \mathbb{Q}$$

$$n \mapsto n/1$$

We now use this idea.

Given integral domain $\mathcal{R}$, we consider the fields of all quotients of $\mathcal{R}$, denoted by

$$Q(\mathcal{R}) = \{r/s : r, s \in \mathcal{R}, s \neq 0\} \in \mathcal{R} \times (\mathcal{R} - \{0\})$$

with

$$(r, s) \sim (t, w) \iff rw = st$$

Claim 78. This is an equivalence relation.

Proof. (1) $(r,s) \sim (s,r) \iff rs = sr$

(2) $(r,s) \sim (t,w) \iff rw = st \iff ts = wr \iff (t,w) \sim (r,s)$

(3) $(r,s) \sim (t,w)$, $(t,w) \sim (a,b) \iff rw = st$ and $tb = wa$. It follows

$$(rb)w = (rw)b = stb = swa = (sa)w$$

Then by cancellation

$$rb = sa \iff (r,s) \sim (a,b)$$

□

So we can define operations $+, \cdot$ as before,

$$r/s + t/w = (rw + st)/sw$$

$$(r/s)(t/w) = (rt)/(sw)$$

It is easy to see that $(Q(\mathcal{R}), +, \cdot)$ is ring, and $\mathcal{R}$ is isomorphic to a subring of $Q(\mathcal{R})$ via

$$\rho(r) = r/1$$

but by usual convention we just say $\mathcal{R}$ as a subring of $Q(\mathcal{R})$.

Example 79. $Q(\mathbb{Z}) = \mathbb{Q}$.

Example 80. F field, let $\mathcal{R} = F[x]$, then

$$Q(F[x]) = \{f(x)/g(x) : f, g \in F[x], g(x) \neq 0\}$$

hence we get a field of rational functions with coefficients in F. Notice unlike $F[x]$, at all r can be evaluated. So if $r \in F$, and $g(r) \neq 0$, then we can evaluate $f(x)/g(x)$ at r to get $f(r)/g(r)$.

Let's summarize:

For a finite ring, $\mathcal{R}$ (as we always assume ring is commutative with unity), then $\mathcal{R}$ is a field (cf theorem 73), so

$$Q(\mathcal{R}) = \mathcal{R}$$

For a infinite ring, $\mathcal{R}$, we have

$$\mathcal{R} \leq Q(\mathcal{R}) = \mathcal{R} \times (\mathcal{R} - \{0\}) / \sim$$

hence

$$Q(\mathcal{R}) \to \mathcal{R} \times (\mathcal{R} - \{0\})$$

is surjective, but a well known result says the cardinality of $\mathcal{R}$ is equal to card of $\mathcal{R} \times \mathcal{R}$, therefore

$$|\mathcal{R}| = |Q(\mathcal{R})|$$

in particular

$$|\mathbb{Q}| = |\mathbb{Z}|\,.$$

Other property we also touch on is that $Q(\mathcal{R})$ is the "smallest" way we can enlarge $\mathcal{R}$ to a field.

Let's summarize them in a theorem.

Proposition 81. *Let $\mathcal{R}$ be an integral domain and let*

$$f : \mathcal{R} \to F$$

be an injective homomorphism from $\mathcal{R}$ to a field F, then there exists a unique homomorphism

$$\tilde{f} : Q(\mathcal{R}) \to F$$

such that

$$\tilde{f}(r/1) = f(r)$$

moreover $\tilde{f}$ is injective, and if every element of F is of the form $f(r)/f(s)$ for $r, s \in \mathcal{R}$, $s \neq 0$, then

$$\tilde{f} : Q(\mathcal{R}) \cong F.$$

Pictorially

$$\begin{array}{ccc} \mathcal{R} & \stackrel{f}{\to} & F \\ \rho\downarrow & \nearrow_{\tilde{f}} & \\ Q(\mathcal{R}) & & \end{array}$$

Proof. If $\tilde{f} : Q(\mathcal{R}) \to F$ exists, it has to look like the following

$$\begin{aligned} \tilde{f}(r/s) &= \tilde{f}(r \cdot s^{-1}) \\ &= \tilde{f}(r)(\tilde{f}(s))^{-1} \\ &= \tilde{f}(r)/\tilde{f}(s) \\ &= f(r)/f(s) \end{aligned}$$

(it is common trick, to show unique before showing existence.)

So we define

$$\tilde{f}(r/s) = f(r)/f(s)$$

check this is well-defined. Want to show $r/s = t/w \iff rw = ts$, then

$$f(r)/f(s) = f(t)/f(w) \in F$$

If $s, w \neq 0$, then $f(s), f(w) \neq 0$ ($\because$ injectivity of f)

$$\begin{aligned} r/s = t/w &\iff rw = ts \\ &\iff f(rw) = f(ts) \\ &\iff f(r)f(w) = f(t)f(s) \end{aligned}$$

then

$$f(r)/f(s) = f(t)/f(w)$$

check $\tilde{f}$ is a homomorphism (hence preserves $+, \cdot$)

check $\tilde{f}$ is injective

$$\tilde{f}(r/1) = f(r)/f(1) = f(r)/1 = f(r)$$

check $\tilde{f}$ is surjective, if every element of F is of the form $f(r)/f(s)$, since $\tilde{f}(r/s) = f(r)/f(s)$.

Therefore

$$\tilde{f} \text{ is an isomomorphism.}$$

□

Let's two applications to this theorem.

Example 82. Let $\mathcal{R}$ be an integral domain, consider $\mathcal{R}[x]$. What is $Q(\mathcal{R}[x])$?

Claim 83. $Q(\mathcal{R}[x]) = Q(\mathcal{R})(x)$.

In the case $\mathcal{R} = \mathbb{Z}$, what is $Q(\mathbb{Z}[x]) = \mathbb{Q}(x)$.

Proof. Clearly

$$Q(\mathbb{Z}[x]) \subset \mathbb{Q}(x)$$

conversely given

$$\mathbb{Q}(x) \ni \frac{f(x)}{g(x)} = \frac{\sum a_i x^i}{\sum b_i x^i} \; a_i, b_i \in \mathbb{Q}$$

multiply a the common denominator (normally called clear the denominator) to get $a_i, b_i \in \mathbb{Z}$ so it is in $Q(\mathbb{Z}[x])$. □

Example 84. Prime fields.

Let F be a field, then

$$\text{char}F = 0 \text{ or } \text{char}F = p$$

We know $\exists$ homomorphism

$$f : \mathbb{Z} \to F$$

$$f(n) = n \cdot 1$$

(notation here $n \cdot 1$ meaning take $1 \in F$ and add 1 n times, $n > 0$. For $n < 0$, use -1.) Because

$$\text{char}F = 0 \iff f \text{ is injective}$$

then by the theorem, $\exists$ injective homomorphism

$$\tilde{f} : \mathbb{Q} \to F$$

$$\tilde{f}(n/m) = f(n)/f(m)$$

Moreover recall a subfield of F must contain 1, and $n1 \, \forall \, n \in \mathbb{Z}$,

$$n \cdot 1/m \cdot 1 = \text{image of } \tilde{f}$$

in other words, image of $\tilde{f}$, the smallest subfield of F, is a subfield isomorphic to $\mathbb{Q}$.

If $\text{char}F = p$, then $\langle 1 \rangle$ has order p. So

$$\langle 1 \rangle \cong \mathbb{Z}/p\mathbb{Z} \text{ or } \mathbb{F}_p$$

is a ring, since

$$(a1)(b1) = (ab)1 \implies$$

F contains a subfield $\cong \mathbb{F}_p$.

Definition 85. We say $\mathbb{Q}$, $\mathbb{F}_p$ are the prime fields in the sense that if $\text{char}F = 0$, F contains a subfield $\cong \mathbb{Q}$; if $\text{char}F = p$, F contains a subfield $\cong \mathbb{F}_p$.

Hence $\mathbb{Q}$, $\mathbb{F}_p$ are the smallest such subfields.

1.5 Ideals

Lecture 5 (2/6/13)

Last time, we constructed quotient to get a field. Today we want to make coset to be a field.

The general set up, $\mathcal{R}$ a ring (commutative with unity), H an additive subgroup of $\mathcal{R}$, i.e.

$$(H, +) \leq (\mathcal{R}, +)$$

Note 86. Recall from last semester, $\mathcal{R}|H = (r + H : r \in \mathcal{R})$, we'll never define coset using multiplication. never do

$$\mathcal{R}|H = (r \cdot H : r \in \mathcal{R}).$$

Since

$$H \triangleleft \mathcal{R}$$

$\mathcal{R}|H$ is an abelian group under coset addition.

Example 87. $\mathbb{Z}/n\mathbb{Z}$ set of cosets of nZ of $\mathbb{Z}$, one can check multiplication is well-defined, so $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ is a ring.

What about in general? What condition on H, turn $\mathcal{R}|H$ into a ring?

Given $r + h_1 \in r + H$, $r + h_2 \in r + H$, we want

$$(r + H) \cdot (s + H) = rs + H \tag{1.4}$$

(of course the product notion here doesn't mean component product (or Cartesian product), it means product of elements)

We need $\forall\, r, s \in \mathcal{R}$, $\forall\, h_1, h_2 \in H$, $\exists\, h_3 \in H$ s.t.

$$(r + h_1)(s + h_2) = rs + h_3$$

or

$$rh_2 + h_1 s + h_1 h_2 = h_3$$

If we take $h_1 = 0$, we want

$$rh_2 = h_3$$

The condition on H is thus

$$\forall\, r \in, \forall\, h \in H \quad rh \in H$$

One can check this condition is necessary and sufficient to make (1.4) well-defined.

Definition 88. A subset I of $\mathcal{R}$ is an ideal of $\mathcal{R}$ if

(1) I is an additive subgroup $(I,+) \leq (\mathcal{R},+)$ (2) $\forall\, r \in \mathcal{R}$, $\forall\, t \in I$ $rt \in I$

The second property is known as "absorbing property". The concept of ideal is analogy to normal subgroup.

We have proved the following

Proposition 89. *$\mathcal{R}$ ring I ideal, coset multiplication is well-defined on $\mathcal{R}/I$.*

Note 90. For a non-commutative ring, one can also define ideals, then there will be left ideals (absorbing multiplication from the left), right ideals, and 2-side ideals. Notice for coset multiplication to work, one has to have 2-side ideals. Also notice no all ring has 2-side ideals, e.g. matrices over $\mathbb{R}$.

We have the following.

Proposition 91. *$(\mathcal{R}/I,+,\cdot)$ is a ring (commutative with unity).*

Proof. $(\mathcal{R}/I,+)$ abelian group. Multiplication is associative

$$[(r+I)(s+I)](t+I) = (rs)t + I$$

$$(r+I)[(s+I)(t+I)] = r(st) + I$$

but

$$(rs)t = r(st)$$

in $\mathcal{R}$.

One can also check distribution, commutative, exists unity $(I+I)$. $\square$

Definition 92. Call $\mathcal{R}/I$ a *quotient ring*.

Some people call this factor ring, but we won't do that.

Consider

$$\pi : \mathcal{R} \to \mathcal{R}/I$$

$$r \mapsto r + I$$

and clearly π is a ring homomorphism, i.e.

$$\pi(r+s) = \pi(r) + \pi(s) \quad \because (r+s) + I = (r+I) + (s+I)$$

$$\pi(rs) = \pi(r)\pi(s) \quad \because rs + I = (r+I)(s+I)$$

$$\pi(1) = 1 + I = I$$

Example 93. (of trivial ideals) $\mathcal{R}$ any ring, $I = \mathcal{R}$ is an ideal, it is called "improper" or "unit" ideal. (later we will see why call it unit). Also $\{0\} \subset \mathcal{R}$ is an ideal, called zero ideal.

Example 94. $\mathcal{R} = \mathbb{Z}$, $I = n\mathbb{Z} = \langle n \rangle$, because $\forall\, a \in \mathbb{Z}$, $a \langle n \rangle$ is

$$a(kn) = (ak)n \in \langle n \rangle$$

This is a very special ideal. Almost no other ring has this kind of ideal. e.g. in $\mathbb{Z}[x]$, although $\mathbb{Z} \leq \mathbb{Z}[x]$, $\langle 1 \rangle = \mathbb{Z}$ is an ideal in $\mathbb{Z}$, it is not ideal in $\mathbb{Z}[x]$, but given $n \in \langle 1 \rangle$ and $f[x] \in \mathbb{Z}[x]$ s.t. $\deg f \geq 1$ then

$$nf \notin \langle 1 \rangle$$

Proposition 95. *Any ring $\mathcal{R}$, I an ideal, if $1 \in I$, then $I = \mathcal{R}$.*

More general if $\exists\, u \in I$ u is a unit, then $I = \mathcal{R}$.

Proof. $1 \in I$, $r \cdot 1 \in I$ so $I = \mathcal{R}$. $u \in I$, so $u^{-1}u = 1 \in I \implies I = \mathcal{R}$. □

That is reason we call $I = \mathcal{R}$ unit ideal.

Proposition 96. *F a field, I an ideal of F, then either $I = \{0\}$ or $I = F$.*

So field has no interesting ideals.

Proof. If $I = \{0\}$, done; otherwise $\exists\, r \in I$, $r \neq 0$, r is a unit, done. □

We know $\mathbb{R}$ has a lot of subgroup, e.g. $\langle 1 \rangle = \mathbb{Z}$, $\left\langle \sqrt{2} \right\rangle$, $\langle \pi \rangle$, $\langle 3/2 \rangle$, but none of them is an ideal.

Proposition 97. *I is an ideal $\iff$ $I \neq \varnothing$, closed under addition, $\forall\, r \in \mathcal{R}$ $\forall\, t \in I$ $rt \in I$.*

Proof. $\implies$ clear.

$\impliedby$ need to show I is an additive subgroup. We have for $t \in I$

$$0t = 0 \in I$$

given $s \in I$

$$(-1)s = -s \in I$$

□

Example 98. (of interesting ideal) In $\mathcal{R}_1 \times \mathcal{R}_2$

$$\{0\} \times \mathcal{R}_2 = \{(0, r) : r \in \mathcal{R}_2\}$$

$$\mathcal{R}_1 \times \{0\} = \{(r, 0) : r \in \mathcal{R}_1\}$$

both are ideals.

Unlike normal subgroup is a group, ideal is usually *not* a subring, because usually $1 \notin I$. Otherwise $I = \mathcal{R}$.

Recall normal subgroup is raised from kernel of some homomorphism. We have a similar result for ideals.

Proposition 99. *Let $\rho : \mathcal{R} \to \mathcal{S}$ be a ring homomorphism, then* $\ker \rho$ *is an ideal of $\mathcal{R}$.*

Proof. We know $\ker\rho$ is a subgroup of $\mathcal{R}$. check absorbing property, if $r \in \mathcal{R}$, $t \in \ker \rho$, then

$$\rho(t) = 0$$

so

$$\rho(rt) = \rho(r)\rho(t) = 0 \implies rt \in I$$

□

Use this proposition, we can find a lot of ideals.

Example 100. 1) $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $\ker \pi = n\mathbb{Z}$. 2) $\mathcal{R}_1 \times \mathcal{R}_2 \overset{\pi_1}{\to} \mathcal{R}_1$, $\ker \pi_1 = \{0\} \times \mathcal{R}_2$ 3) $ev_t : \mathcal{R}[x] \to \mathcal{R}$ or $ev_s : \mathcal{R}[x] \to \mathcal{S}$, $\mathcal{R} \leq \mathcal{S}$, $f(x) \in \ker ev_t \iff f(t) = 0$, $\forall\, g(x)$

$$ev_t(gf) = g(t)f(t) = 0 \implies gf \in I$$

Recall for group homomorphism, it's injective iff kernel is 0. Similarly

Note 101. If $\rho : \mathcal{R} \to \mathcal{S}$ is a ring homomorphism, then ρ is injective $\iff \ker \rho = \{0\}$.

Consider the following ring homomorphism

$$\pi : \mathcal{R} \to \mathcal{R}/I$$

then

$$\ker \pi = \pi^{-1}(0) = \{r \in \mathcal{R} : \pi(r) = 0 + I = I\}$$

This shows every ideal is the kernel of some homomorphism.

Now we give the ring version of fundamental homomorphism theorem:

Theorem 102. *(1st isomorphism theorem) Let $f : \mathcal{R} \to \mathcal{S}$ be a ring homomorphism, let $I = \ker f$, then*

$$Imf \cong \mathcal{R}/I$$

The last line gives an isomorphism between two rings. Pictorially the theorem says

$$\begin{array}{ccc} \mathcal{R} & \xrightarrow{f} & \mathcal{S} \\ \pi \downarrow & & \uparrow i \\ & \tilde{f} & \\ \mathcal{R}/I & \to & \mathrm{Im}f \\ & \cong & \end{array}$$

so $f = i \circ \tilde{f} \circ \pi$, where i is the inclusion, and $\tilde{f}(r + I) = f(r)$.

Proof. We already done most parts, only have to check that $\tilde{f}$ is a ring homomorphism (hence isomorphism)

$$\tilde{f}((r + I)(s + I)) = \tilde{f}(rs + I) = f(rs) = f(r)f(s) = \tilde{f}(r + I)\tilde{f}(s + I)$$

□

Corollary 103. *If $\exists$ surjective homomorphism $\mathcal{R} \to \mathcal{S}$ with kernel I, then*

$$\mathcal{R}/I \cong \mathcal{S}$$

Let's discuss interesting way to construct ideals.

Similarly to generator of a group

$$\langle g \rangle \leq G$$

Given $\mathcal{R}$ ring, $r \in \mathcal{R}$, define (r) *principal ideal* generated by r,

$$(r) = \{sr : s \in \mathcal{R}\}$$

i.e. (r) set of all multiples of r.

Proposition 104. *(r) is an ideal of $\mathcal{R}$, the smallest ideal of $\mathcal{R}$ containing r.*

"Smallest" means if I ideal, $r \in I$ then $(r) \subset I$.

Proof. check $(r) \neq \varnothing$ $(r = 1r)$, closed under addition,

$$(s_1 r) + (s_2 r) = (s_1 + s_2)r \in (r)$$

has absorbing property,

$$t(sr) = (ts)r \in (r).$$

I some ideal, $r \in I \ \forall\, s \in \mathcal{R}$

$$sr \in I \implies (r) \subset I$$

□

The use of ideal is to do factorization.

Example 105. Let $\mathcal{R} = F[x]$,

$0 \in \mathcal{R}$, principal ideal generated by 0,

$$(0) = \{0\}$$

$1 \in \mathcal{R}$

$$(1) = \mathcal{R}$$

u a unit

$$(u) = \mathcal{R}$$

$x \in \mathcal{R}$

$$\begin{aligned} (x) &= \text{all polynomials whose constant term is } 0 \\ &= \ker ev_0 \end{aligned}$$

$$(x - 1) = \ker ev_1$$

$$\begin{aligned} (x^2) &= \text{all polynomials with no const, or linear terms} \\ &= \{f(x) | f(0) = f'(0) = 0\} \end{aligned}$$

here we use the notion of derivative, of course it is true if $F = \mathbb{R}$, but it turns out one can define derivative for any $\mathcal{R}$, although the concept of limit may not be defined for those rings.

Lecture 6 (2/11/13)

More generally, given $r_1, ..., r_n \in \mathcal{R}$, we can definite ideal containing $r_1, ..., r_n$ as follows

Definition 106. $(r_1, ..., r_n)$ = ideal generated by $r_1, ..., r_n$ is

$$\{\sum s_i r_i : s_i \in \mathcal{R}\}$$

which is called a finitely generated ideal (not principal ideal).

It is easy exercise to check that $(r_1, ..., r_n)$ is an ideal, and in fact the smallest ideal.

Fact 107. *In $\mathbb{Z}$ every ideal is (n) for some n. Hence it is principal.*

Later we will show every ideal in $F[x]$ is principal, F a field. This will be very important to us.

Example 108. $F[x_1, x_2] \supset ker\, ev_{(0,0)}$, we know that

$$ev_{(0,0)} : F[x_1, x_2] \to F$$

ring homomorphism. Is $ker\, ev_{(0,0)}$ a principal ideal, i.e. $ker\, ev_{(0,0)} = (P[x_1, x_2])$?

ANS: No. Because $ker\, ev_{(0,0)} = x_1 P_1 + x_2 P_2$ for any polynomial P_1, P_2, i.e. $ker\, ev_{(0,0)} = (x_1, x_2) = ax_1 + bx_2$.

Example 109. In $\mathbb{Z}[x]$, consider this ideal

$$I = \{f(x) = \sum_{}^{n} a_i x^i : 2|a_0\}$$

easy to check I is an ideal. Let

$$\pi : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$$

then

$$ev\pi_0 : \mathbb{Z}[x] \to \mathbb{Z}/2\mathbb{Z}$$

so

$$ev\pi_0 f(x) = \pi(f(0)) = a_0 \text{ in } \mathbb{Z}/2\mathbb{Z}$$

So the I above is the kernel of $ev\pi_0$.

what the elements of I? we know $2 \in I$, $x \in I$, in fact

$$I = (2, x)$$

so not principal ideal.

Now instead do $\mathbb{Z} \leq \mathbb{Z}(\sqrt{2})$, let's consider

$$\mathbb{Z}[x]/(x^2-2)$$

where (x^2-1) is a principal ideal.

$$\mathbb{Z} \to \mathbb{Z}[x] \xrightarrow{\pi} \mathbb{Z}[x]/(x^2-2)$$

Suppose ρ maps $\mathbb{Z}$ to $\mathbb{Z}[x]/(x^2-2)$, with

$$\rho(n) = n + (x^2-1)$$

Check ρ is injective. If $n \in Ker\rho \implies n \in (x^2-1)f(x) \implies deg(x^2-2)f \geq 2 \implies f = 0 \implies n = 0$.

It infers that we can even view $\mathbb{Z}$ as a subring of $\mathbb{Z}[x]/(x^2-1)$, hence identify $n \in \mathbb{Z}$ with $n + (x^2-2)$

Claim 110. There exists an element in $\mathbb{Z}[x]/(x^2-2)$ which is a square root of 2.

Try

$$[x + (x^2-2)]^2 = x^2 + (x^2-2)$$

which is equal to 2.

Similar enlarge $\mathbb{R}$ to find element i with $i^2 = -1$ by taking

$$\mathbb{R}[x]/(x^2+1)$$

identify $t \in \mathbb{R}$ with $t + (x^2+1)$.

General idea: Enlarge $\mathcal{R}$ to where can solve algebraic equation

Proposition 111. *$\mathcal{R}$ any ring $f(x) \in \mathcal{R}[x]$*

$$\mathcal{R} \to \mathcal{R}[x] \xrightarrow{\pi} \mathcal{R}[x]/(f(x))$$

we get a homomorphism ρ from $\mathcal{R}$ to $\mathcal{R}[x]/(f(x))$. It is injective if $(f(x)) \cap \mathcal{R} = \{0\}$

That the last condition $(f(x)) \cap \mathcal{R} = \{0\}$ can be easily satisfied. if we work on integral domain.

Since every non-zero multiple of $f(x)$ has degree ≥ 1, here $\alpha = x+(f(x))$, so

$$f(\alpha) = f(x) + (f(x)) = 0 + (f(x))$$

But it is hard to know what $\mathcal{R}[x]/(f(x))$ looks like.

Now consider

$$\mathbb{R} \to \mathbb{R}[x]/(x^2-2)$$

know it is not integral domain since $(x^2-2) = (x+\sqrt{2})(x-\sqrt{2})$, in particular $x \pm \sqrt{2} \notin (x^2-2)$ ($\because$ it has lower degree)

$$[x+\sqrt{2}+(x^2-2)][x-\sqrt{2}+(x^2-2)] = 0+(x^2-2)$$

What we have done is a very common scheme in algebra. Whenever we cannot solve polynomial, we enlarge to a bigger field.

Recall in $\mathbb{Z}$ every ideal is (n), when is $\mathbb{Z}/n\mathbb{Z}$ an integral domain $\iff$ $n = p$, in this case $\mathbb{Z}/p\mathbb{Z}$ is a field.

We also know $\mathbb{Z}/(0) \cong \mathbb{Z}$ because $n+(0) = m+(0) \implies n = m$.

Definition 112. An ideal I is call prime ideal if 1) $I \neq \mathcal{R}$ 2) $\forall\, r, s \in \mathcal{R}$, if $rs \in I$, then either $r \in I$ or $s \in I$, or equivalently if $r \notin I$, $s \notin I$, then $rs \notin I$.

The first condition $I \neq \mathcal{R}$ has some meaning as we don't say 1 is a prime number.

Example 113. If $\mathcal{R} = \mathbb{Z}$, $I = (n)$, $n > 0$, we know $a \in (n) \iff n|a$, therefore (n) is a prime ideal $\iff n \neq 1$, and we need $n|ab$ then $n|a$ or $n|b$, therefore n has to be a prime.

Note: $(0) \subset \mathbb{Z}$ is also a prime ideal. In fact in any ring, $\mathcal{R}$ is integral domain $\iff$ (0) is a prime ideal. This is equivalent to say if $rs = 0$ then either $r = 0$ or $s = 0$.

Proposition 114. *In a ring $\mathcal{R}$, I is a prime ideal $\iff$ $\mathcal{R}/I$ is an integral domain.*

Proof. $\mathcal{R}/I \neq \{0\} \iff I \neq \mathcal{R}$ and $\mathcal{R}/I$ is an integral domain $\iff$ if $r+I \neq 0$, $s+I \neq 0$, then $(r+I)(s+I) = rs+I \neq 0$, which is saying $r \notin I$, $s \notin I$, then $rs \notin I$. □

Definition 115. I is a maximal ideal if 1) $I \neq \mathcal{R}$, 2) if J is an ideal of $\mathcal{R}$, $I \subset J \subset \mathcal{R}$, then either $I = J$ or $J = \mathcal{R}$.

Example 116. In $\mathbb{Z}$, $(p) \subset \mathbb{Z}$, p prime.

If $(p) \subset (n) \implies p \in (p) \subset (n) \implies n|p \implies$ either $n = \pm 1 \implies (n) = \mathbb{Z}$ or $n = \pm p \implies (n) = (p)$, so (p) is maximal.

Clearly (0) is maximal, (although it is prime ideal).

If n not prime, say $n = ab$, $a, b > 1$, then $(n) \subset (a)$, and $(n) \subset (b)$, so (n) is not prime, not maximal ideals.

Now we come to the important theorem.

Theorem 117. *I is a maximal ideal $\iff$ $\mathcal{R}/I$ is a field.*

Corollary 118. *I is maximal $\implies$ I is prime ideal.*

The proof of the corollary relays on a simple fact that field $\implies$ integral domain.

Proof. $I \neq \mathcal{R} \iff \mathcal{R}/I \neq \{0\}$

($\implies$) suppose I is maximal, to show $\mathcal{R}/I$ is a field, that is to show if $r + I \neq 0 + I$, $r + I$ has a multiplicative inverse in $\mathcal{R}/I$.

Assume $r \notin I \iff r + I \neq 0 + I$, enlarge I to an ideal J

$$J = \{rs + t : s \in \mathcal{R}, r \in I\}$$

Claim: J is an ideal of $\mathcal{R}$ with $I \subset J$.

Proof of claim: $I \subset J$ since $\forall\, t \in I$, $t = 0r + t \in J \implies J \neq \varnothing$

$$(s_1 r + t_1) + (s_2 r + t_2) = (s_1 + s_2)r + (t_1 + t_2) \in J$$

$\forall\, w \in \mathcal{R}$, $\forall\, w(sr + t) = wsr + wt \in J$, note $J \neq I$ since $r \in J$, $r = 1r + 0$ but $r \notin I \in J = \mathcal{R}$.

So $1 \in J \implies 1 = sr + t$, $t \in I \implies (s + I)(r + I) = sr + I$, $1 \in sr + I \implies sr + I = 1 + I$, we found multiplicative inverse $\mathcal{R}/I$ is a field.

Lecture 7 (2/13/13)

($\impliedby$) Suppose $\mathcal{R}/I$ is a field to show I is maximal is to show $I \neq \mathcal{R}$ since $\mathcal{R}/I = \{0\}$. suppose J an ideal $J \supset I$ and $J \neq I$ must show $J = \mathcal{R} \iff 1 \in J$

suppose $\exists\, r \in J$, $r \notin I \implies r + I \in \mathcal{R}/I$ is not $0 + I$ $(r + I)(s + I) = 1 + I \implies rs = i + t$, $t \in I$. Since J is ideal, $r \in J \implies rs \in J \implies rs - t \in J$. □

Example 119. $\mathcal{R}$ any ring $a \in \mathcal{R}$

$$ev_a : \mathcal{R}[x] \to \mathcal{R}$$

since if $r \in \mathcal{R} \subset \mathcal{R}[x]$

$$ev_a(r) = r \implies ev_a \text{ is surjective}$$

Claim: $kerev_a = (x-a)$ i.e. $f(a) = 0 \iff f(x) = (x-a)g(x)$ some $g(x)$

More generally every $f(x) \in \mathcal{R}[x]$

$$f(x) = \sum_{i=0}^{n} a_i x^i = \sum_{i=0}^{n} b_i (x-a)^i = b_0 + (x-a)g(x)$$

since we can write

$$x^i = (x-a+b)^i = \sum \begin{pmatrix} i \\ k \end{pmatrix} (x-a)^k a^{j-k}$$

$$0 = f(x) \iff f(x) = (x-a)g(x)$$

i.e.

$$f(x) \in (x-a)$$

where $(x-a)$ is a principal ideal.

Let's summarize by 1st fundamental theorem

$$\mathcal{R}[x]/kerev_a \cong Imev_a = \mathcal{R} \implies \mathcal{R}[x]/(x-a) \cong \mathcal{R}$$

If $\mathcal{R}$ is a field F

$$F[x]/(x-a) \cong F \implies (x-a) \text{ is maximal in } F[x]$$

It turns out $F[x]$ this ring has many maximal ideals.

We also saw R an integral domain $\implies (x-a)$ is a prime ideal; R field $\implies (x-a)$ maximal ideal.

Example 120. In $\mathbb{Z}[x]$, (x) prime not maximal, $\mathbb{Z}$ an integral domain not a field,

$$\mathbb{Z}[x]/(x) \cong \mathbb{Z}$$

Example 121. $F[x_1, x_2] = F[x_1][x_2]$, set $x_2 = 0$

$$ev_{(x_1,0)} : F[x_1, x_2] \to F[x_1]$$

which is kernel $= (x_2)$, is prime not maximal.

$(x_2) \subset (x_1, x_2) = kerev_{(0,0)}$ is maximal, this is all polynomial in x_1,x_2 with constant term 0.

2 Factorization

Now we back to 1 variable, we now study factorization in $F[x]$, F is always going to be a field.

2.1 Long Division with Remainder

Theorem 122. *Let $f(x) \in F[x]$, $f(y) \neq 0$, let $g(x) \in F[x]$, then $\exists !$ $q(x), r(x) \in F[x]$ such that*

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

where either $r(x) = 0$ or $degr < degf$.

The proof is quite algorithmic.

Proof. (existence) By induction on deg$g(x)$ if $g = 0$ or $degg < degf$, stop, put $q = 0$ or $r = g$.

$$f(x) = \sum_{i=0}^{n} a_i x^i$$

$f = 0$ $n = degf$ $a_n \neq 0$, and

$$g(x) = \sum_{j}^{m} b_j x^j$$

$degg \geq degf \implies m \geq n$, then

$$g(x) - f(x)a_n^{-1}b_m x^{m-n}$$

has smaller degree (notice this is only place we use the property of F, so we have a_n^{-1}). By reduction

$$g(x) - f(x)a_n^{-1}b_m x^{m-n} = f(x)q_1(x) + r(x)$$

so

$$g(x) = f(x)(a_n^{-1}b_m x^{m-n} + q_1(x)) + r(x)$$

Now prove uniqueness

suppose

$$g(x) = f(x)q_1(x) + r_1 = f(x)q_2(x) + r(x)$$

where wither $r_i = 0$ or $\deg r_i < f$ to show $q_1 = q_2$ and $r_1 = r_2$

$$\begin{aligned} fq_1 + r_1 &= fq_2 + r_2 \\ f(q_1 - q_2) &= r_2 - r_1 \end{aligned}$$

If $q_1 - q_2 \neq 0 \implies f(q_1 - q_2) \neq 0 \; degf(q_1 - q_2) \geq degf \implies r_2 - r_1 \neq 0$, but $\deg(r_2 - r_1) \leq max(r_1, r_2) < degf$

contradiction: it must be that $q_1 - q_2 = 0 \implies f(0) = 0 \implies r_1 = r_2$. □

Fact 123. *$\mathcal{R}$ any ring, but $f(x)$ monic, some conclusion of long division with remainder valid.*

Corollary 124. *Let $f(x) \in F[x]$ $f(x) \neq 0$ then every coset in $F[x]/(f(x))$ has unique representation $r(x)$ where either $r(x) = 0$ $degr(x) < degf(x)$.*

Proof. a coset of $(f(x)) = g(x) + (f(x))$ element of this coset $= g(x) + f(x)h(x)$ in the statement of long division take $h(x) = -q(x)$

$$g(x) - f(x)g(x) = r(x)$$

Show existence $\exists\, r(x) \in g(x) + (f(x))$ s.t. $r(x) = 0$ or $degr(x) < degf(x)$

uniqueness same argument as uniqueness in long division. □

We have seen $F[x]/(f(x))$ gives a coset $g(x) + (f(x))$ $\deg f = n > 0$, one can find $r(x) deg < n$

$$r(x) = c_0 + c_1 x + ... + c_{n-1} x^{n-1}$$

Let $\alpha = x + (f(x))$

$$r(x) + (f(x)) = c_0 + c_1 \alpha + ... + c_{n-1} \alpha^{n-1}$$

for unique c_0,..., $c_{n-1} \in F$

Example 125. $F = \mathbb{R}$ $f(x) = x^2 + 1$

$$\mathbb{R}[x]/(x^2 + 1)$$

$\alpha = x + (x^2 + 1)$, every coset is uniquely of the form $a + b\alpha$

$$(a + b\alpha)(c + d\alpha) = (a + c) + (b + d)\alpha$$

we don't show this is a field, we will do that later in a more general context

Corollary 126. *If* $a \in F \ \forall\, g(x) \in F[x]$

$$g(x) = (x-a)q(x) + g(a)$$

Proof. (a new proof use long division)

By long division

$$g(x) = (x-a)f(x) + r(x)$$

wither $r(x) = 0$ or $degr < 1 \iff r = c \in F$, so

$$g(x) = (x-a)q(x) + c$$

where $c = g(a)$. □

We see a is a root or zero of $g(x) \iff x - a$ is a factor i.e. $kerev_a = (x-a)$

Corollary 127. *$f(x) \in F[x]$, $f(x) \neq 0$ $degf = n$ then $f(x)$ has at most n discrete roots in F (or in any field containing F)*

Proof. If f has no roots, $n = 0$, we're done.

By induction in deg$f$, suppose $f(x)$ has a root $a_1 \implies (x-a_1)|f(x) \implies f(x) = (x-a_1)g(x)$ deg$g = n-1$

suppose $a_2 \neq a_1$ is another root $f(x)$

$$f(a_2) = (a_2 - a_1)g(a_2) \implies g(a_2) = 0$$

roots of $f(x)$ not equal to a_1 = roots of $g(x) \neq a_1$

By induction $g(x)$ has at most $n-1$ roots $\implies$ $f(x)$ has at most n roots. □

Remark 128. If we replace F by an arbitrary ring $\mathcal{R}$ or a division ring (e.g. $\mathbb{H}$) $f(x)$ can have infinitely many roots in $\mathbb{Z}$ or $\mathbb{Z}[x]$ If $\mathcal{R}$ is a integral domain, $f(x) \in \mathcal{R}[x]$ with degree $n \implies f(x)$ has at most n roots.

Lecture 8 (2/18/13)

Theorem 129. *(existence of primitive root) Let F field, suppose G is a finite subgroup of $(F^*, \cdot)$ then G is cyclic.*

Example 130. $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \implies (\mathbb{Z}/p\mathbb{Z})^*$ is cyclic

Example 131. $\mathbb{F} = \mathbb{C}$ $\left\langle e^{2\pi i/n} \right\rangle = \{z \in \mathbb{C} : z^n = 1\} = (C^*, \cdot)$

Proof. Let $n = |G|$, Look at for each $d|n$, the set of root in F or G of $x^d - 1$, gives

$$\{a \in G : a^d - 1\} \subset \{a \in F : a^d - 1\}$$

By corollary 127, $|\{a \in G : a^d - 1\}| \leq d$, then by the following thereon 132 gives the result. □

Theorem 132. *Let G be a finite group of $|G| = n$, suppose for each $d|n$,*

$$|\{a \in G : a^d - 1\}| \leq d$$

then G is cyclic.

Proof. Let $\varphi =$ Euler φ-function, namely

$$\varphi(k) = |(\mathbb{Z}/k\mathbb{Z})^*| = \text{number of generators of } \mathbb{Z}/k\mathbb{Z}$$

Basic identity

$$\sum_{d|n} \varphi(d) = n$$

Define $\phi(d)$ for each $d|n$ as follows $\phi(d) =$ number of elements of G of order exactly d.

$$\sum_{d|n} \phi(d) = |G|$$

Claim: $\phi(d) \leq \varphi(d)$.

Proof of claim: 2 cases: if there is no element of order $d \implies \phi(d) = 0 \leq \varphi(d)$. If there is an element of order d

$$|\langle g \rangle| = d$$

any element $a \in \langle g \rangle$ satisfies $a^d = 1$. Since $|\{a : a^d = 1\}| \leq d$, $|\langle g \rangle| \subset \{a : a^d = 1\} \implies \{a : a^d = 1\} = \langle g \rangle$, in case 2

$$\phi(d) = \varphi(d).$$

Now $\sum_{d|n} \phi(d) = |G| = n = \sum_{d|n} \varphi(d)$ only possible if $\forall\, d|n\ \phi(d) = \varphi(d)$.

Take $d = n \implies \phi(n) = \varphi(n) \neq 0 \implies$ there exists at least one element of G of order $n \implies G$ is cyclic. □

Back to factorization in $F[x]$

Theorem 133. *Let I be an ideal in $F[x]$, then I is a principal ideal.*

Proof. Let I be an ideal, if $I = \{0\} = (0)$ we are done. so assume I is not $\{0\}$. then $\exists\, f(x) \in I,\ f \neq 0 \implies \deg f$ is defined (could be 0). By well ordering principle, there exists an $f \in I$ s.t. $\deg f$ is smallest possible degree among degrees of elements of I. i.e. $\forall\, g \in I$, $g \neq 0 \implies deg f \leq deg g$. Then claim $I = (f)$.

Let $g \in I$ to show $g \in (f)$, apply long division

$$g = fq + r$$

where $r = 0$ or $\deg r < \deg f$. Assume $r \neq 0 \implies r = g - fq$, know $g \in I$ $f \in I \implies fg \in I$, so $r \in I$ and $\deg r < \deg f$, which contradicts smallest possible degree. Conclusion $r = 0$, or $g = fq \in (f)$.

Conversely since $f \in I$. $\forall\, q \in F[x]$. $fq \in I \implies (f) \subset I \implies I = (f)$. □

Note 134. This fails for $F[x_1, x_2]$ or $\mathbb{Z}[x]$.

Definition 135. Given $f, g \in F[x]$, we say $f|g$ (f divides g) iff $\exists\, h \in F[x]$ s.t. $g = fh$.

Note 136. If $g = 0$, $\forall\, f|0$. But $f = 0$ only divides 0.

Definition 137. Given $f, g \in F[x]$, not both 0, then a *gcd* of f, g is a $d \in F[x]$ s.t.

(1) $d|f$, $d|g$ (2) If $e|f$, $e|g \implies e|d$, write $d = gcd(f, g)$.

Remark 138. These definitions are same words to words with factorization of $\mathbb{Z}$.

(1) *gcd* is never 0, because at least one of f, g is not 0

(2) If d_1,d_2 are two *gcd* of f, g, then $\exists\, c \in F^*$ s.t. $d_1 = cd_2$. So d could be unique if we require d to be monic, but such definition is not so natural, we'll not follow it.

Proof. (of remark 2) Suppose d_1,d_2 are two *gcd* of $f, g \implies d_1|d_2$, $d_2|d_1$ say $d_2 = ud_1$ and $d_1 = vd_2 \implies d_1 = (uv)d_1$, since $d_1 \neq 0 \implies 1 = uv \implies u, v \in F^*$ □

So *gcd* is not quite unique but all almost, so we've proven unique, now prove *gcd* exists. Exactly as for $\mathbb{Z}$.

Theorem 139. *Let $f, g \in F[x]$ not both 0, then a gcd of f, g exists, is unique up to a multiplying by $c \in F^*$ and $d = rf + sg$ for some $r, s \in F[x]$.*

Proof. Consider $I = \{rf + sg : r, s \in F[x]\}$. Claim: I is an ideal in $F[x]$, in fact $I = (f, g) = (f) + (g)$, which is proved in the hw.

$f = 1f + 0g \in I$, so is $g \in I$, know I is principal, say $I = (d)$, then $f \in I = (d) \implies d|f$, so is $d|g$.

Say $e|f$ and $e|g$, then by easy calculation $e|rf+sg$ for any $r, s \in F[x] \implies e|d$. □

Definition 140. $f, g \in F[x]$ are relatively prime if a *gcd* of f, g is 1 $\iff \exists r, s \in F[x]$ s.t. $1 = rf + sg$.

Corollary 141. *If f, g are relatively prime and $f|gh$ then $f|h$.*

Proof. Write $1 = rf + sg$ multiplied by h

$$h = rhf + sgh$$

$f|(rh)f$, $f|gh \implies f|s(gh) \implies f|rhf + sgh = h$. □

2.2 Irreducibility

Lecture 9 (2/25/13)

Definition 142. a polynomial $p(x) = p \in F[x]$ is irreducible if $\deg p > 0$ (i.e. p is not 0 or a unit, which is the same in $\mathbb{Z}$, we say 1 is not a prime) and if $p = fg$, then one of f, g is unit $c \in F*$ then the other is $c^{-1}p$.

Equivalently p is irreducible if it doesn't factor as a product of 2 polynomial of strictly smaller degree.

Example 143. Any linear polynomial $x + a$ is irreducible.

Example 144. Quadratic polynomial is reducible $\iff$ it has 2 linear factors $\iff$ it has a root.

Example 145. Cubit polynomial is reducible $\iff$ it has a root, because its degree either $2 + 1$ or $1 + 1 + 1$

Note 146. For higher polynomials such analogous statement is not true. One can have a reducible polynomial with no roots.

Example 147. $x^2-2 \in \mathbb{Q}[x]$ is irreducible, but $x^2-2 \in \mathbb{R}[x]$ is reducible.

Example 148. $x^4 - 4 \in \mathbb{Q}[x]$ is reducible but no roots.

Since irreducibility is a basic toward factorization, but in general whether $f(x) \in \mathbb{Q}[x]$ is irreducible is a hard problem.

Note 149. If p irreducible and f anything in $F[x]$, either $p|f$ or p, f are relative prime.

Proof. $d = gcd(p, f)$, $d|p \implies$ either d a unit $\implies$ p, f relative prime; or $d = cp$, $c \in F^*$ so may just assume $d = p \implies p|f$. □

Corollary 150. *If $p \in F[x]$ is reducible and $p|fg \implies$ either $p|f$ or $p|g$.*

Proof. If $p|f$ done, otherwise by noting p, f are relatively prime, so $p|g$. □

We are now ready to show uniqueness factorization of polynomial

Theorem 151. *Let $f(x) \in F[x]$, $degf > 0$ then $\exists\, p_1, ..., p_k$ irreducible in $F[x]$ s.t.*

$$f = p_1 ... p_k$$

If also $f = q_1 ... q_l$, irreducible, then $k = l$, after reordering $\exists\, c_i \in F^*$ s.t. $q_i = c_i p_i$.

Proof. Existence can be done by complete induction on $\deg f$. $\deg f = 1 \implies f$ irreducible, done.

Otherwise assume okay for all degree $< n$, show it is true for n

$$\deg f = n,\ f \text{ irreducible} \implies \text{done}$$

otherwise $f = g_1 g_2$ with $\deg g_i < n$, $i = 1, 2$.

By induction hypothesis each g_i is a product of irreducible $\implies$ so is $f = g_1 g_2 \implies$ we showed existence.

Uniqueness is the interesting part.

Suppose $f = p_1 ... p_k = q_1 ... q_l$, p_i,q_i are irreducible. Argue by induction on k, if $k = 1$

$$p_1 = q_1 ... q_l \implies p_1 | q_1 ... q_l$$

by induction starting $l = 2$ $p_1 | q_i$ for some i, q_i irreducible, $p_1 \neq constant \implies$ $p_1 = cq_i$ after reordering one can assume $i = 1$, so

$$p_1 = cq_1 = q_1 q_2 ... q_l \implies c = q_2 ... q_l$$

we canceling q_1 because $F[x]$ is integral domain. But $\deg q_2...q_l > 0$ impossible $\implies l = 1$, $p_1 = q_1$

General case

$$p_1...p_k = q_1...q_l \implies p_1 | q_1...q_l$$

implies $\exists\, i\ p_1|q_i \implies p_1 = cq_i$ reorder so that $i = 1$

$$(cq_1)p_2...p_k = q_1...q_l$$

so $cp_2...p_k = q_2...q_l$ has $(k-1)$ factors. By induction $k-1 = l-1 \implies l = k$. After reordering $p_i = c_i q_i$, $i = 1, ..., k$. □

Theorem 152. *Let F be field, Let I be an ideal in $F[x]$ then the following are equivalent*

(1) I is a maximal ideal; (2) I is a prime ideal and $I \neq \{0\}$; (3) $I = (p)$ where p is irreducible.

Proof. (1) $\implies$ (2) say I is maximal so I is prime and $I \neq \{0\}$ because $F[x]$ not a field.

(2) $\implies$ (3) suppose I is a prime ideal, $I \neq \{0\}$ know $I = (p)$ for some polynomial p, to show p irreducible, we know $p \neq$ a unit ($\because$ if p is a unit, $(p) = F[x]$ but prime ideal is not $F[x]$. That is the reason when we define prime ideal we excluded the case) we also know $p \neq 0$ (if $p = 0$, then $(p) = (0) = I$ but $I \neq (0)$)

To show if $p = fg$ then one of f, g is a unit and the other is unit times p.

$p = fg \implies fg \in (p) = I \implies$ either $f \in I$ or $g \in I$. Say $f \in (p) \implies f = hp$ Since $p = fg = hgp \implies hg = 1 \implies h, g$ are unit so $f =$ unit times p so p is irreducible.

(3) $\implies$ (1) Must show if p is irreducible then (p) is a maximal ideal

Must show if $(p) \subset J$ then either $J = (p)$ or $J = F[x]$. $(1) \neq F[x]$ since $\deg p \geq 1$. Know $\exists\, f$ such that $J = (f)$ $p \in (p) \subset J = (f) \implies p$ is a multiple of f, say $p = fg$. 2 possibilities:

1) f is a unit, then $J = (f) = F[x]$. since J contains a unit.

2) $f = cp_1$, c nonzero constant $(p) \subset (f) = (cp) \subset (p)$, so $(p) = (f) = J$, so (p) is a maximal ideal. □

Applications to the theorem

$$F[x]/(f) \text{ is a field} \iff f \text{ is irreducible}$$

Example 153. $\mathbb{Q}[x]/(x^2-2)$ elements look like $c_0 + c_1\alpha$, α =coset $x + (x^2-2)$, $\alpha^2 = \sqrt{2}$.

Example 154. $\mathbb{R}[x]/(x^2+1)$ elements look like $c_0+c_1\alpha$, $\alpha^2 = 1$, $c_0, c_1 \in \mathbb{R}$

Example 155. $\mathbb{Q}[x]/(x^3-2)$ elements are $c_0+c_1\alpha+c_2\alpha^2$, $c_0, c_1, c_2 \in \mathbb{Q}$ $\alpha = x + (x^3-2)$, $\alpha^2, \alpha^3 = 2$.

We now learn today this is a field, although this is not so easy to write out the multiplicative inverse, nevertheless we know they exist.

Now think about examples in $\mathbb{F}_2[x]$

Example 156. $x^2+x+1 \in \mathbb{F}_2[x]$ neither 0 nor 1 is a root, then x^2+x+1 is irreducible, then we will make

$$\mathbb{F}_2/(x^2+x+1) \equiv E$$

elements are $c_0+c_1\alpha$, $c_0, c_1 \in \mathbb{F}_2$, $\alpha = x+(x^2+x+1)$, $\alpha^2 = -\alpha-1 = \alpha+1$. E is a new field with 4 elements.

Lecture 10 (2/27/13)

We have shown

$$F[x]/(f) \text{ is a field} \iff I \text{ is maximal ideal} \iff f \text{ is irreducible}$$

Given $f(x) \in F[x]$ want to find a root of $f(x)$

Lecture 11 (3/4/13)

Lecture 12 (3/6/13)

Lecture 13 (3/11/13)

Lecture 14 (3/13/13)

Lecture 15 (3/25/13)

Lecture 16 (3/27/13)

Lecture 17 (4/1/13)

Lecture 18 (4/8/13)

Lecture 19 (4/10/13)

Lecture 20 (4/15/13)

Lecture 21 (4/17/13)

Lecture 22 (4/22/13)