Basic Ring Theory :-

1) **Def$^{\underline{n}}$ of Ring :-** $(R,+,\cdot)$ s.t $(R,+)\in Ab$, $(R,\cdot)\in$ Monoid
$a(b+c) = ab+ac$
$(a+b)c = ac+bc$

2) **Def$^{\underline{n}}$ of Unit :-** $u\in R$ is unit if $\exists\, v\in R$ s.t $uv=1$ $\qquad \mathbb{Z}\ \{+1,-1\}$

3) **Irreducible vs Prime :-**

$R[x] := \{a_nx^n+\dots+a_1x+a_0 : a_i\in R\}$

$F[x] := \{a_nx^n+\dots+a_1x+a_0 : a_i\in F\}$

4) **Polynomial Rings :-**

Given a field F, $F[x]$ behaves similarly "like" $\mathbb{Z}$, most importantly one can do long division among polynomials.

a) **Division algorithm for Polynomials :-**

Given a polynomial $a(x)$ and $b(x)\in F[x]$, $\exists$ unique polynomials $q(x)$ and $r(x)$ s.t

$$b(x) = a(x)\,q(x) + r(x)\ ; \quad r(x)=0 \ \text{or}\ 0\leq \deg(r) < \deg(q)$$

(See the resemblence with integers) $\qquad 0\leq$ remainder $<$ |divisor|

$a(x)\mid b(x) \iff$ remainder $0\in F[x]$

b) So polynomials behave like integer.

Now prove the following for integers

i) Let an integer p have no other divisor but ± 1 and $\pm p$. Suppose $p\mid ab$ for some $a,b\in\mathbb{Z}$. Prove that p divides at least one of a and b

ii) Let $p\in\mathbb{Z}$. For any $a\in\mathbb{Z}, b\in\mathbb{Z}$, if $p\mid ab$, then $p\mid a$ or $p\mid b$ or both. Prove that p has no divisor other than 1 and p

$R[x]$ is also a ring!

$$(a_n x^n + \dots + a_1 x + a_0) + (b_m x^m + \dots + b_n x^n + \dots + b_1 x + b_0)$$

$$=$$

$$a_0 b_0 + (a_1 b_0 + a_0 b_1)x + (a_2 b_0 + a_1 b_1 + a_0 b_2)x^2 + \dots$$

$0 \in R[x]$ $\quad$ $1 \in R[x] \rightarrow$

$\neq$ $\quad$ $\neq$

$0 \in R$ $\quad$ $1 \in R$

$1 \in \mathbb{Z}$

$1 \in \mathbb{Z}[x]$

$a_0 = 1$

$$R[x] := \{(a_0, a_1, \dots, a_n, 0, 0, 0, \dots)\}$$

set of all seq^{n} in R s.t only finitely many of element are nonzero

$$\mathbb{Z}[x] := \{(1, 2, 3, 0, 0, \dots, 0 \dots), (1, 1, 0, 2, 0, 0, \dots 0)\}$$

$3x^2 + 2x + 1$ $\quad$ $2x^3 + x^2 + 1$

$$(a_0, a_1, a_2, \dots, a_n, 0, 0, 0, \dots) \longrightarrow a_n x^n + \dots + a_1 x + a_0$$

$$a \neq (a, 0, 0, 0, \dots, 0, \dots)$$

$1 \in R[x]$ $\quad$ $1 \in R$ $\quad$ $2 \in \mathbb{Z} \neq 2 \in \mathbb{Z}[x]$

$$(1, 0, 0, \dots, 0, \dots)$$

$$\boxed{(a, 0, \dots, 0) = \begin{cases} 0 & \text{if } a \neq 0 \\ \infty & \text{if } a = 0 \end{cases}}$$

1

$F[x]$ $\mathbb{Z}$

i) $p | ab$. Let $p \nmid b$. To show $p | a$

$p \nmid b \Rightarrow b = pk_1 + r_1$, $0 < r_1 < |p|$ (let $p > 0$)

$\Rightarrow ab = apk_1 + ar_1$

$\Rightarrow p | ar_1$

$(r_1, p) = 1 \Rightarrow p | a$

$bx + py = 1$

$\Rightarrow abx + apy = a \Rightarrow p | a$

ii) $p = cq$ where $|c| \neq 1$, & $|q| \neq 1$

$\Rightarrow p | cq \Rightarrow p | c$ or $p | q$

$\Rightarrow |c| \geq |p|$ or $|q| \geq |p|$

but $|p| = |cq| = |c| \cdot |q| > |c|$

and $|p| > |q|$

-5 5

$5 = (-1)(-5)$

i) Let $p(x) \in F[x]$ be a polynomial having no other factors but units

$F[x]$ :: = { nonzero constants } $\{1, 2, 3 \ldots \frac{1}{2} \frac{1}{3}$

$\mathbb{R}[x]$

$\in \mathbb{R}[x]$

$$2x^2 + 3x + 1 = 2\left(x^2 + \frac{3}{2}x + \frac{1}{2}\right)$$

If $a = ub$ where u is a unit, then a is "an associate" of b

i) $\left\{ p(x) \in F[x] \text{ having no factor other than units or associates of itself} \right\}$

c. p(x)

$$\Updownarrow$$

$$\left\{ p(x) = a(x)\, b(x) \Leftarrow a(x) \text{ or } b(x) \text{ is unit} \right\}$$

Then $p(x) \mid q(x) \cdot r(x) \Rightarrow p(x) \mid q(x)$ or $p(x) \mid r(x)$

$\mathbb{Z}$, $F[x]$

Def$^{\underline{n}}$:- Let R be a ring.

i) An element $r \in R$ s.t. $r \neq 0$ and r not a unit is "irreducible" if

$$r = uv \Rightarrow u \text{ or } v \text{ are unit}$$

ii) An element $p \in R$ (p nonunit) is "prime" if for any $a \in R, b \in R$ if $p \mid ab$ then $p \mid a$ or $p \mid b$

$x \mid y$ in R iff $y = xz$ for some $z \in R$

$$\mathbb{Z}[\sqrt{-5}] := \{ a + b\sqrt{-5} : a \in \mathbb{Z}, b \in \mathbb{Z} \}$$

$2 \in \mathbb{Z}[\sqrt{-5}]$ 2 irred.

$2 \mid (1+\sqrt{-5})(1-\sqrt{-5})$ $2 \mid 6$ in $\mathbb{Z}[\sqrt{-5}]$

$$\underbrace{(1+\sqrt{-5})(1-\sqrt{-5})}_{6}$$