Ring and Field theory PART-1

LECTURE 1

* A ring $(R,+,\cdot)$ is a set R with two binary operations: $+$ (addition) and $\cdot$ (multiplication) such that the following heads:

  (i) $(R,+)$ is an abelian group

  (ii) (Associative) $\forall a,b,c \in R$, $a\cdot(b\cdot c) = (a\cdot b)\cdot c$

  (iii) (Distributive) $\forall a,b,c \in R$, $a\cdot(b+c) = a\cdot b + a\cdot c$ and $(b+c)\cdot a = b\cdot a + c\cdot a$

* We say R is a unital ring if there is $1 \in R$ such that $1\cdot a = a\cdot 1$ $\forall a \in R$.

* We say R is a commutative ring if $a\cdot b = b\cdot a$ $\forall a,b \in R$

* • $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are rings
  • $\mathbb{Z}_{\geq 0}$ is not ring
  • $2\mathbb{Z}$ is commutative ring but not unital
  • $M_n(\mathbb{R})$ is unital but not commutative $(n>1)$

If R is unital then so is $M_n(R)$

proof: Consider $\begin{pmatrix} 1_R & & 0 \\ & \ddots & \\ 0 & & 1_R \end{pmatrix}$ ■

If $M_n(R)$ is unital then R is unital

proof: Let I be the identity. Then for $x \in R$, set M_x the matrix with $(1,1)$ being x.

So $M_x I = M_x$ and $IM_x = M_x$. Denote e in $(1,1)$ coefficient of I. We get $ex = xe = x$. ■

* • The set $\mathbb{Z}_n$ of integers modulo n is a ring
  • $R[x] = \{ a_n x^n + \cdots + a_0 \mid n \in \mathbb{Z}^{\geq 0}, a_0, \ldots, a_n \in R \}$ is a ring

Compute $([3]_4 x + [1]_4)([2]_4 x^2 + [3]_4 x + [1]_4)$ in $\mathbb{Z}_4[x]$

Solution: $([3]_4 x + [1]_4)([2]_4 x^2 + [3]_4 x + [1]_4)$

$= [2\cdot 3]_4 x^2 + [2\cdot 1]_4 x + [1\cdot 2]_4 x^2 + [1\cdot 3]_4 x + [1\cdot 1]_4$

$= [2]_4 x^2 + [2]_4 x + [2]_4 x^2 + [3]_4 x + [1]_4$

$= [2+2]_4 x^2 + [2+3]_4 x + [1]_4$

$= [1]_4 x + [1]_4$

$= x+1 \rightarrow$ for simplicity

Compute $(x+1)^3$ in $\mathbb{Z}_3[x]$

solution: $(x+1)^3 = x^3 + 1 + 3x(x+1) \equiv x^3 + 1$

Suppose p is prime. Compute $(x+1)^p$ in $\mathbb{Z}_p[x]$

solution: $(x+1)^p = x^p + \binom{p}{1} x^{p-1} + \cdots + 1^p = x^p + 1$ as $p \mid \binom{p}{i}$ $\forall\ 1 \le i \le p-1$.

* Here polynomials are also defined as $\Sigma_{i=0}^{\infty} a_i x^i$. Two polynomials are equal only if coefficient are same.

* The direct product of rings R_i:

$R_1 \times \cdots \times R_n := \{(r_1, \dots, r_n) \mid r_1 \in R_1, \dots, r_n \in R_n\}$

with operations

$(r_1, \dots, r_n) + (r_1', \dots, r_n') := (r_1 + r_1', \dots, r_n + r_n')$

$(r_1, \dots, r_n) \cdot (r_1', \dots, r_n') = (r_1 \cdot r_1', \dots, r_n \cdot r_n')$

Compute $(2,2)\cdot(3,3)$ in $\mathbb{Z}_5 \times \mathbb{Z}_6$

Solution: $(2\cdot 3, 2\cdot 3) = (1,0)$

Suppose R is a ring and 0 is the neutral element of the abelian group $(R,+)$. Then $\forall\ a,b \in R$, the following hold:

1) $0\cdot a = a\cdot 0 = 0$

2) $(-a)\cdot b = -(a\cdot b) = a\cdot(-b)$

3) $(-a)\cdot(-b) = a\cdot b$

proof: (1) Since $0 = 0+0$, we have $0 \cdot a = (0+0) \cdot a \ \forall a \in R$

$$0 \cdot a = (0 \cdot a) + (0 \cdot a) \Rightarrow 0 = 0 \cdot a \ \blacksquare$$

(2) Note that $a \cdot b + (-a) \cdot b = (a + (-a)) \cdot b = 0 \cdot b = 0 \Rightarrow (-a) \cdot b = -(a \cdot b)$

(3) $(-a) \cdot (-b) = -(a \cdot (-b)) = -(-(a \cdot b)) = a \cdot b \ \blacksquare$

* Suppose R is a unital ring. Then there is a unique $1_R \in R$ such that

$$1_R \cdot a = a \cdot 1_R = a$$

proof: suppose both 1 & $1'$ satisfy $1 = 1 \cdot 1' = 1'$ $\blacksquare$

♥ Whenever we learn a new structure, you should look for subsets that share the same properties & maps that preserves those

* Suppose $(R, +, \cdot)$ is a ring. A subset S of R is called subring of R if

1. $(S, +)$ is a subgroup of $(R, +)$
2. S is closed under multiplication. This means that for every $a, b \in S$, we have $ab \in S$.

* $\mathbb{Z}$ is a subring of $\mathbb{Q}$. $\mathbb{Q}$ is subring of $\mathbb{R}$. $\mathbb{R}$ is subring of $\mathbb{C}$.

* 1. What is the smallest subring of $\mathbb{C}$ that contain $\mathbb{Q}$ and i?
2. What is the smallest subring of $\mathbb{C}$ that contains $\mathbb{Q}$ and $\sqrt{2}$?
3. What is the smallest subring of $\mathbb{C}$ that contains $\mathbb{Q}$ and $\sqrt[3]{2}$?

solution: 1. $\mathbb{Q}[i]$

2. $\mathbb{Q}[\sqrt{2}]$

3. $\mathbb{Q}[\sqrt[3]{2}, \sqrt[3]{4}]$

* Suppose R_1 & R_2 are two ring. Then a function $f: R_1 \to R_2$ is called ring homomorphism $\forall a, b \in R$:

1. $f(a+b) = f(a) + f(b)$ Additionally, $f(1_{R_1}) = 1_{R_2}$
2. $f(a \cdot b) = f(a) \cdot f(b)$

* For every positive integer n, $c_n: \mathbb{Z} \to \mathbb{Z}_n$, $c_n(a) := [a]_n$ is a ring homomorphism.

LECTURE 2

Suppose $f: R_1 \to R_2$ is a bijective ring homorphism. Then $f^{-1}: R_2 \to R_1$ is a ring homorphism.

proof: Since f is bijection, it is invertible and there is the function $f^{-1}: R_2 \to R_1$.

$$f(f^{-1}(a)) + f^{-1}(b)) = f(f^{-1}(a)) + f(f^{-1}(b)) = a+b = f(f^{-1}(a+b))$$

$$\Rightarrow f^{-1}(a) + f^{-1}(b) = f^{-1}(a+b) \quad \text{(by injectivity)}$$

Similarly, $f(f^{-1}(a \cdot b)) = a \cdot b = f(f^{-1}(a)) \cdot f(f^{-1}(b)) = f(f^{-1}(a) \cdot f^{-1}(b))$

$\Rightarrow f^{-1}(a \cdot b) = f^{-1}(a) \cdot f^{-1}(b)$ by injectivity ∎

* A bijective ring homorphism is called ring isomorphism. We say two ring are isomorphic, if there is a ring isomorphism between them.

* Subgroup criterion: Suppose $(G, \cdot)$ is a group and H is a non-empty subset. If for every $h, h' \in H$, $hh'^{-1} \in H$, then H is a subgroup.

* Subring criterion: Suppose R is a ring and S is a non-empty subset of R. If for every $a, b \in S$, we have

1. $a - b \in S$
2. $a \cdot b \in S$

then S is a subring

proof: By subgroup criterion, by 1) we deduce that $(S,+)$ is a subgroup of $(R,+)$. Since S is also closed under multiplication, we get S is subring ∎

* • Kernel of group homorphism f between two abelian groups A_1 & A_2 is $\ker f := \{a \in A_1 \mid f(a_1) = 0\}$, $\ker f \leq A_1$.
  • Image of f is $\operatorname{Im} f := \{f(a) \mid a \in A_1\} \leq A_2$.

Suppose $f: R_1 \to R_2$ is a ring homorphism. Then the kernel $\ker f$ of f is a subring of R_1 and $\operatorname{im} f$ is a subring of R_2. Moreover, $\forall a \in A$, $x \in \ker f$, $ax, xa \in \ker f$.

proof: It is enough to show that they are closed under multiplication.

$\forall a \in \ker f$ and $\forall a' \in R_1$, we have $f(a \cdot a') = f(a) \cdot f(a') = 0 \cdot f(a') = 0 \Rightarrow a \cdot a' \in \ker f$

So closed.

$\forall b, b' \in \operatorname{im} f \Rightarrow \exists c, c' \in R_1$ st $f(c) = b$, $f(c') = b' \Rightarrow f(c \cdot c') = b \cdot b'$. ∎

Find the Kernel of $c_n: \mathbb{Z} \to \mathbb{Z}_n$, $c_n(a) := [a]_n$

Solution: Note $a \in \ker c_n \iff c_n(a) = [0]_n \iff n \mid a$.

So $\ker c_n = n\mathbb{Z}$.

Note $c_n : \mathbb{Z}[x] \to \mathbb{Z}_n[x]$, $c_n\left(\sum_{i=0}^{\infty} a_i x^i\right) := \sum_{i=0}^{\infty} c_n(a_i) x^i$ is a ring homomorphism. Find Kernel of c_n.

proof: $\sum_{i=0}^{\infty} a_i x^i \in \ker c_n \iff \sum_{i=0}^{\infty} c_n(a_i) x^i = 0 \iff$ all $c_n(a_i) = 0 \iff$ all $a_i \in \ker c_n$

So $\ker c_n = n\mathbb{Z}[x]$.

✱ If $(G, \cdot)$ is a group and $g \in G$, then cyclic groups generated by g is $\{g^n \mid n \in \mathbb{Z}\}$ and $e_g(n) := g^n$ is a group homorphism.

✱ Suppose R is unital with the identity element 1_R. Then

$$e : \mathbb{Z} \to R, \quad e(n) := n 1_R$$

is a ring homorphism

proof: we show $e(mn) = e(m) \cdot e(n)$

Case 1: $m = 0$ or $n = 0$

$\rightarrow$ $e(0) = 0$

case 2: $m, n > 0$

$\rightarrow$ $e(mn) = \underbrace{1_R + \cdots + 1_R}_{mn \text{ times}}$

$e(m) \cdot e(n) = (\underbrace{1_R + \cdots + 1_R}_{m \text{ times}})(\underbrace{1_R + \cdots + 1_R}_{n \text{ times}})$

clearly both are equal.

Others can be dealt similarly.

Suppose B is a commutative ring and A is a subring of B. Suppose $b \in B$, then evaluation map $\phi_b : A[x] \to B$, $\phi_b(f(x)) := f(b)$ is a ring homorphism

proof: We have to show that for every $f_1, f_2 \in A[x]$

(i) $\phi_b(f_1(x) + f_2(x)) = \phi_b(f_1(x)) + \phi_b(f_2(x))$

(ii) $\phi_b(f_1(x) f_2(x)) = \phi_b(f_1(x))\, \phi_b(f_2(x))$

(i) $\phi_b(f_1(x)+f_2(x)) = \phi_b((f_1+f_2)(x)) = (f_1+f_2)(b)$

$= f_1(b)+f_2(b) = \phi_b(f_1(x)) + \phi_b(f_2(x))$

(ii) $\phi_b(\underbrace{f_1(x)\cdot f_2(x)}_{\text{multiply them}}) = \phi(p(x)) = p(b)$

$f_1(x)\cdot f_2(x) = p(x)$

then $f_1(b)\cdot f_2(b) = p(b)$. So done ∎

$\ker\phi_b = \{p(x)\in A[x] \mid p(b)=0\}$

$\operatorname{im}\phi_b = \{p(b) \mid p(x)\in A[x]\} = \{\sum_{i=0}^{n} a_i b^i \mid a_i\in A, n\in\mathbb{Z}\}$

LECTURE 3

* Evaluation map is $\phi_b : A[x] \to B$, $\phi_b(f(x)) := f(b)$

\# Suppose A is a subring of a unital commutative ring B and $b \in B$. Then the image of the evaluation map ϕ_b is the smallest subring of B that contains both A and b

proof : Since ϕ_b is a ring homomorphism, its image is a subring. For every $a \in A$, $\phi_b(a) = a$ & $\phi_b(x) = b$. So $A, b \in \text{Im}\,\phi_b$.

Let S contain both A & b. Then $\forall\, a_0, \dots, a_n \in A$, by considering $p(x) = a_0 + a_1x + \dots + a_nx^n$, we get if $p(b) \in \text{Im}\,\phi_b$, it also belongs to S.

$\Rightarrow \text{Im}\,\phi_b \subseteq S$.

$\Rightarrow \text{Im}\,\phi_b$ is the smallest such set ■

* Suppose A is a subring of a unital commutative ring B, and $b \in B$

The smallest subring of B which contains A & b is denoted by $A[b]$.

* Suppose R is a unital ring. We say $a \in R$. We say $a \in R$ is a unit if there is $a' \in R$ such that $a \cdot a' = a' \cdot a = 1_R$. The set of all units of R is denoted by $R^\times$.

\# Suppose R is a unital commutative ring and $a \in R$ is a unit. Then there is a unique $a' \in R$ such that $a \cdot a' = 1_R$.

proof : Say a' & a'' are inverses.

Note $a'' = a'' \cdot a \cdot a' = a'$ ■

\# Suppose R is a unital ring. Then $(R^\times, \cdot)$ is a group.

proof : It alredy has inverses property. It clearly has inverses.

It is closed as $(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = (b^{-1} \cdot a^{-1}) \cdot (a \cdot b) = 1_R$ ■

* $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$

\# Find $\mathbb{Z}^\times$

proof: If $a \in \mathbb{Z}^\times \Rightarrow aa' = 1 \Rightarrow |a|\,|a'| = 1 \Rightarrow a = 1$ or -1.

So $\mathbb{Z}^\times = \{1, -1\}$ which works ■

Find 2^{-1} in $\mathbb{Z}_3$

Solution: $[2]_3 \cdot [2]_3 = [1]_3 \Rightarrow 2^{-1} = 2$ in $\mathbb{Z}_3$.

♥ $a\mathbb{Z} + b\mathbb{Z} = \gcd(a,b)\mathbb{Z}$

♥ · $\mathbb{Z}_n^{\times} = \{ [a]_n \mid \gcd(a,n) = 1 \}$

· $|\mathbb{Z}_n^{\times}| = \phi(n)$

♥ (Euler's theorem) Suppose n is a positive integer and $\gcd(a,n) = 1$.

$$a^{\phi(n)} \equiv 1 \mod n$$

* A unital commutative ring F is called field if $F^{\times} = F \setminus \{0\}$

* $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields. $\mathbb{Z}$ is not.

Suppose n is a positive integer. Then $\mathbb{Z}_n$ is a field if and only if n is prime

proof: $\mathbb{Z}_n$ is field $\Leftrightarrow$ $\mathbb{Z}_n^{\times} = \mathbb{Z}_n \setminus \{[0]_n\}$ $= \{ [a]_n \mid \gcd(a,n) = 1 \}$ $\Leftrightarrow$ $\forall$ +ve integer less than n is coprime with n. ■

* Suppose R is a commutative ring. We say $a \in R$ is a zero-divisor if $a \neq 0$ and $ab = 0$ for some non-zero $b \in R$. The set of zero divisors is denoted as $D(R)$.

* A unital commutative ring D is called an Integral domain if D has no zero divisors and more than one element.

$\Leftrightarrow 1_R \neq 0_R$. If $1_R \neq 0_R$ then more than one element.

If $1_R = 0_R \Rightarrow$ if $x \in R \Rightarrow 0 = 0 \cdot x = 1 \cdot x = x$. So $R = \{0\}$

* $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are integral domains and $\mathbb{Z}_6$ is not integral domain.

Suppose R is a unital commutative ring. Then $R^{\times} \cap D(R) = \emptyset$.

proof: let $0 \neq a \in R^{\times} \cap D(R) \Rightarrow \exists\, a^{-1} \in R$ st $a \cdot a^{-1} = 1$ and $0 \neq b \in R$ st $a \cdot b = 0 \Rightarrow$ $0 = a^{-1} \cdot (a \cdot b) = (a^{-1} \cdot a)\, b = b \Rightarrow b = 0$. A contradiction ■

Every field is an integral domain.

proof: We know F is a field if $F^{\times} = F / \{0\}$.

We know $F^{\times} \cap D(F) = \emptyset \Rightarrow D(F) = \emptyset \Rightarrow F$ is integral domain.

(Cancellation law) Suppose D is an Integral domain. Then $\forall\ 0 \neq a \in D,\ b, c \in D$

$$ab = ac \Rightarrow b = c$$

proof: Since $ab = ac \Rightarrow a(b-c) = 0 \Rightarrow b-c = 0 \Rightarrow b = c$ ∎

integral domain

Suppose D is a finite integral domain. Then D is a field.

proof: Since D is integral domain, it is also a commutative ring and $0_D \neq 1_D$.

So we need to show that every non-zero element $a \in D$ is a unit.

We do the the "FLT" trick.

let $\{x_1, \dots, x_n\}$ be the set.

Note that $1 \in \{x_1, \dots, x_n\}$

Consider $\{a \cdot x_1, \dots, a \cdot x_n\}$

Note that $\{a \cdot x_1, \dots, a \cdot x_n\} = \{x_1, \dots, x_n\}$ else $\exists\, b \neq c$ st $ab = ac \Rightarrow a(b-c) = 0$. H is integral domain.

So $\exists\ x_i$ st $ax_i = 1$. So x_i is the inverse of a. ∎

★ Suppose R is a ring. let

$$N^+(R) := \{ n \in \mathbb{Z}^+ \mid \forall a \in R,\ na = 0 \}$$

If $N^+(R)$ is empty, we say that characteristic of R is zero. If $N^+(R)$ is not empty, the characteristic of R is minimum of

The characteristic of R is denoted by $\text{char}(R)$

Subgroups of $\mathbb{Z}$ are of the form $a\mathbb{Z}$

Let R be a unital ring and $e: \mathbb{Z} \to R$, $e(t) := t\,1_R$. For every unital ring R, we have $\ker e = \text{char}(R)\,\mathbb{Z}$.

proof: Note that $\ker e \leq \mathbb{Z}$, hence is of the form $n_0\mathbb{Z}$. let $\text{char}(R) = n$.

Clearly $n 1_R = 0 \Rightarrow n\mathbb{Z} \leq \ker e$.

If $n_0 < n \Rightarrow e(n_0) = n_0 1_R = 0$ is not possible $\text{char}(R) = n > n_0$.

Here $\ker e = n\mathbb{Z}$. ∎

Suppose D is an integral domain. Then $\text{char}(D)$ is either 0 or a prime.

proof: If $\text{char}(D) = n \neq 0$ and say n is composite $\Rightarrow \exists\ a, b \neq 1$ st $n = ab$

Then $(\underbrace{1_D + \dots + 1_D}_{a})(\underbrace{1_D + \dots + 1_D}_{b}) = (a 1_D)(b 1_D) = ab\, 1_D = 0$ and $a 1_D \neq 0$, $b 1_D \neq 0$. Not possible as ID ∎

LECTURE 4

$f: X \to Y$ is embedding if it is injective and structure preserving

- Every integral domain can be embedded into a field

* Suppose D is an integral domain. For (a,b) and (c,d) in $D \times (D \setminus \{0\})$, we say $(a,b) \sim (c,d)$ if $ad = bc$. Note $\sim$ is equivalance relation as :

(i) $(a,b) \sim (a,b)$ as $ab = ba$

(ii) If $(a,b) \sim (c,d) \Rightarrow ad = bc \Rightarrow cb = da \Rightarrow (c,d) \sim (a,b)$

(iii) If $(a,b) \sim (c,d)$ & $(c,d) \sim (e,f) \Rightarrow ad = bc,\ cf = de \Rightarrow ade = bce,\ adf = bcf,\ acf = ade,\ bcf = bde$

$\Rightarrow ade = bce = acf$ -

$adf = bcf = bde \Rightarrow afd = bed \Rightarrow af = be$ as integral domain and commutative ■

* We let $\frac{a}{b}$ be the equivalence class $[(a,b)]$, let

$$Q(D) = \left\{ \frac{a}{b} \,\middle|\, (a,b) \in D \times (D \setminus \{0\}) \right\}$$

* $\frac{a}{b} + \frac{c}{d} := \frac{ad+bc}{bd}$ and $\frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}$

To check if it is well defined :

let $\frac{a_1}{b_1} = \frac{a_2}{b_2}$ and $\frac{c_1}{d_1} = \frac{c_2}{d_2}$

- $\frac{a_1}{b_1} + \frac{c_1}{d_1} = \frac{a_1 d_1 + c_1 b_1}{b_1 d_1}$, $\frac{a_2}{b_2} + \frac{c_2}{d_2} = \frac{a_2 d_2 + c_2 b_2}{b_2 d_2}$

We need to show $\frac{a_1 d_1 + c_1 b_1}{b_1 d_1} = \frac{a_2 d_2 + c_2 b_2}{b_2 d_2}$

to show
$\Rightarrow (a_1 d_1 + c_1 b_1)(b_2 d_2) = (a_2 d_2 + c_2 b_2)(b_1 d_1)$

to show
$\Rightarrow a_1 d_1 b_2 d_2 + c_1 b_1 b_2 d_2 = a_2 d_2 b_1 d_1 + c_2 b_2 b_1 d_1$

but we know $a_1 d_2 = a_2 d_1$ & $c_1 d_2 = c_2 d_1$

Hence the equality follows.

- $\frac{a_1}{b_1} = \frac{a_2}{b_2}$, $\frac{c_1}{d_1} = \frac{c_2}{d_2}$. To show $\frac{a_1 \cdot c_1}{b_1 \cdot d_1} = \frac{a_2 \cdot c_2}{b_2 \cdot d_2}$ or show $a_1 \cdot c_1 \cdot b_2 d_2 = a_2 \cdot c_2 \cdot b_1 \cdot d_1$

which is true as $a_1 b_2 = a_2 b_1$, $c_1 d_2 = c_2 d_1$ ■

✱ $(Q(D), +, \cdot)$ is a ring.

as $\frac{a}{b} + \frac{(-a)}{b} = \frac{0}{b} = \frac{0}{1}$. So $Q(D)$ is group. Multiplication is defined too. So a ring.

✱ · $\frac{0}{1}$ is additive identity as $\frac{0}{1} + \frac{a}{b} = \frac{0 \cdot b + a \cdot 1}{1 \cdot b} = \frac{a}{b}$. Note $\frac{0}{1} = \frac{0}{b}$.

· $\frac{1}{1}$ is multiplicative identity : $\frac{1}{1} \cdot \frac{a}{b} = \frac{a}{b}$

· Note $\frac{a}{b} \cdot \frac{b}{a} = \frac{a \cdot b}{ba} = \frac{1}{1}$. $\Rightarrow$ $Q(D)$ is a field

\# Suppose D is an integral domain. Let $i : D \to Q(D)$, $i(a) = \frac{a}{1}$.

Then i is an injective ring homorphism.

proof: We need to show $i(a) + i(b) = i(a+b)$ and $i(a) \cdot i(b) = i(a \cdot b)$ $\forall\, a, b \in D$

$$i(a) + i(b) = \frac{a}{1} + \frac{b}{1} = \frac{a \cdot 1 + b \cdot 1}{1 \cdot 1} = \frac{a+b}{1} = i(a+b)$$

$$i(a) \cdot i(b) = \frac{a}{1} \cdot \frac{b}{1} = \frac{a \cdot b}{1 \cdot 1} = i(a \cdot b)$$

It is injective as $i(a) = i(b) \Rightarrow \frac{a}{1} = \frac{b}{1} \Rightarrow a \cdot 1 = 1 \cdot b \Rightarrow a = b$. ■

Suppose A and B are rings. We say A can be embedded in B if there is an injective ring homorphism from A to B.

We also say B has a copy of A

\# Suppose D is an integral domain and F is a field. Suppose $f : D \to F$ is an injective ring homorphism.

Then $\tilde{f} : Q(D) \to F$, $\tilde{f}\left(\frac{a}{b}\right) = f(a) f(b)^{-1}$ is well defined.

Called Universal property of field of fractions

Moreover the following is a commuting diagram

$$\begin{tikzcd} D \arrow[r, "i"] \arrow[dr, "f"'] & Q(D) \arrow[d, "\tilde{f}"] \\ & F \end{tikzcd}$$

$\Rightarrow$ $\tilde{f} \circ i = f$, $i : D \to Q(D)$, $i(a) = \frac{a}{1}$.

proof: • $\tilde{f}$ is well defined as

Say $\frac{a_1}{b_1} = \frac{a_2}{b_2}$

$\tilde{f}\left(\frac{a_1}{b_1}\right) = f(a_1) f(b_1)^{-1}$

$\tilde{f}\left(\frac{a_2}{b_2}\right) = f(a_2) f(b_2)^{-1}$

To show $f(a_1)f(b_1)^{-1} = f(a_2)f(b_2)^{-1}$

But $a_1b_2 = a_2b_1 \Rightarrow f(a_1b_2) = f(a_2b_1)$

$\Rightarrow f(a_1)f(b_1)^{-1} = f(a_2)f(b_1)^{-1}$.

- $\tilde{f}$ is ring homorphism as f is ring homorphism.

- $\tilde{f}$ is injective as $0 = \tilde{f}\left(\frac{a}{b}\right) = f(a)f(b^{-1}) \Rightarrow f(a) = 0 \Rightarrow a = 0$. So kernel is trivial.

- To show the diagram commute, we need to show

  $\tilde{f}(i(a)) = f(a) \quad \forall a \in D$.

  $\tilde{f}(i(a)) = f\left(\frac{a}{1}\right) = f(a)f(1) \; \forall a \in D$

  But $f(1 \cdot 1) = f(1)f(1) \Rightarrow f(1) = 1$ as f is injective

  So done. ■

$\Rightarrow$ Hence if F is a field which contains a copy of $D \Rightarrow F$ contains a copy of $Q(D)$.

✱ $Q(D)$ is the smallest field which contains a copy of D.

♥ To show $Q(D) \cong F$:

1> Prove F is a field

2> Find an injective ring homorphism $f: D \to F$

3> Use universal property of field of fractions to get the injective ring homorphis $\tilde{f}: Q(D) \longrightarrow F$, $\tilde{f}\left(\frac{a}{b}\right) = f(a)f(b)^{-1}$

4> Show that every element of F is of the form $f(a)f(b)^{-1}$

12 12:45 1:30
6, 7, 8, 9, 10, 11, 12, 13, 14

LECTURE 5

Prove that $Q(\mathbb{Z}[i]) \cong \mathbb{Q}(i)$

proof: Step 1: $\mathbb{Q}(i)$ is a field

$\mathbb{Q}(i)$ is a ring clearly. Just to show inverses exist. let $a+bi \in \mathbb{Q}[i]$ be a non zero element.

$$\frac{1}{(a+bi)} = \frac{a-bi}{(a+bi)(a-bi)} = \frac{a-bi}{a^2+b^2} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2} i$$

Since $a,b \in \mathbb{Q}$, we are done.

Step 2: $f: \mathbb{Z}[i] \to \mathbb{Q}[i]$, $f(z) := z$

this is clearly an injective ring homomorphism.

Step 3: By the universal property of field of fractions.

$$\tilde{f}: Q(\mathbb{Z}[i]) \to \mathbb{Q}[i], \quad \tilde{f}\left(\frac{z_1}{z_2}\right) = f(z_1) f(z_2)^{-1}$$

which is well defined injective ring homomorphism.

Step 4: $\tilde{f}$ is surjective

Suppose $a+bi \in \mathbb{Q}[i] = \frac{r+si}{t} = f(r+si) f(t)^{-1}$.

So surjective.

Hence isomorphism ∎

✱ Suppose A is a ring, and I is a non-empty subset. We say I is an ideal of A if

1. For every $x, y \in I$, $x - y \in I$ and
2. For every $x \in I$ and $a \in A$, then $ax \in I$, $xa \in I$.

So I is subring

For every ring homomorphism $f: A \to B$, we have that $\ker f$ is an ideal.

proof: If $a \in \ker f$, $b \in \ker f$ $\Rightarrow f(a-b) = f(a) - f(b) = 0 - 0 = 0$.

If $a \in \ker f$, $x \in A$ $\Rightarrow f(ax) = f(a) \cdot f(x) = 0 \cdot f(x) = 0$. ∎

\# Suppose A is a unital commutative ring, and $x_1, \dots, x_n \in A$. Then the smallest ideal of A which contains $x_1, \dots, x_n$ is

$$I = \{a_1 x_1 + \cdots + a_n x_n \mid a_1, \dots, a_n \in A\}$$

We denote this ideal by $\langle x_1, \dots, x_n \rangle$ call it ideal generated by $\langle x_1, \dots, x_n \rangle$.

proof: we show that it is an ideal.

Suppose $y, y' \in I$.

$$y = \sum_{i=1}^{n} a_i x_i \quad \text{and} \quad y' = \sum_{i=1}^{n} a_i' x_i$$

$$\Rightarrow y - y' = \sum_{i=1}^{n} (a_i - a_i') x_i \in I$$

$$\Rightarrow ay = \sum_{i=1}^{n} a a_i x \in I$$

So it is an ideal.

Clearly, $x_i \in I$.

Suppose J is ideal containing x_i's.

Then for $a_i \in A$, we get $a_i x_i \in J \Rightarrow \sum a_i x_i \in J$. So $\forall\, i \in I,\ i \in J$.

So $I \subseteq J$ ∎

* We say ideal I is a principal ideal if it is generated by one element.

$$\langle x \rangle = \{ax \mid a \in A\}$$

We denote $\langle x \rangle$ by xA.

* $(x + I) + (y + I) := (x+y) + I$

\# Suppose $I \trianglelefteq A$. The following is a well defined operation on A/I.

$(x+I) \cdot (y+I) := xy + I$

proof: Suppose $x_1 + I = x_2 + I$ and $y_1 + I = y_2 + I$.

Then $x_1 - x_2 \in I$ and $y_1 - y_2 \in I$.

To show $x_1 y_1 + I = x_2 y_2 + I$

$\Rightarrow x_1 y_1 - x_2 y_2 \in I$

But $x_1(y_1-y_2) \in I$ & $y_2(x_1-x_2) \in I$

So done.

Suppose A is a ring and $I \trianglelefteq A$. Then

1. $(A/I, +, \cdot)$ is a ring where for every $x+I, y+I \in A/I$ we have

$(x+I) + (y+I) := (x+y)+I$ and $(x+I)\cdot(y+I) = xy+I$

2. $p_I : A \to A/I$, $p_I(x) := x+I$ is a surjective ring homomorphism

3. $\ker p_I = I$

proof: 1 is clear.

2. $p_I(x) + p_I(y) = (x+I) + (y+I) = (x+y)+I = p_I(x+y)$

$p_I(x)\cdot p_I(y) = (x+I)\cdot(y+I) = (xy)+I = p_I(xy)$

let $x+I \in A/I$ and $p_I(x) = x+I \Rightarrow p_I$ is surjective ■

3. $x \in \ker p_I \Leftrightarrow p_I(x) = 0+I \Leftrightarrow x+I = 0+I \Leftrightarrow x \in I$.

♥ The ring A/I is called a quotient ring of A and p_I is called the natural map

* Suppose A is a ring and I is a subset of A. Then I is the kernel of a ring homomorphism iff I is an ideal.

* (The 1st isomorphism theorem for groups) Suppose $f: G \to G'$ is a group homomorphism. Then

$\bar{f}: G/\ker f \to \operatorname{Im} f$, $\bar{f}(g \ker f) = f(g)$

is a well defined group isomorphism.

* Suppose $f: A \to A'$ is a ring homomorphism. Then

$\bar{f}: A/\ker f \to \operatorname{Im} f$, $\bar{f}(a+\ker f) := f(a)$ is a ring isomorphism.

proof: We know by 1st isomorphism theorem for groups, $\bar{f}$ is isomorphism. We show that it preserve multiplication

$\bar{f}(xy+\ker f) = f(xy) = f(x)f(y) = \bar{f}(x+\ker f)\bar{f}(y+\ker f) \quad \forall x,y \in A$ ■

* Suppose n is a positive integer. Then $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$

proof: let $c_n: \mathbb{Z} \to \mathbb{Z}_n$ be the residue map $c_n(x) := [x]_n$. Then c_n is surjective and $x \in \ker c_n \Leftrightarrow x \in n\mathbb{Z}$

So $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ ■

* $\mathbb{Q}[x]/\langle x^2-2\rangle \cong \mathbb{Q}[\sqrt{2}]$ and $\mathbb{Q}[\sqrt{2}] = \{a+b\sqrt{2} \mid a,b\in\mathbb{Q}\}$

proof: $\langle x^2-2\rangle$ = ideal generated by x^2-2

$= \{q(x^2-2) \mid q\in\mathbb{Q}\}$

$\phi_{\sqrt{2}} : \mathbb{Q}[x] \to \mathbb{C}$ be the evaluation map.

$\mathbb{Q}[x]/\ker\phi_{\sqrt{2}} \cong \operatorname{Im}\phi_{\sqrt{2}}$

Clearly $\operatorname{im}\phi_{\sqrt{2}} = \mathbb{Q}[x]$

$\ker\phi_{\sqrt{2}}$:= Note that $\sqrt{2}$ is zero of x^2-2.

let $f(x)\in\ker\phi_{\sqrt{2}}$.

let $f(x) = q(x)\cdot(x^2-2) + r(x)$

$\Rightarrow r(x)\in\ker\phi_{\sqrt{2}}$ and $\deg r < 2$.

$\Rightarrow r(x) = ax+b \Rightarrow a\sqrt{2}+b = 0$ but $a,b\in\mathbb{Q} \Rightarrow a=b=0$.

$r(x)=0 \Rightarrow x^2-2 \mid f(x)$.

So $\ker\phi_{\sqrt{2}} = \langle x^2-2\rangle$. ■

LECTURE 6

* Suppose A is a unital commutative ring and $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in A[x]$ and $a_n \neq 0$.

we say $a_n x^n$ is the leading term of f / $ld(f) := a_n x^n$

leading coefficient a_n

degree $:= n$

* for zero polynomial

$\deg 0 = -\infty$ and $ld(0) = 0$

* Find $\deg((2x+1)(3x^2+1))$ in $\mathbb{Z}_6[x]$

Solution: $(2x+1)(3x^2+1) = 6x^3 + 3x^2 + 2x + 1 = 3x^2 + 2x + 1$

Hence $\deg((2x+1)(3x^2+1)) = 2$.

Suppose A is a unital commutative ring and $f(x), g(x) \in A[x]$

1. Suppose the leading coeffecient of f is a and the leading coefficient of g is b. If $ab \neq 0$, then $ld(fg) = ld(f)\, ld(g)$ and $\deg(fg) = \deg(f) + \deg(g)$

2. Suppose that the leading coefficient of f is not a zero-divisor. Then

$ld(fg) = ld(f)\, ld(g)$, $\deg fg = \deg f + \deg g$

proof: (1) Suppose

$$\left.\begin{aligned} f(x) &= a_0 + a_1 x + \cdots + a_n x^n \\ g(x) &= b_0 + b_1 x + \cdots + b_m x^m \end{aligned}\right\} \text{ If } a_n b_m \neq 0 \text{ then leading term is } a_n b_m.$$

Similarly for 2. ∎

Suppose D is an integral domain. Then $D[x]$ is an integral domain.

proof: Since D is unital commutative ring. Therefore $D[x]$ is a unital commutative ring.

Suppose $f(x) g(x) = 0$. Then $\deg fg = -\infty \Rightarrow \deg f + \deg g = -\infty$

$\Rightarrow$ atleast one of them 0. (also we can look at leading cfs and compare)

Suppose D is an integral domain. Then $D[x]^\times = D^\times$

proof: Clearly $D^\times \subseteq D[x]^\times$

Say $f(x) \in D[x]^\times \Rightarrow g(x) \in D[x]^\times$

st $f(x)g(x) = 1 \Rightarrow \deg f + \deg g = \deg fg = \deg 1 = 0$

$\Rightarrow$ f & g degrees are 0.

So $f, g \in D$

* long division: Suppose A is unital commutative ring $f(x), g(x) \in A[x]$ and leading cf of $g(x)$ is a unit in A.

$f(x) = g(x)q(x) + r(x)$ and $\deg r < \deg g$.

Then there are unique $q(x) \in A[x]$ (quotient) & $r(x)$

proof: • We proceed by strong induction on $\deg f$. If $\deg f < \deg g$, then $q(x) = 0$ and $r(x) = f(x)$

If assume $\deg f \geq \deg g$.

Suppose $f(x) = \sum_{i=0}^{n} a_i x^i$, $g(x) = \sum_{i=0}^{m} b_i x^i$, $a_n \neq 0$ and $b_m \neq 0$.

$\bar{f}(x) := f(x) - (b_m^{-1} a_n) x^{n-m} g(x)$

Note $\deg \bar{f} < \deg f$ then by induction hypothesis

$\bar{f}(x) = \bar{q}(x)\, g(x) + r(x)$

then $f(x) = \left(\bar{q}(x) + (b_m^{-1} a_n) x^{n-m}\right) g(x) + r(x)$

• Say $f(x) = q_1(x) g(x) + r_1(x)$

$= q_2(x) g(x) + r_2(x)$

$\Rightarrow (q_1(x) - q_2(x)) g(x) = r_2(x) - r_1(x)$

but $\deg(r_1 - r_2) < \deg g(x)$

$\Rightarrow r_2(x) - r_1(x) = 0 \quad \Rightarrow q_1(x) - q_2(x) = 0$ ∎

LECTURE 7

Suppose A is a unital commutative ring and $f(x) \in A[x]$. Then

1. for every $a \in A$, there is a unique $q(x) \in A[x]$ such that

$$f(x) = (x-a)\,q(x) + f(a)$$

2. (The factor theorem) we have that a is a zero iff $\exists\, q(x) \in A[x]$ such that

$$f(x) = (x-a)\,q(x)$$

proof: Note by long divison $\exists\, q(x)$ & $r(x)$ unique such that

$$f(x) = (x-a)\,q(x) + r(x)$$

but note that $r(x)$ will have $\deg < 1$. So it is a constant polynomial.

Note $f(a) = 0 \cdot q(x) + r(x) \Rightarrow r(x) = f(a)$.

2. If a is zero $\Rightarrow$ $f(a) = 0 \Leftrightarrow r(x) = 0 \Leftrightarrow x-a \mid f(x)$.

$\ker \phi_a = \langle x-a \rangle$, where $\phi_a : A[x] \to A$, $\phi_a(f(x)) = f(a)$

Suppose D is an integral domain, $f(x) \in D[x]$ and $a_1, \ldots, a_n$ are distinct elements of D. Then $a_1, \ldots, a_n$ are zeros of $f(x)$ iff there is $q(x) \in D[x]$

$$f(x) = (x-a_1) \cdots (x-a_n)\,q(x)$$

proof: We proceed by induction on n. Base case $n=1$ follows.

Suppose $a_1, \cdots, a_{n+1}$ are distinct zeroes of $f(x)$.

By induction, $\exists\, \tilde{q}(x)$ st $f(x) = (x-a_1) \cdots (x-a_n)\,\tilde{q}(x)$

Note a_{n+1} is zero of $\tilde{q}(x)$ as $f(a_{n+1}) = 0$ and $(a_{n+1}-a_1) \cdots (a_{n+1}-a_n) \neq 0$ and we know that it is integral domain. So $\tilde{q}(x) = (x-a_{n+1})\,q(x)$

$$f(x) = (x-a_1) \cdots (x-a_n)(x-a_{n+1})\,q(x)$$

* Factor theorem is true for any unital commutative ring, but generalized require ID.

Give an example where Generalized theorem fails

Solution: see $\mathbb{Z}_6[x]$

we have $(x-2)(x-3) = x^2 - 5x = x(x-5)$

So zeroes of x^2-5x are $2, 3, 0, 5$.

But $(x-2)(x-3)\,x\,(x-5)\,q(x) \neq x^2-5$. as $\deg (x-2)(x-3)\,x\,(x-5) > \deg(x^2-5)$

Suppose D is an integral Domain and $f(x) \in D[x] \setminus \{0\}$. Then f does not have more than $\deg f$ distinct zeroes in D.

proof: Suppose $a_1, \dots, a_m$ are distinct zeroes of $f(x)$. Then by generalised factor theorem there is $q(x) \in D[x]$

$$f(x) = (x-a_1) \cdots (x-a_m) q(x)$$

So $\deg f = m + \deg q$ ■

Suppose p is a prime number. Then

$$x^p - x = x(x-1) \cdots (x-(p-1)) \text{ in } \mathbb{Z}_p[x].$$

proof: By FLT, we know $0, 1, \dots, p-1$ are zeroes and

$\mathbb{Z}_p[x]$ is Id. By degree comparision, we are done.

Clearly $x^p - x = x(x-1) \cdots (x-(p-1)) c$

clearly $c = 1$. Done ■

Suppose p is an odd prime number. Deduce that $\binom{p-1}{i} \equiv (-1)^i \bmod p$ for every $0 \le i \le p-1$

proof: We know $(x-1)^p = x^p - 1$ in $\mathbb{Z}_p[x]$

$$\Rightarrow (x-1)^{p-1} = x^{p-1} + \cdots + x + 1$$

So by comparing cfs, we get $\binom{p-1}{i}(-1)^{p-1-i} \equiv 1 \bmod p$

$$\Rightarrow \binom{p-1}{i}(-1)^{-i} \equiv 1 \bmod p \quad \text{as } p-1 \text{ is even}$$

$$\Rightarrow \binom{p-1}{i} \equiv (-1)^i \bmod p. \quad ■$$

♥ Note $\phi_\alpha : \mathbb{Q}[x] \to \mathbb{C} \Rightarrow \mathbb{Q}[x]/\ker \phi_\alpha \cong \mathbb{Q}[\alpha]$.

Suppose F is a field. Then every ideal of $F[x]$ is a principal.

proof: Suppose I is an ideal of $F[x]$. If I is a zero ideal then done.

Say $I \neq 0$, then choose $p_0(x) \in I$ such that

$\deg p_0 = \min \{\deg p \mid p \in I \setminus \{0\}\}$

claim: $I = \langle p_0 \rangle$

proof: let $f(x) \in I$. Then long division gives $f(x) = p_0(x) q(x) + r(x)$ and $\deg r < \deg p_0$.

So $r(x) \in I$ but $\deg r(x) < \deg p_0(x)$. NP.

so $r(x) = 0$. So $f(x) \in \langle p_0(x) \rangle$ ■

* Suppose D is an integral domain. We say D is a Principal Ideal Domain if every ideal of D is principal.

♥ $\mathbb{Z}$ and $F[x]$, F is field are PIDs

↪ Subrings are $n\mathbb{Z} = \langle n \rangle$

* An integral domain D is called a Euclidean domain if there is a norm function $N: D \to \mathbb{Z}^{\geq 0}$ with the following properties:

1. $N(d) = 0$ iff $d = 0$
2. $\forall a \in D$ & $b \in D \setminus \{0\}$, there are $q, r \in D$ such that not unique q?
   (i) $a = bq + r$
   (ii) $N(r) < N(b)$

\# Suppose D is a Euclidean Domain. Then D is a PID.

proof: Suppose I is an ideal of D. If I is zero, we are done. Suppose I is not zero. Choose $a_0 \in I$ such that $N(a_0)$ is minimum

claim: $I = \langle a_0 \rangle$

proof: let $a = a_0 q + r$. then $N(r) < N(a_0)$

but clearly $r \in I \Rightarrow r = 0 \Rightarrow a = a_0 q \in \langle a_0 \rangle$ ■

LECTURE 8

$\mathbb{Z}[i]$ is a Euclidean domain and PID

proof: We define the norm function

$$N: \mathbb{Z}[i] \to \mathbb{Z}^{\geq 0}, \; N(z) := |z|^2$$

So $N(a+bi) = a^2+b^2 \in \mathbb{Z}^{\geq 0}$

Note $N(z) = 0 \Leftrightarrow |z| = 0 \Leftrightarrow z = 0$.

Now to show the existence of q, r st

$z = qw + r$ st $N(r) < N(w)$

say $z \in \mathbb{Z}[i]$ & $w \in \mathbb{Z}[i]$

$\frac{\alpha}{\beta} = r + is$, where $r, i \in \mathbb{Q}$ (rationalise denominator)

choose integers st $|r-a| \leq \frac{1}{2}$ and $|s-b| \leq \frac{1}{2}$.

$$\begin{aligned}\alpha &= \beta(r+is) \\ &= \beta(a+ib) + \beta((r-a) + i(s-b)) \\ &= \beta q + r.\end{aligned}$$

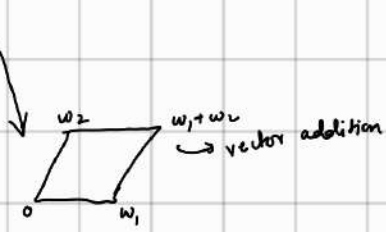
We need to show $N(r) < N(\beta)$

$$\begin{aligned}N(r) &= N(\beta) \cdot N((r-a) + i(s-b)) \\ &= N(\beta) \cdot ((r-a)^2 + (s-b)^2) \\ &\leq N(\beta) \cdot \left(\tfrac{1}{4} + \tfrac{1}{4}\right) = \frac{N(\beta)}{2}\end{aligned}$$

Let $\omega = \frac{-1}{2} + \frac{\sqrt{3}}{2} i$ and $\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}$. Show it is a PID.

proof: 1) Draw a picture of the lattice in the complex plane of points $a + b\omega$ where $\omega = \frac{(1+\sqrt{-3})}{2}$.

Say $a, b \in \mathbb{Z}[\omega]$



2) Draw point b and take corner st qa is closest to b.

So $b = qa - r$

Note that the r distance is $\leq \frac{|a|\sqrt{2}}{2}$

$$|r| \leq |a|\frac{\sqrt{2}}{2} < |a|$$

So $N(r) < N(a)$

So yay!

★ 1. We say $\alpha \in \mathbb{C}$ is an algebraic number if it is a zero of a polynomial $f(x) \in \mathbb{Q}[x]$

So E is field extension of F

2. More generally, when F is a subfield of another field E, we say $\alpha \in E$ is algebraic over F if α is a zero of polynomial $f(x) \in F[x]$

3 A complex number α is called transcendtal if it is not algebraic.

4. Assuming E is a field extension of F, we say $\alpha \in E$ is transcendental over F if it is not algebraic over F

Note that for E, a field extension of F, $\alpha \in E$ is algebraic over F iff $\ker \phi_\alpha \neq 0$.

$\phi_\alpha : F[x] \to E$, $\phi_\alpha(f(x)) := f(\alpha)$

- $F[x]/\ker \phi_\alpha \cong F[\alpha]$

Suppose E is a field extension of F, and $\alpha \in E$ is transcendental over F. Then $F[\alpha] \cong F[x]$.

proof: Since α is transcendental over F $\Rightarrow \ker \phi_\alpha = 0$.

Note F[x] is a PID and ED over $\forall$ field F.

(The minimal polynomial). Suppose E is a field extension of F, $\alpha \in E$ is algebraic over F. Then the following statement holds.

1. There is a unique non-constant monic polynomial $m_\alpha(x) \in F[x]$ such that such that $\ker \phi_\alpha = \langle m_\alpha(x) \rangle$. ($m_\alpha(x) \in F[x]$ is called the minimal polynomial of α over F)

2. The minimal polynomial $m_\alpha(x) \in F[x]$ is non constant monic polynomial which cannot be written as a product of smaller degree polynomials in F[x].

proof: (1) Since F[x] is pid $\ker F_\alpha[x]$ is generated by 1 single polynomial $f(x) \in F[x]$.

Since α is algebraic $\Rightarrow$ $f(x) \neq 0$ and clearly is not non constant.

$f(x) = a_n x^n + \cdots + a_0$, $a_n \neq 0$.

Then since we are working in F. So a_n is unit.

$\bar{f}(x) = a_n^{-1} f(x) = x^n + (a_n^{-1} a_{n-1}) x^n + \cdots + (a_n^{-1} a_0)$

Note $\bar{f}(x) \in \langle f(x) \rangle$

and $f(x) = a_n \bar{f}(x) \in \langle \bar{f} \rangle$

So $\langle \bar{f} \rangle = \langle f \rangle = \ker \phi$

So a monic polynomial does exists

claim: f_1 & f_2 are non constant monic polynomials in F[x] and $\langle f_1 \rangle = \langle f_2 \rangle$. Then $f_1 = f_2$.

proof: Since $\langle f_1 \rangle = \langle f_2 \rangle$, there are polynomials $q_1, q_2 \in F[x]$ such that $f_1 q_1 = f_2$ & $f_1 = q_2 f_2$. $\Rightarrow$ $\deg f_1 = \deg f_2$.

$\Rightarrow f_1 | f_2$ & $f_2 | f_1 \Rightarrow f_1 = f_2$ as they both are monic.

(2) Suppose $m_\alpha(x) = g(x)h(x)$ for some $g(x), h(x) \in F[x]$ st $\deg g, h < \deg m$

Since $m_\alpha(\alpha) = 0 \Rightarrow g(\alpha)h(\alpha) = 0$ & $\deg m_\alpha > \deg g$ & $\deg m_\alpha \geq \deg h$

But $F[x]$ is ID $\Rightarrow g(\alpha) = 0$ or $h(\alpha) = 0$

$\Rightarrow \deg g \geq \deg m_\alpha$ or $\deg h \geq \deg m_\alpha$. NP. ∎

\# (Characterization of minimal polynomials) Suppose E is a field extension of F, and $\alpha \in E$ is algebraic over F. Then a monic non-constant polynomial $p(x)$ in $F[x]$ is the minimal poly of α iff $p(\alpha) = 0$ and $p(x)$ cannot be written as product of smaller degree polynomials in $F[x]$.

proof: We showed $\Rightarrow$ direction above.

Since $p(\alpha) = 0$, $p(x) \in \ker \phi$. Since $\ker \phi$ is generated by a minimal polynomial m_α. So $p(x) = m_\alpha(x) q(x)$. , but $p(x)$ cannot be written as smaller factors

$\Rightarrow c m_\alpha(x) = p(x)$, $c \in F$. But leading of must be 1 as $p(x)$ is monic.

So $m_\alpha(x) = p(x)$ ∎

♥ So $m_\alpha(x)$ has the smallest degree among non-zero polynomials in $F[x]$ that α has zero.

\# Suppose E is a field extension of F, $\alpha \in E$ is algebraic over F. Then the following hold:

1. For $f(x) \in F[x]$, $f(\alpha) = 0$ if and only if $m_\alpha(x) | f(x)$ in $F[x]$.

2. Suppose α is a zero of a non-zero polynomial $p(x) \in F[x]$. If $\deg p \leq \deg m_\alpha$, then there is a non-zero constant c such that $p(x) = c\, m_\alpha(x)$

proof: (1) $f(\alpha) = 0 \Leftrightarrow f \in \ker \phi_\alpha = \langle m_\alpha(x) \rangle \Leftrightarrow m_\alpha(x) | f(x)$

(2) if $p(\alpha) = 0 \Rightarrow p \in \ker \phi_\alpha \Rightarrow m_\alpha(x) | p(x) \Rightarrow p(x) = m_\alpha(x) q(x) \Rightarrow \deg p(x) = \deg m_\alpha(x)$. ∎

So quotienting by $\langle p(x) \rangle$

\# Suppose A is a unital commutative ring and $p(x) \in A[x]$ is a monic polynomial of degree $n \geq 1$. Then every element of $A[x]$ can be written uniquely as

$a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + \langle p(x) \rangle$

proof: let $f(x) \in A[x]$.

Then $f(x) = q(x) p(x) + r(x)$ & $\deg r(x) < \deg p(x)$.

If $r(x) = \sum_{i=0}^{n-1} a_i x^i$

Then $f(x) + \langle p(x) \rangle = \sum_{i=0}^{n-1} a_i x^i$

Uniqueness: Suppose $\sum_{i=0}^{n-1} a_i x^i + \langle p(x) \rangle = \sum_{i=0}^{n-1} a_i' x^i + \langle p(x) \rangle$

$\Rightarrow \quad \sum_{i=0}^{n-1} (a_i - a_i') \, x^i \in \langle p(x) \rangle$

but max degree is $n-1$

$\Rightarrow \quad a_i - a_i' = 0 \;\; \forall i \in [n-1] \blacksquare$

LECTURE 9

Suppose E is a field extension of F, and $\alpha \in E$ is algebraic over F.

Suppose the degree of the minimal polynomial $m_\alpha(x)$ of α over F is n. Then every element of $F[\alpha]$ for some a_i's in F.

proof: $\bar{\Phi}_\alpha : F[x]/\langle m_\alpha(x)\rangle \longrightarrow F[\alpha]$

$\bar{\Phi}_\alpha(f(x)+\langle m_\alpha(x)\rangle) = f(\alpha)$ is isomorphism

we every element $F[x]/\langle m_\alpha(x)\rangle$ can be written uniquely as $(\sum_{i=0}^{n-1} a_i x^i) + \langle m_\alpha(x)\rangle$.

so $\bar{\Phi}_\alpha\left(\sum_{i=0}^{n-1} a_i x^i + \langle m_\alpha(x)\rangle\right) = \sum_{i=0}^{n-1} a_i \alpha^i$ ■

$\mathbb{Q}[i] = \{a+bi \mid a,b \in \mathbb{Q}\}$ because $m_{i,\mathbb{Q}}(x) = x^2+1$

and $\mathbb{Q}[\sqrt[3]{2}] = \{a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{4} \mid a_0, a_1, a_2 \in \mathbb{Q}\}$ because $m_{\sqrt[3]{2},\mathbb{Q}}(x) = x^3-2$.

* Suppose D is an integral domain. We say $d \in D$ is irreducible if

1. $d \notin D^\times \cup \{0\}$ and
2. If $d = ab$ for some $a,b \in D$, then either $a \in D^\times$ or $b \in D^\times$.

For instance an integer n is irreducible in $\mathbb{Z}$ if $n = \pm p$ for some p prime.

Suppose F is a field. Then $p(x) \in F[x]$ is irreducible if and only if $p(x)$ is not constant and it can not be written as product of smaller degree polynomials.

proof: $\Rightarrow$ Since $f(x)$ is irreducible $\Rightarrow f(x)$ is non constant (by def as constants are units).

$\Rightarrow$ If $f(x) = g(x)h(x)$ then if $\deg g, h < f \Rightarrow \deg g$ or $h = 0$ as unit

$\Leftarrow$ Suppose $f(x) = g(x)h(x)$, since f can not be written as a product of smaller degree polynomials in $F[x]$, $\deg g = \deg f$ or $\deg h = \deg f$

$\Rightarrow \deg g = 0$ or $\deg f = 0$, which is unit.

(Minimal polynomial and irreducibility) Suppose E is a field extension of F, $\alpha \in E$ is algebraic over F, and $p(x) \in F[x]$ is a monic polynomial. Then $p(x) = m_\alpha(x)$ if and only if $p(\alpha) = 0$ and $p(x)$ is irreducible.

Q. What can we say about ideals generated by irreducible elements & their quotient rings

* For irreducible p of $\mathbb{Z}$, $\mathbb{Z}/\langle p\rangle$ is a field.

Suppose D is an integral domain and $a, b \in D$. Then $\langle a\rangle = \langle b\rangle$ if and only if $a = bu$ for some unit u.

proof: $\langle a\rangle = \langle b\rangle \iff \exists x, y \in D$, $a = bx$ and $b = ay$, x, y are units

$\Leftarrow$ if $a = bu$ for some unit then $b = au^{-1}$. So $\langle a\rangle = \langle b\rangle$

$\Rightarrow$ if $a = bx = ayx = a(yx) \Rightarrow yx = 1 \Rightarrow x, y$ are units. ∎

Suppose A is a unital commutative ring, and $a \in A$. Then a is a unit iff $\langle a\rangle = A$.

proof: $\Rightarrow$ if a is unit then done

$\Leftarrow$ if $\langle a\rangle = A \Rightarrow 1 \in \langle a\rangle \Rightarrow a$ is unit ∎

Suppose F is unital commutative ring. Then F is a field if and only if F has exactly two distinct $\{0\}$ and F.

proof: $\Rightarrow$ If F is a field $\Rightarrow$ all elements are units, so if $a \in I$, I is ideal then by above, $I = F$.

$\Leftarrow$ Since F and $\{0\}$ are distinct $\Rightarrow 0 \notin F^{\times}$.

Suppose $a \in F \setminus \{0\}$. Consider $\langle a\rangle$. As F is only ideal $\Rightarrow \langle a\rangle = F \Rightarrow F = aF \Rightarrow 1 \in \langle a\rangle$. So a is unit. ∎

* Suppose Σ is a collection of subsets of a given set X.

$A \in \Sigma$ is maximal if and only if $\forall B \in \Sigma$, $A \subseteq B \Rightarrow B = A$.

a is irred iff $\langle a\rangle$ is maximal ideal

* Suppose D is an integral domain which is not a field and $a \in D$. Then a is irreducible in D iff $\langle a\rangle \neq D$ and for every $b \in D$,

$\langle a\rangle \subseteq \langle b\rangle \Rightarrow$ either $\langle a\rangle = \langle b\rangle$ or $\langle b\rangle = D$

proof: $\Rightarrow$ Suppose a is irreducible in D and $\langle a\rangle \subseteq \langle b\rangle$. As a is irreducible, it is not a unit. So $\langle a\rangle$ is proper ideal.

As $a \in \langle b\rangle$, $a = bc$ for some $c \in D$. Since a is irreducible, $b \in D^{\times}$ or $c \in D^{\times}$. If $b \in D^{\times} \Rightarrow \langle b\rangle = D$, if $c \in D^{\times}$

$\Rightarrow \langle a\rangle = \langle b\rangle$.

$\Leftarrow$ Say $\langle a\rangle$ is a proper ideal, $\Rightarrow a$ is not a unit.

If $a = bc$ for $b, c \in D$, then $\langle a\rangle \subseteq \langle b\rangle$ we get $\langle a\rangle = \langle b\rangle$ or $\langle b\rangle = D$.

So $a = bu$, $u \in D^{\times}$ or $b \in D^{\times}$. So a is irreducible.

* Suppose A is a unital commutative ring and $I \trianglelefteq A$. We say I is a maximal ideal if $\forall J \trianglelefteq A$, $I \subseteq J \Rightarrow I \subseteq J \Rightarrow J = I$ or $J = A$.

• So suppose D is a PID, and $a \in D$. Then

1. $\{0\}$ is maximal ideal iff D is a field
2. for $a \neq 0$, $\langle a \rangle$ is maximal ideal iff a is irreducible.

\# Suppose A is a unital commutative ring and $I \trianglelefteq A$. Then $\bar{J}$ is an ideal of A/I if and only if $\bar{J} = J/I$ for some $J \trianglelefteq A$ which contains I.

proof: $\Leftarrow$ $J/I \leq A/I$. Say $a+I \in b/I$ and $b+I \in A/I$. Since $J \trianglelefteq A \Rightarrow$ $ab \in J \Rightarrow$ $(a+I)(b+I) \in J/I$

$\Rightarrow$ Say $\bar{J}$ is an ideal of A/I and let $J := \{a \in A \mid a+I \in \bar{J}\}$

We show $\bar{J} = J/I$ and $J \trianglelefteq A$. Note $I \subseteq J$.

Say $a, a' \in J$. Then $a+I$, $a'+I \in \bar{J}$.

So $(a+I) - (a'+I) \in \bar{J} \Rightarrow (a-a') + I \in \bar{J} \Rightarrow a - a' \in J$.

For $a \in J$, $b \in A$, $a+I \in \bar{J}$, $b+I \in A/I$

$ba + I \in \bar{J} \Rightarrow ab \in J$. So J is ideal. ■

\# Suppose A is a unital commutative ring and $I \trianglelefteq A$. Then I is a maximal ideal if and only if A/I is a field.

proof: We A/I is field $\Leftrightarrow$ it has only two ideals I/I and A/I $\Leftrightarrow$ A/I has exactly two ideals A & I which contain I $\Leftrightarrow$ I is maximal ideal ■

\# D is a PID and not a field, and $a \in D$. Then $D/\langle a \rangle$ is a field iff a is irreducible in D.

proof: $D/\langle a \rangle$ is a field $\Leftrightarrow$ $\langle a \rangle$ is a maximal ideal $\Leftrightarrow$ Since D is not a field, $\langle a \rangle$ is maximal iff irreducible ■

\# Suppose E is field extension of F, and $\alpha \in E$ is algebraic over F.

Then $F[\alpha]$ is a field.

proof: We $F[\alpha] \cong F[x]/\langle m_{\alpha,F}(x) \rangle$.

We know $m_{\alpha,F}(x)$ is irreducible in $F[x]$ and $F[x]$ is PID and not a field. So above corollary proves that $F[\alpha]$ is a field.

\# Suppose $\alpha \in \mathbb{C}$ is zero of $x^3 - x + 1$. Express $\frac{1}{\alpha}$, $\frac{1}{\alpha+1}$, $(\alpha^2+1)^{-1}$ in terms of $a_0 + a_1\alpha + a_2\alpha^2$ for $a_i \in \mathbb{Q}$

solution: So essentially α is algebraic over $\mathbb{Q}$.

$$\mathbb{Q}[\alpha] \cong \mathbb{Q}[x]/\langle x^3 - x + 1\rangle$$

$\alpha(\alpha^2-1) \Rightarrow \alpha(\alpha+1)(\alpha+1)$

So $\mathbb{Q}[\alpha]$ is a field. And $\alpha^3 - \alpha + 1 = 0$ $\quad \alpha^3 - \alpha = -1$

$\alpha^3 + 1 \quad\quad \alpha(\alpha^2 - 1)$

So $\frac{1}{\alpha} \in \mathbb{Q}[\alpha]$ as $\quad \alpha(-\alpha^2+1) = -\alpha^3 + 1 = 1 \Rightarrow -\alpha^2 + 1 = \frac{1}{\alpha}$

$\frac{1}{\alpha+1} \in \mathbb{Q}[\alpha]$ as $\quad (\alpha+1)(-\alpha(\alpha-1)) = 1 \Rightarrow -\alpha(\alpha-1) = \frac{1}{\alpha+1}$

We use extended euclid algorithm.

$f = x^3 - x + 1 \quad = \langle 1, 0\rangle$

$g = x^2 + 1 \quad = \langle 0, 1\rangle$

$1 \cdot f - x \cdot g = x^3 - x + 1 - (x^3 + x) = -2x + 1 \quad \langle 1, -x\rangle$

$x + 2 = 2x^2 + 2 - 2x^2 + x = 2 \cdot \langle 0, 1\rangle + x\langle 1, -x\rangle = \langle 0, 2\rangle + \langle x, -x^2\rangle = \langle x, -x^2+2\rangle$

$-2x + 1 + 2(x+2) = 5$

$\Rightarrow \langle 1, -x\rangle + 2\langle x, -x^2+2\rangle = 5$

$\Rightarrow \frac{1}{5}\langle 1, -x\rangle + \frac{1}{5}\langle 2x, -2x^2+4\rangle = 1$

$\Rightarrow \left(-\frac{x}{5} - \frac{2x^2}{5} + \frac{4}{5}\right)(x^2+1) = 1$

LECTURE 10

\# Suppose F is a field and $f(x) \in F[x]$

1. if $\deg f = 1$, then f is irreducible

2. if $\deg f \geq 2$ and f has a zero in F, then f is not irreducible

3. suppose $\deg f = 2$ or 3. Then f is irreducible in $F[x]$ iff f does not have a zero in F.

proof: (1) suppose $\deg f = 1 \Rightarrow$ if $f = gh \Rightarrow 1 = \deg g + \deg h \Rightarrow$ both $\deg \geq 1$ not possible

(2) $\Rightarrow$ If a is root of $f(x)$. Then $(x-a) \mid f(x) \Rightarrow g(x)(x-a) = f(x)$. Hence $\deg f - 1 < \deg f$ & $\deg(x-a) < \deg f$

So $f(x)$ is not irreducible.

(3) Suppose $\deg f = g(x)h(x)$ and $\deg g, \deg h < \deg f \leq 3$.

$\deg f = \deg g + \deg h \Rightarrow \deg g = 1$ or $\deg h = 1$

WLOG say $g(x) = a_0 + a_1 x \Rightarrow -a_0 a_1^{-1} \in F$ is a zero. ■

\# 1. $f(x) = x^3 - x + 1$ is irreducible in $\mathbb{Z}_3[x]$

2. $\mathbb{Z}_3[x]/\langle f(x)\rangle$ is a field of order 27

proof: (i) Since $\deg f = 3$, f is irreducible in $\mathbb{Z}_3[x]$ iff it does not have a zero in $\mathbb{Z}_3$. Checking $x = 1, -1, 0$, we get that there is no zero.

(ii) $\mathbb{Z}_3/\langle f(x)\rangle = \mathbb{Z}_3/\langle x^3 - x + 1\rangle \Rightarrow \mathbb{Z}_3/\langle x^3-x+1\rangle$ is field as $\langle x^3-x+1\rangle$ is a maximal ideal $\Rightarrow \mathbb{Z}_3[x]/\langle f(x)\rangle$ is field as $f(x)$ is irred and $\langle f(x)\rangle$ is maximal ideal

So any element $\in \mathbb{Z}_3[x]/\langle f(x)\rangle$ can be uniquely written as $r(x) + \langle f(x)\rangle$ with polynomial with deg at most 2. Note that there are 27 poly ■

\# (Rational root criterion) Suppose $f(x) := a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$.

$a_0 \neq 0$ and $a_n \neq 0$. If $f(\frac{b}{c}) = 0$ & $b, c \in \mathbb{Z}$, $\gcd(b,c) = 1$ then $b \mid a_0$ and $c \mid a_n$

proof: Since $f(\frac{b}{c}) = 0 \Rightarrow a_n\left(\frac{b}{c}\right)^n + a_{n-1}\frac{b^{n-1}}{c^{n-1}} + \cdots + a_0 = 0$

$\Rightarrow a_n b^n + a_{n-1} b^{n-1} c + \cdots + a_0 c^n = 0$

$\Rightarrow c \mid a_n$

Similarly $b \mid a_0$.

\# Suppose $f(x) \in \mathbb{Z}[x]$ is a monic polynomial. Then every rational zero of f is an integer which divides $f(0)$.

proof: Suppose $\frac{b}{c}$ is a zero of f and $\gcd(b,c) = 1$, $c \mid 1 \Rightarrow c = \pm 1$

$\Rightarrow \frac{b}{c} = \pm b \in \mathbb{Z} \Rightarrow b \mid a_0$ ■

Suppose $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + 1 \in \mathbb{Z}[x]$. Prove that f has a rational zero if and only if $f(1)=0$ or $f(-1)=0$

proof: Since f is monic integer polynomial. So every rational divisor is integer and $\mid f(0)=1$ $\Rightarrow$ it is ± 1. ■

Suppose A and B are unital commutative rings and $c: A \to B$ is a ring homomorphism. Then

1. $c: A[x] \to B[x]$, $c\left(\sum_{i=0}^{n} a_i x^i\right) = \sum_{i=0}^{n} c(a_i) x^i$ a ring homomorphism.

2. For $a \in A$, $b \in B$,

$\phi_a: A[x] \to A$, $\phi_a(f(x)) := f(a)$

$\phi_b: B[x] \to B$, $\phi_b(g(x)) := g(b)$

be the evaluation maps. Then for every $a \in A$, we have

$$c(\phi_a(f(x))) = \phi_{c(a)}(c(f(x)))$$

Proof: double ■

* So suppose $c: A \to B$ is a ring homomorphism and $f(x) \in A[x]$. If $c(f(x))$ doesn't have a zero in B, then $f(x)$ does not have zero in A.

$f(a)=0$, $a \in A$, $f(x) \in A[x] \Rightarrow c(f(x))\big|_a = c(f(a)) = c(0) = 0$ ■

Suppose $f(x) \in \mathbb{Z}[x]$ is a monic polynomial. If $f(x)$ does not a zero in $\mathbb{Z}_n$, then $f(x)$ does not have a zero in $\mathbb{Q}$

proof: suppose $f(x)$ has a zero in $\mathbb{Q}$. Since $f(x) \in \mathbb{Z}[x]$ is monic $\Rightarrow$ $f(x)$ has zero in $\mathbb{Z}$, then consider the residue map and done ■

Note: $a^{c_n p^n + c_{n-1}p^{n-1} + \cdots + c_0} = a^{c_n + \cdots + c_0}$ in $\mathbb{Z}_p$

Suppose p is prime. Prove that $f(x) = x^{p^2} + px^{p^2-p} - x + (2p+1)$ doesn't have a rational zero.

proof: let $x^{p^2} + px^{p(p-1)} - x + 2p+1$ be the polynomial.

Working in $\mathbb{Z}_p[x]$, we get $x^{p^2} + px^{p(p-1)} - x + 2p+1 = x + px^{p-1} - x + 2p+1 = 2p+1 \equiv 1 \bmod p$ $\forall$. So doesn't have root in $\mathbb{Z}_p$

So irreducible ■

LECTURE 11

$2x$ is irreducible in $\mathbb{Q}[x]$, but it is not irreducible in $\mathbb{Z}[x]$

proof: • $2x$ is irreducible in $\mathbb{Q}[x]$ as every degree 1 polynomial with cf in Field is irreducible.

• $2x = 2 \cdot x$ both are not units. ■

↳ if gcd of cfs is not 1, then $f(x)$ cannot be irreducible in $\mathbb{Z}[x]$

* Suppose $f(x) := a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$ is a non-zero polynomial. The content of f is the greatest common divisor of the coefficients $a_0, \ldots, a_n$ and we denote it by $\alpha(f)$.

1. $\alpha(2x^2-6)=2$ and $\alpha(2x^2-5x+3)=1$

2. The content of a monic polynomial is 1.

Let n be a positive integer $c_n: \mathbb{Z}[x] \to \mathbb{Z}_n[x]$ be the modulo residue map, $a \in \mathbb{Z} \setminus \{0\}$, and suppose $f(x), g(x) \in \mathbb{Z}[x]$ are two non-zero polynomials. Then

1. $\alpha(a f(x)) = |a| \alpha(f)$
2. If $\alpha(f) = d$, then $\frac{1}{d} f(x) \in \mathbb{Z}[x]$ and $\alpha\left(\frac{1}{d} f(x)\right) = 1$
3. $n \mid \alpha(f)$ iff $f \in \ker c_n$.

proof: • $\gcd(aa_0, \cdots, aa_m) = |a| \gcd(a_0, \cdots, a_m)$

• $\gcd(a_0, \ldots, a_m) \Rightarrow \gcd\left(\frac{a_0}{d}, \ldots, \frac{a_m}{d}\right) = 1$

• $n \mid a_0, \cdots, n \mid a_m \Leftrightarrow n \mid \gcd(a_0, \ldots, a_m)$

* $f(x) \in \mathbb{Z}[x]$ is a primitive polynomial if $\alpha(f) = 1$

↳ $f(x) = \alpha(f) \bar{f}(x)$

Every non-zero polynomial $f(x) \in \mathbb{Q}[x]$, there are unique positive rational number q and primitive polynomial $\bar{f}$ such that $f(x) = q \bar{f}(x)$. Moreover for $f(x) \in \mathbb{Z}[x]$, $\alpha(f) = q$.

proof: (Existence) After multiplying by the common denominator n of the coefficients, we get $\tilde{f}(x) := n f(x)$.

so $\tilde{f}(x) = \alpha(\tilde{f}) \bar{f}(x) \Rightarrow f(x) = \dfrac{\alpha(\tilde{f}) \bar{f}(x)}{n}$.

(Uniqueness) Suppose $q_1, q_2 \in \mathbb{Q}$ are positive integers st $f(x) = q_1 \bar{f}_1(x) = q_2 \bar{f}_2(x)$.

let n be smallest integer st $mq_i \in \mathbb{Z}$. So $\underbrace{mq_1}_{= n_1} \bar{f}_1(x) = \underbrace{mq_2}_{= n_2} \bar{f}_2(x)$.

So $n_1 \bar{f}_1(x) = n_2 \bar{f}_2(x) \Rightarrow \alpha(n_1 \bar{f}_1(x)) = \alpha(n_2 \bar{f}_2(x)) \Rightarrow n_1 = n_2$. ■

* The unique rational number given in above is called content of f and it is denoted by $\alpha(f)$.

For every non-zero $f(x) \in \mathbb{Q}[x]$ and $a \in \mathbb{Q} \setminus \{0\}$, we have $\alpha(af(x)) = |a| \alpha(f(x))$

proof: We know that there is a primitive polynomial $\bar{f}(x)$ such that $f(x) = \alpha(f)\bar{f}(x)$. Hence $af(x) = a\,\alpha(f)\bar{f}(x)$.

As $\bar{f}(x)$ is primitive, we get that $\alpha(af(x)) = |a|\,\alpha(f)$. ■

(Gauss lemma) If f and g are two primitive polynomial then fg is also primitive.

proof: Suppose $\alpha(fg) \neq 1 \Rightarrow \exists$ prime $p \mid \alpha(fg)$. So $c_p(fg) = 0 \Rightarrow c_p(f) \cdot c_p(g) = 0 \Rightarrow c_p(f) = 0$ or $c_p(g) \Rightarrow p \mid \alpha(f)$ or $p \mid \alpha(g)$.

(Gauss lemma) Suppose f and g are two non-zero polynomials in $\mathbb{Q}[x]$. Then

$$\alpha(fg) = \alpha(f)\,\alpha(g)$$

proof: We $f(x) = \alpha(f)\,\bar{f}(x)$

$$g(x) = \alpha(g)\,\bar{g}(x)$$

$$\Rightarrow f(x)g(x) = \alpha(f)\,\bar{f}(x)\,\alpha(g)\,\bar{g}(x)$$

$$\Rightarrow \alpha(f(x)\,g(x)) = \alpha(\alpha(f)\,\bar{f}(x)\,\alpha(g)\,\bar{g}(x))$$

$$= \alpha(f)\alpha(g)\,\alpha(\bar{f}(x))\,\alpha(\bar{g}(x))$$

$$= \alpha(f)\alpha(g) \quad ■$$

Suppose $f(x)$ is a primitive polynomial and $f(x) = \prod_{i=1}^{n} g_i(x)$ for some $g_i \in \mathbb{Q}[x]$. Then there are primitive polynomials $\bar{g}_i(x)$ such that

$g_i(x) = \alpha(g_i)\,\bar{g}_i(x)$, $\prod_{i=1}^{n} \alpha(g_i) = 1$ and $f(x)$ and $f(x) = \prod_{i=1}^{n} \bar{g}_i(x)$

proof: $1 = \alpha(f) = \alpha\left(\prod_{i=1}^{n} g_i\right) = \prod_{i=1}^{n} \alpha(g_i)$.

$$\prod_{i=1}^{n} \bar{g}_i(x) = \prod_{i=1}^{n} \left(\alpha(g_i)^{-1} g_i(x)\right) = \left(\prod_{i=1}^{n} \alpha(g_i)\right)^{-1} \prod_{i=1}^{n} g_i(x) = f(x) \quad ■$$

Suppose $f(x)$ is primitive and $\deg f \geq 1$. Then $f(x)$ is irreducible in $\mathbb{Z}[x]$ iff it is irreducible in $\mathbb{Q}[x]$.

proof: Suppose $f(x)$ is not irreducible in $\mathbb{Q}[x]$. As $\deg f \geq 1 \Rightarrow \exists\, g_1(x), g_2(x)$ with $\deg \geq 1$ st $f(x) = g_1(x) g_2(x)$. Since $\alpha(f) = 1$

$\Rightarrow f(x) = \overline{g}_1(x)\overline{g}_2(x)$ & $\deg \overline{g}_j = \deg g_j$.

So $f(x)$ is not irreducible in $\mathbb{Z}[x]$.

Say $f(x)$ is not irreducible in $\mathbb{Z}[x]$. Since $\deg f \geq 1$, it is not unit.

So $f(x) = h_1(x) h_2(x)$. Note both h_j $\deg \geq 1$ as if constant (and not unit) then $\alpha(f) \neq 1$. So $f(x)$ is not irred. in $\mathbb{Q}[x]$ ■

(mod-p irreducibility criterion) Suppose $f(x) \in \mathbb{Q}[x]$ is primitive, p is prime which doesnt divide the leading cf of $f(x)$ and $c_p : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ is the modulo p residue map

If $c_p(f(x))$ is irreducible in $\mathbb{Z}_p[x]$, then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

proof: Say $f(x)$ is not irreducible in $\mathbb{Q}[x]$. Hence $f(x)$ is either const or two smaller degree. Since it is irreducible

in $\mathbb{Z}_p[x] \Rightarrow c_p(f)$ is not constant. $\Rightarrow f(x)$ not const

$\Rightarrow \exists\, g_i(x) \in \mathbb{Q}[x]$ st $f(x) = g_1(x) g_2(x)$, g_i non const. As $f(x)$ is primitive $\Rightarrow f(x) = \overline{g}_1(x)\overline{g}_2(x) \Rightarrow$ Since $p \nmid$ leading cf of f

$\Rightarrow p \nmid$ leading cf of $\overline{g}_i$.

So $\deg c_p(\overline{g}_i) = \deg \overline{g}_i = \deg g_i$

So $c_p(f) = c_p(\overline{g}_1) c_p(\overline{g}_2)$

So in $\mathbb{Z}_p[x]$, $c_p(f)$ is not irred. ■

LECTURE 12

Prove that $f(x)=x^7-7x^5+21x^3+14x^2-8x+11$ is irreducible in $\mathbb{Q}[x]$.

proof: Note $f(x)$ in $\mathbb{Z}_7[x]$ is x^7-x+4. Hence irreducible in $\mathbb{Z}_7[x]$. Note $f(x)$ is primitive and leading of is not a multiple of 7. So by the mod-p- criterion, $f(x)$ is irreducible in $\mathbb{Q}[x]$.

1. Prove that x^4+x+1 is irreducible in $\mathbb{Z}_2[x]$

2. Prove that $f(x):=5x^4+2x^3\cdot 2020x^2+2021x+1$ is irreducible in $\mathbb{Q}[x]$

proof: (1) In $\mathbb{Z}_2$, $a^4+a+1=1$ $\forall a\in\mathbb{Z}_2$. So no one degree polynomial divides. Note there are 2^2 degree 2 polynomials in $\mathbb{Z}_2[x]$.

x^2, x^2+1, x^2+x, x^2+x+1 and brute force it.

(2) Note that $f(x)$ is primitive. In $\mathbb{Z}_2[x]$,

$f(x)=x^4+x+1$ which is irreducible in $\mathbb{Z}_2[x]$

So irreducible in $\mathbb{Q}[x]$.

(Eisenstein's irreducibility criterion) let $f(x)=a_nx^n+\cdots\cdots+a_1x+a_0\in\mathbb{Z}[x]$ and p be prime. Suppose $p\nmid a_n$, $p\mid a_{n-1},\dots,p\mid a_0$ and $p^2\nmid a_0$. Then $f(x)$ is irreducible in $\mathbb{Q}[x]$

proof: Suppose $\exists\, g_1,g_2\in\mathbb{Q}[x]$ st $f(x)=g_1(x)g_2(x)$. let $\bar{g}_i(x)$ be the primitive polynomial such that $g_i(x)=\alpha(g_i)\bar{g}_i(x)$

So $\alpha(f)=\alpha(g_1g_2)=\alpha(g_1)\alpha(g_2)$

$\Rightarrow f(x)=\alpha(f)\,\bar{g}_1(x)\bar{g}_2(x)$

Note that the leading of a_n imply the $p\nmid$ the leading of of $\bar{g}_1(x)$ & $\bar{g}_2(x)$

Also $c_p(f)=c_p(\alpha(f))c_p(\bar{g}_1)c_p(\bar{g}_2)$

Note $\deg(c_p(\bar{g}_i))=\deg(\bar{g}_i)>0$

lemma: Suppose F is a field and $\bar{g}_1,\bar{g}_2\in F[x]$ are two non-constant polynomials such that $\bar{g}_1(x)\bar{g}_2(x)=cx^n$ for some $c\in F^\times$.

Then $\bar{g}_1(0)=\bar{g}_2(0)=0$

proof: Suppose $\bar{g}_1(x) = b_r x^r + \cdots + b_1 x + b_0$

$\bar{g}_2(x) = c_s x^s + \cdots + c_1 x + c_0$

$b_i, c_j \in F$, $b_r, c_s \in F^\times$

So $b_r c_s x^{r+s}$ is the largest term.

by comparing cfs, $c_0 b_0 = 0 \Rightarrow$ either c_0 or b_0 is 0. WLOG $c_0 = 0$. Then say s' is the smallest st $c_{s'}$ is nonzero.

and let r' be the smallest index st $b_{r'} \neq 0$.

Note that cf $x^{r'+s'} = c_{s'} b_{r'} = 0$ if $r' \neq r$ or $s' \neq s$. Contradiction.

So $\bar{g}_1(0) = 0$, $\bar{g}_2(0) = 0$. ∎

Using the above lemma,

$c_p(\bar{g}_1)(0) = c_p(\bar{g}_2)(0) = 0$

$\Rightarrow p \mid \bar{g}_1(0)$, $p \mid \bar{g}_2(0)$

$\Rightarrow p^2 \mid \bar{g}_1(0)\,\bar{g}_2(0)$

$a_0 = f(0) = \alpha(f)\,\bar{g}_1(0)\,\bar{g}_2(0)$

$\Rightarrow p^2 \mid a_0$. NP. ∎

\# Prove that $f(x) = \frac{5}{2}x^6 - \frac{4}{3}x^3 + 7x - \frac{3}{11}$ is irreducible in $\mathbb{Q}[x]$

proof: $f(x) = \frac{5}{2}x^6 - \frac{4}{3}x^3 + 7x - \frac{3}{11}$

$f(x)$ is primitive form is $(33\times5)x^6 - (22\times4)x^3 + (66\times7)x - (6\times3)$

We work in $\mathbb{Z}_2$ and use eisenstein.

\# Suppose p is prime. Then $f(x) = x^{p-1} + x^{p-2} + \cdots + 1$ is irreducible in $\mathbb{Q}[x]$.

proof: $f(x)(x-1) = (x^{p-1} + x^{p-2} + \cdots + 1)(x-1) = x^p - 1$

So $f(x) = \frac{x^p - 1}{x-1}$

let $g(y) := f(y+1)$

$g(y) = \frac{(y+1)^p - 1}{y} = y^{p-1} + \binom{p}{p-1} y^{p-2} + \cdots + \binom{p}{1}$

Note by eisenstein criterion, we get $g(y)$ is irreducible in $\mathbb{Q}[y] \Rightarrow f(x)$ is irreducible in $\mathbb{Q}[x]$. ∎

existence

* An integral domain D is called Unique factorization Domain (UFD) if every non-zero unit element of D can be written as a product of irreducible elements and the irreducible factors are unique up to reordering and multiplying by a unit.

uniqueness

* The ring of integers is a UFD.

* Suppose D is an ID.

let $d \in D$.

1. If d is irreducible, we are done
2. If not, $\exists\ d_1, d_1' \in D$ st $d = d_1 d_1'$
3. Repeat this process for each one of the factors

* Saying that d is multiple of d_1 $\Rightarrow$ $\langle d \rangle \subseteq \langle d_1 \rangle$

Note $\langle d \rangle = \langle d_1 \rangle$ iff $d = u d_1$, $u \in D^\times$.

So we get chain of (principal) ideals:

$$\langle d \rangle \subsetneq \langle d_1 \rangle \subsetneq \langle d_2 \rangle \cdots$$

* A ring A is called Noetherian if there is no infinite ascending chain of ideals

So if D is Noetherian Integral domain. Then every non-zero element of D can be written as a product of irreducible elements of D.

* Suppose A is a unital commutative ring. Then A is Noetherian iff every ideal of A is finited generated.

proof: $\Rightarrow$ Suppose there is an ideal I which is not finitely generated.

So consider the elements of I (we can get it) st

$$\langle a_1 \rangle \subsetneq \langle a_1, a_2 \rangle \subsetneq \cdots$$

$\Leftarrow$ Say every ideal of A is finitely generated.

let $I_1 \subsetneq I_2 \subsetneq \cdots$ be an ascending chain of ideals. let $I = \bigcup_{i=1}^{\infty} I_i$.

Note that I is an ideal as $i \in I$, $a \in A$ then $ia \in I$ as $i \in I_i$, $ai \in I_i$.

if $a \in I_i$, $a' \in I_{i'}$. WLOG $I_i \subseteq I_{i'}$ $\Rightarrow$ $a' - a \in I_{i'}$ $\Rightarrow$ $a' - a \in A$.

Since I is finitely generated, the chain has to end. ■

D is a PID $\Rightarrow$ D is Noetherian

LECTURE 13

* Suppose $p_1, p_2, \cdots, p_m$ and $q_1, \cdots, q_n$ are irreducible elements of D.

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

  then $p_1 = u_1 q_{i_1}, p_2 = u_2 q_{i_2}, \cdots$ for some $u_i \in D^\times$.

  So $1 \to i_1, \cdots, m \to i_m$ so in particular $m = n$.

* Suppose D is an integral domain

  1. For $a, b \in D$, we say $a \mid b$ if $\exists\, d \in D$ st $b = ad$
  2. A non-zero, non unit element p of D is called prime when for every $a, b \in D$ if $p \mid ab \Rightarrow p \mid a$ or $p \mid b$

Let D be an integral domain. Suppose every non-zero unit element of D can be written as a product of irreducible elements. Then D is a UFD iff every irreducible element is prime

Idea of proof: $\Rightarrow$ Say p is irredubile. Say $p \mid ab$. Then $ab = p \cdot d$ for some d. decompose a, b, d into irreducible factors.

So by uniqueness of UFD, there should be a factor p in the expansion of ab. So $p \mid a$ or $p \mid b$.

$\Leftarrow$ We only need to show uniqueness. if $p_1 \cdots p_m = q_1 \cdots q_n$, where p_i, q_i are primes

$\Rightarrow p_1 \mid q_1 \cdots q_n \Rightarrow p_1 \mid q_i$. As q_i is irreducible $\Rightarrow p_1 = q_i$. So cancel, use induction. ■

Suppose D is an integral domain and $a, b \in D$

1. $a \mid b$ iff $b \in \langle a \rangle$ iff $\langle b \rangle \subseteq \langle a \rangle$
2. $a \mid b$ & $b \mid a$ iff $a = bu$ for some unit u

proof: · $a \mid b \Leftrightarrow \exists c$ st $b = ac \Leftrightarrow \langle a \rangle = \{ar \mid r \in D\}$, $b \in \langle a \rangle \Leftrightarrow \langle b \rangle \subseteq \langle a \rangle$.

· $a \mid b$ & $b \mid a \Rightarrow b = ac$ & $a = bd \Rightarrow a = bd = acd \Rightarrow c, d$ are units. ■

(1) $\langle p \rangle$ is a nonzero proper ideal
(2) if $ab \in \langle p \rangle$, then either $a \in \langle p \rangle$ or $b \in \langle p \rangle$.

* Suppose A is a unital commutative ring and I is an ideal of A. We say I is a prime ideal if

  (1) I is proper $(I \neq A)$

  (2) if $ab \in I$ for some $a, b \in D$, then either $a \in I$ or $b \in I$

Suppose D is an integral domain $p \in D$. Then p is a prime element iff $p \neq 0$ and $\langle p \rangle$ is a prime ideal.

Suppose A is a unital commutative ring and I is an ideal of A. Then I is a prime ideal iff A/I is an integral domain.

proof: $\Leftarrow$ let I be a prime ideal.

So say $(a+I)(b+I) = (0+I)$

$\Rightarrow ab \in I \Rightarrow a \in I$ or $b \in I \Rightarrow a+I = 0+I$ or $b+I = 0+I$.

So A/I is ID.

$\Leftarrow$ If A/I is ID, then $(a+I)(b+I) = 0+I$

$\Rightarrow a+I$ or $b+I = 0+I$

$\Rightarrow a \in I$ or $b \in I$

So if $ab \in I \Rightarrow a \in I$ or $b \in I$ ■

Suppose A is unital commutative ring and I is an ideal of A. If I is a maximal ideal, then I is a prime ideal.

If I is maximal ideal $\Rightarrow A/I$ is Field $\Rightarrow A/I$ is ID $\Rightarrow I$ is a prime ideal.

Suppose D is a PID. Then every irreducible element of D is prime.

proof: Since D is a PID, every ideal is generated by one element. let p be irreducible in D. $\langle p \rangle$ is maximal ideal. So $\langle p \rangle$ is prime ideal. So it is prime. ■

Suppose D is an integral domain and $p \in D$. If p is a prime element, then p is irreducible.

proof: let p be prime. If $p = ab \Rightarrow p \mid ab \Rightarrow p \mid a$ or $p \mid b \Rightarrow a = pa'$ or $pb' = b \Rightarrow a = pa' = aba' \Rightarrow ba' = 1$. So b is unit.

Suppose D is a PID. Then

1. An element $d \in D$ is irreducible iff it is prime.

2. D is a UFD

proof: Since D is ID, every prime is irreducible. Since D is PID, every irreducible element of D is prime.

We know that D is a PID, so D is Noether, so any element can be written as irreducible. And it is unique as irreducible = prime here ■

So $\mathbb{Z}, F[x], \mathbb{Z}[i], \mathbb{Z}[\omega]$ are UFD.

* The ring $\mathbb{Z}[\sqrt{-6}]$ is not a UFD.

$\longrightarrow$ let $N : \mathbb{Z}[\sqrt{-6}] : \mathbb{Z}$, $N(z) = |z|^2$

not N is multiplicative.

Note $z \in \mathbb{Z}[\sqrt{-6}]$ is a unit iff $N(z) = 1$

$\sqrt{-6}$ is irreducible. Note $\sqrt{-6}$ is not unit. If $\sqrt{-6} = xy$ then $N(\sqrt{-6}) = xy$. Then $6 = N(x)N(y)$

But there is no x st $N(x) = 2$ as $a^2 + 6b^2 = 2$ as $a^2 + 6b^2 \geq 6$ if $b \neq 0$.

$\sqrt{-6}$ is not prime. As $\sqrt{-6} \mid 2 \times 3$. But $\sqrt{-6} \nmid 2$ & $\sqrt{-6} \nmid 3$ as $N(\sqrt{-6}) = 6$, $N(2) = 4$, $N(3) = 9$. So $\mathbb{Z}[\sqrt{-6}]$ is not UFD.