Abstract Algebra : Ring Theory.

Yashas.N

0 symbols used

$_s|_t$ $\rightarrow$ such that.

1 Basic Definitions

Ring R : is a set together with two binary operations $+$ and $\times$ (addition and multiplication) with properties :
- $(R, +)$ is an abelian group
- $\times$ is associative (i.e. $a \times (b \times c) = (a \times b) \times c$)
- $\times$ distributes over $+$ (i.e. $(a + b) \times c = (a \times c) + (b \times c)$).

if R is commutative w.r.t. $\times$ then R is a **Commutative ring**.

Additive identity in R is denoted by 0.

R is said to have identity (1) if there is a multiplicative identity in R
i.e. $\exists 1 \in R\ _s|_t\ 1 \times a = a \times 1 = a\ \forall a \in R$.

now for $a \in R$ additive inverse of a is denoted by $-a$ and multiplicative inverse (if exists in R) by a^{-1}.

Division Ring (or skew field) D

is ring with identity 1, $1 \neq 0$ and for a element $a \in R$ not equal to 0 there exists $b \in R\ _s|_t\ ab = ba = 1$. i.e. $\forall 0 \neq a \in R\ a^{-1} \in R$.

for a ring R is a non zero $a \in R$ is a **Zero Divisor** if there is non zero $b \in R$ such that $ab = 0$ or $ba = 0$.

for a ring R with $1 : u \in R$ is a **unit** in R if it has multiplicative inverse in R

Integral domain I

is a commutative ring with identity $1 \neq 0$ having no zero divisors.

Field F

is a commutative ring with identity in which any non zero element is unit i.e. $0 \neq a \in F \implies a^{-1} \in F$. or a commutative Division ring.

Subring S of ring R is subgroup of R which is in itself a ring with same operations i.e. S is subring of R if $(S, +)$ is subgroup of $(R, +)$ and S is closed under $\times$.
(i.e. $a, b \in S \implies ab \in S$)

Center of a ring R is set $\{z \in R\ _s|_t\ zr = rz \forall r \in R\}$ i.e. all the elements that commute in R. (multiplicatively.)

$a \in R$ commutative ring is **nilpotent** if $a^m = 0$ for some $m \in \mathbb{Z}^+$

$a \in R$ commutative ring is **idempotent** if $a^2 = a$.

2 Properties of Rings

(instead of writing $a \times b$ we just write ab)

for any $a, b \in R$ (ring)
- $a0 = 0a = 0$.
- $(-a)b = a(-b) = -(ab)$.
- $(-a)(-b) = ab$

■ if $1 \in R$ then $-a = (-1)a$.

An element cannot be both a zero divisor and a unit in R. (There can be elements that are neither)

if $ab = 0$ in a integral domain I with $a, b \in I$ then at least on of a or b is zero.

Cancellation Laws holds in any Integral domain. (note: the existence of multiplicative inverse is not needed here.)

Any Finite Integral Domain is a Field
(use bijective map $I \to I$ by $x \to ax$ for non-zero $a \in I$.)

if S, T subgrings of R then :
■ $S \cap T$ is subring of R. (thus any arbitrary non-empty intersection of subrings is a subring.)
■ S is subring of T is subring of R then S is subring of R.

Properties of Center of a Ring

■ Center of a ring is a subring.
■ Center of a Division ring is a Field.
■ for fixed $a \in R$ set $C(a) = \{r \in R \,_s|_t\, ra = ar\}$ is a subring of R containing a.
■ Center of $R = \bigcap_{a \in R} C(a)$.
■ for any $a \in D$ division ring then $C(a)$ is a division ring.

if $x^2 = 1$ for some $x \in I$ integral domain then $x = \pm 1$ only.

if $x \in R$ commutative ring is nilpotent then
■ x is either zero or zero divisor (use $x^m = x^{m-1}x = 0$)
■ rx is nilpotent for any $r \in R$.
■ if $1 \in R$ then $1 + x$ is a unit in more general $u + x$ is a unit for any unit u and nilpotent x. (use $(1+x)(1 - x + x^2 + .. + (-1)^{m-1}x^{m-1}) = 1 + (-1)^{m-1}x^m = 1$.)

for rings R and S their direct product $R \times S$ is ring under corresponding component wise operation. (thus even any number of direct product of rings is a ring)

Characteristic $ch(R)$

Characteristic of a ring is a number
$n \,_s|_t\, n1 = \overbrace{1 + 1 + .. + 1}^{n \text{ times}} = 0$ if order of 1 is infinite then characteristic is said to be 0 (not ∞.)

every Integral domain has a Character 0 or prime. (if $q = mn$ is characteristic of I then $mn.1 = 0$ so either $m.1 = 0$ or $n.1 = 0$ a contradiction for minimality.)

3 Ring Homomorphism and Ideals

if R, S are two rings the a map $\phi : R \to S$ is a ring Homomorphism if it satisfies
■ $\phi(a + b) = \phi(a) + \phi(b)$
■ $\phi(ab) = \phi(a)\phi(b)$

■ kernel of ϕ $\ker \phi$ is the set in R mapped to 0 in S
■ image of ϕ and $\ker \phi$ are subrings.
■ if $\alpha \in \ker \phi$ then $r\alpha \in \ker \phi \; \forall r \in R$
i.e. $r \ker \phi \subseteq \ker \phi$

Concept of Ideal

From the above point and to define the quotient operations as in group homomorphism i.e. if $I \subseteq R$ and to the quotient operations

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

to be well defined we need to have that replacement by any class representative gives same classes i.e. if $\alpha, \beta \in I$ then
$(r + \alpha)(s + \beta) + I = rs + I$
to achive this : we need $I \trianglelefteq R$ (w.r.t +) this

can be satisfied by any subgroup of R as R is abelian in $+$, letting $r = s = 0$ we need I closed under multiplication so these two conditions boils down to I must be subring of R and also we need to have that I must be closed under left and right multiplication from any element in R i.e. $rI \subseteq I, Ir \subseteq I \; \forall r \in R$ this leads us to define Ideals

$I \subseteq R$ is a **left ideal** in R if I is subring of R and closed under left multiplications by elements of R, similarly $I \subseteq R$ is a **right ideal** in R if I is subring of R and closed under right multiplications by elements of R.
Finally $I \subseteq R$ is an **Ideal** of R if it is both left and right ideal of R

Ideal for Rings is 'similar' to Normal subgroups for Groups, Most of the following properties are Ring analogue of Group properties.

if I is an ideal of R ring then the quotient group (additive $\{r + I\}$) is a ring with binary operations as defined above. This Group R/I is called the **Quotient ring** of R by I.

Isomorphism Theorems for Ring

■ **1st Isomorphism Theorems for Ring** :
if $\phi : R \to S$ is a ring homomorphism then $\ker \phi$ is an ideal of R, image of ϕ in S is a subring of S and $R/ker(\phi)$ is isomorphic (bijective ring homomorphism) to $\phi(R)$. let $\cong$ denote Ring isomorphism from here on so $R/ker(\phi) \cong \phi(R)$
if I is an ideal of R then the natural projection homomorphism $\pi_I : R \to R/I$ by $\pi_I(r) = r + I$ is ring homomorphism with kernel I i.e. ideal $\iff$ kernel.
■ **2st Isomorphism Theorems for Ring** :
If A is subring of R and B ideal of R then $A + B = \{a + b | a \in A, b \in B\}$ is a subring of R, $A \cap B$ is an ideal of A and $(A + B)/B \cong A/(A \cap B)$.
■ **3st Isomorphism Theorems for Ring** :
if I, J are ideals of R such that $I \subset J$ then J/I is an ideal of R/I and $(R/I)/(J/I) \cong R/J$
■ **4st Isomorphism Theorems for Ring** :
If I is an Ideal of R ring then the map $A \to A/I$ is bijective between the set of subrings A of R that contain I and set of subrings of R/I also A is an ideal of R containing I iff A/I is an ideal of R/I.

if $\phi : R \to S$ is homomorphism and $x \in R$ is nilpotent then $\phi(x)$ is nilpotent in S.

3.1 Properties of ideal

Let** R **be a ring with identity for this subsection.

for ideals I, J of R ring define $I + J = \{a + b | a \in I, b \in J\}$ and $IJ = \langle ab | a \in I, b \in J \rangle$ (i.e. the set generated by ab or set of finite sums of element of form ab) then
$I + J$ is the smallest ideal containing both I and J in R,
$IJ \subset I \cap J$ and both $IJ, I \cap J$ are ideals in R.

Ideal Generated by $A \subseteq R$ denoted by (A) is the smallest ideal of R ring containing A.

define $RA = \{r_1a_1 + r_2a_2 + .. + r_na_n | r_i \in R, a_i \in A\}$ and $AR = \{a_1r_1 + a_2 + r_2a_2 + .. + a_nr_n | a_i \in A, r_i \in A\}$ and $RAR = \{r_1a_1r_1' + r_2a_2r_2' + .. + r_na_nr_n' | r_i, r_i' \in R, a_i \in A\}$

if R is commutative then $RAR = RA = AR = (A)$.

Principle Ideal

An ideal generated by a single element is called a Principle Ideal,
An ideal generated by a finite set is called **Finitely generated ideal.**

I is an ideal of R ring and $I = R$ iff I contains an unit of R.
So we get R is a field iff the only ideals of R are $\{0\}$ and R.

if F is field then any homomorphism from F is trivial ($\ker(\phi) = F$) or injective ($\ker(\phi) = 0$) i.e. **any non trivial homomorphism from a field is injective**

Maximal Ideal

M a proper ideal of R ring is called a Maximal Ideal of R if the only ideal containing M in R is R. i.e. no other proper ideals contains M in R.

M is maximal ideal of R ring iff R/M is a field.

for a Ring with identity every proper ideal is contained in a maximal ideal
(inclusion forms a partial ordering of proper ideals (non empty set) in the ring so a chain exist whose elements always contain the given proper ideal, now form an ideal by union of these ideals which is also proper (prove) thus a having upper bound and by Zorn's lemma a maximal element which is the maximal ideal.)

Prime ideal

An ideal P is Prime Ideal of R ring if $P \neq R$ and whenever $ab \in R$ the $a \in P$ or $b \in P$.
(this is sort of generalising 'prime' to a give ring R as in $\mathbb{Z}^+$ if p is a prime and $p|ab$ then $p|a$ or $p|b$.)

for R a commutative ring P is prime ideal in R iff R/P is an Integral domain.

from above point and similar point for maximal ideals we get :
in commutative ring R every maximal ideal is a prime ideal

similarly a commutative ring with identity is an integral domain iff $\{0\}$ is prime ideal in the ring.

in an Integral domain R $(a) = (b)$ for some $a, b \in R$ iff $a = ub$ for some unit $u \in R$.

if P a prime ideal of R commutative ring and P contains no zero divisors then R is an integral domain.

if $\phi : R \to S$ be a ring homomorphism between two commutative rings with identity:
■ for P prime ideal in S then $\phi^{-1}(P)$ is a prime ideal in R or $\phi^{-1}(P) = R$
■ if ϕ is **surjective** and M maximal ideal in S then $\phi^{-1}(M)$ is maximal in R.

In a finite commutative ring with identity every prime ideal is maximal ideal.
(use finite integral domain is a field.)

if R is commutative ring with property : for every $a \in R$ $\exists n \in \mathbb{Z}^+$ depending on a $_s|_t$ $a^n = a$ then every prime ideal of R is maximal idea.

4 Ring of fractions

let R be a commutative ring and $\{0\} \neq D \subseteq R$ that doesn't contain 0, doesn't contain any zero divisors of R, closed under multiplication then there is a commutative ring Q with 1 such that R is a subring of Q and every element of D in Q has an inverse.
This ring Q has following additional properties :
■ every element of Q is of the form rd^{-1} for some $r \in R$, $d \in D$ in particular If $D = R - \{0\}$ then Q is a field.
■ Ring Q is the smallest ring containing R in which all elements of D are units
(i.e. if $\phi : R \to S$ is an injective homomorphism $_s|_t$ $\phi(d)$ is a unit in S then there is An isomorphic copy of Q in S.)
this Q is called the **Ring of Fractions.** of D w.r.t R.

Construction of Ring of fractions

let $\mathcal{F} = \{(r, d)\ {}_s|_t\ r \in R, d \in D\}$ and define relation $\sim$ on $\mathcal{F}$ by $(r, d) \sim (s, e)$ iff $re = sd$ this becomes an equivalence relation as d, e are not zero divisors, denote equivalence class of (r, d) by

$$\frac{r}{d} = \{(a, b)\ {}_s|_t\ a \in R, b \in D \text{ and } rb = ad\}$$

then Q becomes the set of equivalence classes under $\sim$
properties such as commutativity , $1 = \frac{d}{d}$, additive inverse of $\frac{a}{d}$ is $\frac{-a}{d}$, $d^{-1} = \frac{1}{d}\ \forall d \in D$ hold making this Q the ring of fractions.

Q may also be denoted by $D^{-1}R$ to emphasize the envolved R, D.
If R is integral domain and $D = R - \{0\}$ then $D^{-1}R$ is a field so is called **Field of Fractions** of R.
If R is an integral domain, Q its field of fractions then if any field F contains $R'\ {}_s|_t\ R' \cong R$ then the subfield generated by R' in F is isomorphic to Q.

This concept of integral domains and field of fractions are derived from observing $\mathbb{Z}, \mathbb{Q}$ this is generalized by
if F is Field then F contains a unique smallest subfield that is either isomorphic to Q or $\mathbb{Z}/p\mathbb{Z}$. (depending on its characteristic.)

5 Chinese Remainder Theorem (c.r.t)

proper ideals I, J of R ring are comaximal ideals if $I + J = R$

c.r.t

let $A_1, A_2, .., A_k$ be ideals in R then the map $R \to R/A_1 \times R/A_2 \times .. \times R/A_k$ defined by $r \to (r + A_1, r + A_2, .., r + A_k)$ is a ring homomorphism with kernel $A_1 \cap A_2 \cap .. \cap A_k$. and if for each $i, j \in \{1, 2, .., k\}$ with $i \neq j$ A_i, A_j are comaximal then this map is surjective and $A_1 \cap A_2 \cap .. \cap A_k = A_1 A_2 .. A_k$.

Consequences of c.r.t

■ if $n = p_1^{a_1} p_2^{a_2} .. p_k^{a_k} \in \mathbb{Z}$ where $p_i's$ are prime in $\mathbb{Z}, a_i \in \mathbb{Z}^+$ then

$$\mathbb{Z}/n\mathbb{Z} \cong (\mathbb{Z}/p_1^{a_1}\mathbb{Z}) \times (\mathbb{Z}/p_2^{a_2}\mathbb{Z}) \times .. \times (\mathbb{Z}/p_k^{a_k}\mathbb{Z}).$$
$$(\mathbb{Z}/n\mathbb{Z})^* \cong (\mathbb{Z}/p_1^{a_1}\mathbb{Z})^* \times (\mathbb{Z}/p_2^{a_2}\mathbb{Z})^* \times .. \times (\mathbb{Z}/p_k^{a_k}\mathbb{Z})^*.$$

■ Chinese Remainder problem :
if $n_1, .., n_k$ are integers which are relatively prime i.e. $(n_i, n_j) = 1$ for $i \neq q$ and $a_1, .., a_k \in \mathbb{Z}$ then there is a solution to simultaneous congruences

$$\begin{aligned} x &\equiv a_1 \pmod{n_1}, \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_k \pmod{n_k}. \end{aligned}$$

${}_s|_t\ x \in \mathbb{Z}$ and is unique $\bmod n = n_1 n_2 .. n_k$ the solution given by :
let $n = n_1 n_2 .. n_k$, $n_i' = n/n_i$ and t_i be the inverse of $n_i' \pmod{n_i}$ then

$$x = a_1 t_1 n_1' + a_2 t_2 n_2' + .. + a_k t_k n_k' \pmod{n}$$

now if R, S are non zero fields then $R \times S$ is never a field. (as $(1, 0)(0, 1) = (0, 0)$)

6 Euclidean Domain.

Norm N

Norm N on R integral domain is a function from $R \to Z^+ \cup \{0\}$ with $N(0) = 0$.
if $N(a) > 0$ for $a \neq 0$ in R then N is called **positive norm .**

for R an integral domain is called an **Euclidean Domain** if there is a norm N on R such for any $a, b \in R$ with $b \neq 0$ there exist elements $q, r \in R$ such that

$$a = qb + r \text{ with } r = 0 \text{ or } N(r) < N(b)$$

here q is called quotient and r the remainder of the division.

Euclidean Division algorithm is valid in an Euclidean Domain (i.e. it stops after finite steps.)

Every ideal in Euclidean Domain is principal (i.e. generated by single element that has the minimum norm.)

in a commutative ring R, $a, b \in R$ and $b \neq 0$
■ a is said to be multiple of b if there exist $x \in R_{s}|_{t}$ $a = bx$. denoted by $b|a$
■ **Greatest common divisor** of $a, b \in R$ is a non zero $d \in R_{s}|_{t}$ $d|a, d|b$ and if any other $d'|a, d'|b$ then $d'|d$
this is denoted by $(a, b) = d$.

Properties of Gcd

■ if $a, b \in R$ not zero , ideal generated by a, b is principal and equal to (d) then $(a, b) = d$ (literally $(a, b) = (d)$)
■ now $(a, b) = d$ in R if I ideal generated by a, b is contained in (d) and any principle ideal (d') contains $I \implies (d) \subseteq (d')$
■ as $(d) = (d')$ then $d = ud'$ for some unit $u \in R$ Integral domain we have :
in an Integral domain R if d', d are both g.c.d of a, b then $d = ud'$ for some unit $u \in R$.
■ if R is an Euclidean domain if $(a, b) = d$ in R then $d = r_n$ the last remainder in euclidean algorithm applied to a, b in R and $d = xa + yb$ for $x, y \in R$.

Universal side divisor

$u \in R$ is Universal side divisor if for every $x \in R$ there is some $z \in R^* \cup \{0\}$ (set of units in $R + \{0\}$) such that $u|(x - z)$. i.e every x can be written as $x = qu + z$. for z unit or zero.

Test for not Euclidean domain

If R is an integral domain which is not a field , R is a Euclidean domain then there is a universal side divisor in R

(this point can be used to disprove a given ring is euclidean domain.)

7 Principal Ideal Domains

Principle ideal Domain is an Integral domain in which every ideal is principal.

Every Euclidean domain is a principal ideal domain.

if R is a P.I.D. (Principal Ideal Domains) , $(a, b) = d$ in R then $d = xa + by$ for $x, y \in R$ and d is unique upto multiplication by a unit in R.

Every non zero prime ideal of a P.I.D. is a maximal ideal

Dedekind-Hasse Norm

is positive norm on integral domain$R$ such that for every non zero $a, b \in R$ either $a \in (b)$ or there exist a non zero element of ideal (a, b) which has a norm strictly smaller than norm of b i.e. $\exists s, t \in R_{s}|_{t}\ 0 < N(sa - tb) < N(b)$.

test for not a P.I.D

Integral domain R is a P.I.D. iff R has a Dedekind-Hasse Norm.

if R is an Integral domain in which every prime ideal is principal then R is a P.I.D.

8 Unique Factorization Domain

Irreducible and prime

For an Integral domain R :

■ $r \in R$ a non-zero non-unit element is called **irreducible** in R if whenever $r = ab$. with $a, b \in R$
then at least one of a, b is a unit in R (i.e. r cannot be factored into only non units)
otherwise r is said to be **reducible**.

■ non zero $p \in R$ is called **prime** in R if (p) is a prime ideal in R.
(i.e. if $ab \in (p)$ then $p|ab$ so $p|a$ or $p|b$ analogous to definition of 'primes' in $\mathbb{Z}$.)

■ two elements $a, b \in R$ are called **associates** in R if the differ by a unit in R i.e $a = ub$ for some unit $u \in R$

In an integral domain every prime is irreducible.

In a P.I.D. every non zero element is prime iff irreducible.

U.F.D. (Unique Factorization Domain) : is an integral domain in which every non zero element which is not a unit can be written as finite product of irreducibles and this decomposition is unique upto associates. (i.e. for every non zero non unit $r \in R$, $r = p_1 p_2 .. p_n$ for $p_i's$ irreducibles and if same $r = q_1 q_2 .. q_m$ for q_i irreducible then $m = n$ and we can rearrange these decompositions such that p_i, q_i are associates .)

In a U.I.D. every non zero element is prime iff irreducible.

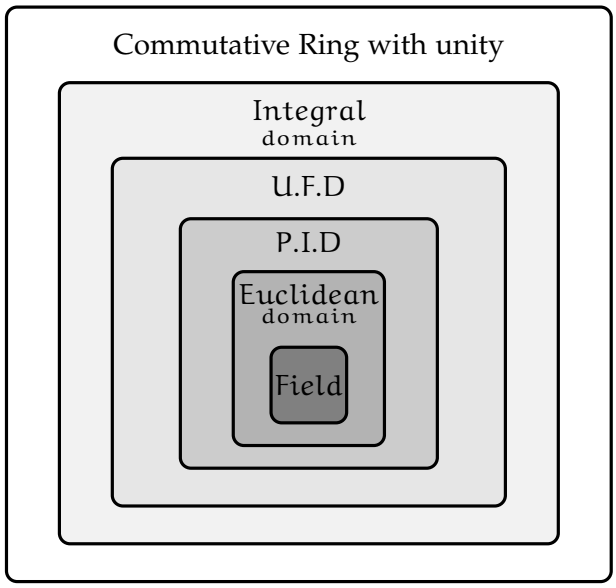
if $a, b \in R$ a U.I.D are such that $a = up_1^{e_1} p_2^{e_2} .. p_n^{e_n}$ and $b = vp_1^{f_1} p_2^{f_2} .. p_n^{f_n}$ for u, v units and $p_i's$ primes in R then

$$(a, b) = d = p_1^{\min(e_1, f_1)} p_2^{\min(e_2, f_2)} .. p_n^{\min(e_n, f_n)}.$$

Every P.I.D. is a U.I.D. in particularly every Euclidean Domain is a U.I.D.

Fundamental theorem of Arithmetic

$\mathbb{Z}$ is U.F.D.



i.e. **Field** $\subset$ **Euclidean Domains** $\subset$ **P.I.D.** $\subset$ **U.F.D.** $\subset$ **Integral domains** $\subset$ **Commutative Rings with** 1

■ Subring of an Integral domain may not be an Integral domain (may not contain unity)

■ But if a Subring of Integral Domain contains unity then it is an Integral domain
Here define a **Subdomain** of a Ring is Subring which is an Integral domain
so any Subring of Integral domain containing unity is a Subdomain

■ Subrings and Subdomains of U.F.D maynot be U.F.D (eg: $Z[\sqrt{5}]$ subring of C but not an U.F.D)

■ Subrings and Subdomains of P.I.D maynot be P.I.D (eg: Z[x] subring of Q[x], Z[x] is not a P.I.D as $\langle x, 2 \rangle$ is not principle ideal)

■ Subrings and Subdomains of Euclidean Domains may not be Euclidean Domain (eg Z[x] $\subset$ Q[x])

■ Subrings and Subdomains of Fields maynot be fields (eg Z $\subset$ Q)

9 Quadratic Field and Quadratic Integer Ring

if $D \in \mathbb{Q}$ is such that $\sqrt{D} \notin \mathbb{Q}$ i.e. D is not a perfect square in $\mathbb{Q}$ then

$$\mathbb{Q}[\sqrt{D}] = \{a + b\sqrt{D} | a, b \in \mathbb{Q}\}$$

forms a Field called Quadratic Field. (more precisely a subfield of $\mathbb{C}$)($(a + b\sqrt{D})^{-1} = a - b\sqrt{D}/(a^2 - Db^2)$ this is possible as $a^2 - Db^2 \neq 0$ if any one of $a, b \neq 0$ as D is not a perfect square in $\mathbb{Q}$.)

if $D \in \mathbb{Q}$ and D' is the square free part of D i.e. $D = kD'$ no square divides D' and $k = b^2$ for some $b \in \mathbb{Q}$. then $\mathbb{Q}[\sqrt{D}] = \mathbb{Q}[\sqrt{D'}]$.

If D is square free in $\mathbb{Z}$ then

$$\mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{D} | a, b \in \mathbb{Z}\}$$

forms a ring called Quadratic integer ring more precisely a subring of $\mathbb{Q}[\sqrt{D}]$.

if D square free in $\mathbb{Z}$ and $D \equiv 1 \pmod 4$ then

$$\mathbb{Z}[\sqrt{D}] \subset \mathbb{Z}[\frac{1 + \sqrt{D}}{2}] \subset \mathbb{Q}[\sqrt{D}]$$

i.e. $\mathbb{Z}[(1 + \sqrt{D})/2]$ is a slightly larger subring in $\mathbb{Q}[\sqrt{D}]$.

Define field norm $N(a + b\sqrt{D}) = a^2 - Db^2$ in $\mathbb{Z}[\sqrt{D}]$ clearly $N(\alpha\beta) = N(\alpha)N(\beta)$ and $N(\alpha) \in \mathbb{Z}$ only. (Generally **norm** is taken to be $|a^2 - Db^2|$ but field norm maps $\mathbb{Q}[\sqrt{D}] \to \mathbb{Q}$ which may be negative here it is restricted to $\mathbb{Z}[\sqrt{D}] \to \mathbb{Z}$).

thus $\alpha = a + b\sqrt{D}$ is a unit in $\mathbb{Z}[\sqrt{D}]$ iff $N(\alpha) = \pm 1$ (units in $\mathbb{Z}$)
iff $a^2 - Db^2 \in \{\pm 1\}$.

for $D \equiv 1 \pmod 4$,$\mathbb{Z}[\frac{1+\sqrt{D}}{2}]$, $w = \frac{1+\sqrt{D}}{2}$ and $\bar{w} = \frac{1-\sqrt{D}}{2}$ define the field norm as $N(a + bw) = (a + bw)(a + b\bar{w}) = a^2 + ab + \frac{1-D}{4}b^2$ same rule of units follow : $a + bw$ is unit iff $a^2 + ab + \frac{1-D}{4}b^2 = \pm 1$.

using the above defined field norm $N(a + b\sqrt{D}) = a^2 - Db^2$ or the other general **norm** we can use this norms property $N(ab) = N(a)N(b)$ to check for irreducibility, reducibility and prime nature of an element in $Z[\sqrt{D}]$ like if $N(a) = \pm p$ for a prime p then a is irreducible in $\mathbb{Z}[\sqrt{D}]$
■ from this property we get if D is square free and $a, b \in Z[\sqrt{D}]$ are such that ab is a unit in $Z[\sqrt{D}]$ then both a and b are units in $Z[\sqrt{D}]$
■ $\mathbb{Z}[\sqrt{D}]$ for $D < 0$ is an U.F.D iff $D = -1$ or -2.

Gaussian integer ring $\mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[i]$. is an U.F.D

10 Polynomial Rings

for any commutative ring R with identity we define R[x] as the ring of polynomial a set containing elements of type : $a_n x^n + a_{n-1}x^{n-1} + .. + a_1 x + a_0$ for $a_i \in R$, $n \geqslant 0$ and x a variable (simply denoted) is called the polynomial of x with coefficients in R, where n is degree a_n if $\neq 0$ the leading coefficient.
This set is a ring with addition defined component wise and multiplication is done by defining $(ax^j)(bx^i) = abx^{i+j}$ distributing it over $+$.
i.e. if $a(x) = \sum_{i=1}^{n} a_i x^i$ and $b(x) = \sum_{j=1}^{m} b_j x^j$ then $a(x) + b(x) = \sum_{i=1}^{\max(m,n)} (a_i + b_i)x^i$ $a(x)b(x) = \sum_{i=1}^{m+n} (\sum_{j=0}^{i} a_i b_{i-j})x^i$

(we can write any number of terms in a given polynomial for these operations by assuming coefficients are 0)

if R is an **Integral domain** then
- degree $a(x)b(x)$= degree $a(x)$ +degree $b(x)$
- the only units of $R[x]$ are the units of R
- $R[x]$ is an Integral domain.

(use fact that when polynomial with non zero leading coeffs are multiplied give a non zero leading coeff .)

$p(x)$ is zero divisor in $R[x]$ iff $bp(x) = 0$ for some $b \in R$ (use fact that $g(x)p(x) = 0 \; s|t \; g(x)$ has minimal degree then the leading coeff $p_n g_m = 0$ so $p_n g(x)p(x) = 0$ but degree $p_n g(x) <$ degree g_x so only possibility is $p_n g(x) = 0$ and by induction $p_i g(x) = 0 \forall i$ so $g_m p(x) = 0$ as $g_m p_i = 0 \forall i$)

if R is commutative $p(x) = a_n x^n + a_{n-1}x^{n-1} + .. + a_1 x + a_0$ is an element of $R[x]$ then
- $p(x)$ is nilpotent iff $a_n, a_{n-1}, .., a_1, a_0$ are nilpotent in R

(use induction: if $n = 0$ then clearly true, if $n = 1$ then $p(x) = a_1 x + a_0$ then any $p^k(x)$ has leading coeff a_1^k and constant term a_0^k so $p(x)^m = 0$ iff $a_1^m = 0, a_0^m = 0$ now for any n, $p(x) = x(a_n x^{n-1} + a_{n-1}x^{n-2} + .. + a_1) + a_0 = xq(x) + a_0$ by induction hypothesis $q^m(x) = 0$, if $a_0^n = 0$ let $k = max(n, m)$ now $(xq(x) + a_n)^{2k} = \sum_{i=0}^{2k} \binom{2k}{i} (xq(x))^i a_0^{2k-i}$ where the power of atleast one term $\geqslant k$ so $(xq(x) + a_n)^{2k} = 0$)
- $p(x)$ is a unit in $R[x]$ iff a_0 is a unit in R and $a_n, a_{n-1}, .., a_1$ are nilpotent in R.

(for converse use $p(x) = xq(x) + a_0 =$ nilpotent + unit = unit , now if $p(x) = xq(x) + 1$ is a unit then $p^{-1}(x)(xq(x) + 1) = 1$ so $xq(x)p^{-1}(x) = 1 - p^{-1}(x)$ equating for coefficients $p^{-1}(x)$ we get $p^{-1}(x) = 1 - q(x)x + q^2(x)x^2 + .. + (-1)^n q^n(x)x^n + ..$ and goes on so as degree of $p^{-1}(x)$ is finite we get $q^m(x) = 0$ for some $m \in \mathbb{Z}^+$ thus $q(x)$ is nilpotent and preceding point gives this point)

Ideals in Polynomial rings

if I is an ideal in R then
- $(I) = I[x]$ is an ideal in $R[x]$ and
- $R[x]/(I) \cong (R/I)[x]$.
- if I is prime ideal in R then $(I) = I[x]$ is prime ideal of $R[x]$.
- if I is a maximal ideal in R then (I, x) i.e. ideal generated by I, x is maximal in $R[x]$

(note : if I is maximal in R then $I[x]$ may not be maximal in $R[x]$

for eg: $2\mathbb{Z}$ is maximal in R but $2\mathbb{Z}[x]$ is not maximal in $\mathbb{Z}[x]$ as $2\mathbb{Z}[x] \subset (x, 2) \subset \mathbb{Z}[x]$)

Characterisation of Poly rings

- if F is a field then $F[x]$ is a Euclidean Domain (with norm = degree of the polynomial.)

Hence $F[x]$ is P.I.D. and U.F.D.
- if R is a commutative ring with identity then (x) is a prime ideal in $R[x]$ iff R is integral domain and (x) is maximal ideal in $R[x]$ iff R is a field. (use $R[x]/(x) \cong R$)
- if R is commutative ring such that $R[x]$ is a P.I.D then R is a field.

Irreducibility

a polynomial $f(x)$ is irreducible in $R[x]$ if whenever $f(x)$ can be expressed as $f(x) = g(x)h(x)$ then either $g(x)$ or $h(x)$ is a unit in $R[x]$ (note: we don't say any thing about the degree of $g(x)$ or $h(x)$ some times they can be equal to $f(x)$ also for eg: $2x^2 + 4 = 2(x^2 + 2)$ in $\mathbb{Z}[x]$ this becomes reducible but is irreducible in $\mathbb{Q}[x]$)

Primitive Polynomial

a polynomial non-zero polynomial $a_n x^n + a_{n-1}x^{n-1} + .. + a_0$ is called a **primitive polynomial** if gcd of $a_i's$ are 1
- product of two primitive polynomials is a primitive polynomial.
- A polynomial in $\mathbb{Z}[x]$ is irreducible then it is primitive.

for $f(x) \in F[x]$ a polynomial ring generated by field F :

■ $\langle f(x)\rangle$ is a maximal ideal in $F[x]$ i.e. $F[x]/(f(x))$ is a field iff $f(x)$ is irreducible in $F[x]$.
■ $f(x)$ is irreducible in F then $\{a + \langle f(x)\rangle \ _s|_t \ a \in F\}$ is subfield in $F[x]/(f(x))$ that is isomorphic to F.
■ if degree $f(x) = n \geqslant 1$ and if bars on top denote the passage to $F[x]/(f(x))$ then for each $\overline{g(x)}$ there is a unique $g_o(x) \in F[x]$ with degree $< n \ _s|_t \ \overline{g(x)} = \overline{g_o(x)}$ i.e. $F[x]/(f(x))$ is n dimensional vector space with basis $\bar{1}, \bar{x}..x^{\overline{n-1}}$
■ if F is a finite field of order q, degree $f(x) = n \geqslant 1$ then $F[x]/(f(x))$ has q^n elements.

if F is a finite field (or an infinite one) then there are infinitely many primes in $F[x]$.

Gauss Lemma

Let R be a U.F.D. , F its field of fractions and if $P(x)$ is reducible in $F[x]$ then $P(x)$ is reducible in $R[x]$

sort of converse of Gauss Lemma

Let R be a U.F.D. , F its field of fractions if $p(x) \in R[x] \ _s|_t$ the g.cd of its coefficients is 1 i.e. $p(x)$ is primitive polynomial then $p(x)$ is irreducible in $R[x]$ iff $P(x)$ is irreducible in $F[x]$, in particular if $p(x)$ is monic polynomial irreducible in $R[x]$ then $p(x)$ is irreducible in $F[x]$.

from above point we get : Let R be a integral domain, F its field of fractions if $p(x) \in R[x]$ is a monic polynomial reducible in $F[x] \ _s|_t \ p(x) = a(x)b(x)$ where $a(x), b(x)$ are monic and if $a(x) \notin R[x]$ then $R[x]$ is not a U.F.D.

R is a U.F.D. iff $R[x]$ is a U.F.D.

Irreducibility Criterion and properties

■ for F is a field and $p(x) \in F[x]$ has a factor of degree one iff $p(x)$ has a root in F.
■ immediately from above point we get polynomial of degree two or three in $F[x]$ for F field is reducible iff it has roots in F.

Rational root Theorem

let $p(x) = a_n x^n + a_{n-1}x^{n-1} + .. + a_o$ be a polynomial with integer coefficients, if $r/s \in \mathbb{Q}$ in lowest form (i.e. $(r, s) = 1$) is a root of $p(x)$ then $r|a_o$ and $s|a_n$, in particular if $p(x)$ is monic with integer coefficients and $p(d) \neq o$ for all integer dividing the constant term of $p(x)$ then $p(x)$ has no root in $\mathbb{Q}$.

■ if I is a prime ideal of Integral Domain R, $p(x)$ a non constant monic polynomial in $R[x] \ _s|_t$ its image in $(R/I)[x]$ cannot be factored into two polynomials of smaller degree in $(R/I)[x]$ then $p(x)$ is irreducible in $R[x]$. From this we get :

Mod p irreducibility test

For $f(x) \in \mathbb{Z}[x]$ with $deg(f(x)) \geqslant 1$, $\overline{f(x)} \in \mathbb{Z}_p[x]$ obtained from reducing coefficients of $f(x)$ modulo p for a prime $p \in \mathbb{Z}$ and if $\overline{f(x)}$ is irreducible in $\mathbb{Z}_p[x]$ and $deg(f(x)) = deg(\overline{f(x)})$ then $f(x)$ is irreducible in Q (**converse is not true** : i.e. if $\overline{f(x)}$ is reducible in $\mathbb{Z}_p$ then it may not be reducible in $\mathbb{Z}[x]$)

Eisenstein's Criterion

for P a prime ideal of integral domain R , $f(x) = x^n + a_{n-1}x^{n-1} + .. + a_1x + a_o \in R[x] \ _s|_t \ a_{n-1}, .. a_1, a_o$ are elements of P and a_o is not an element of P^2 then $f(x)$ is irreducible in $R[x]$.
For eg : $f(x) = x^n + a_{n-1}x^{n-1} + .. + a_o \in \mathbb{Z}[x] \ _s|_t \ p|a_i$ but if $p^2 \not| a_o$ then $f(x)$ is irreducible in $\mathbb{Z}[x]$ which makes it irreducible in $\mathbb{Q}[x]$.
$f(x) = a_n x^n + a_{n-1}x^{n-1} + .. + a_o \in \mathbb{Z}[x] \ _s|_t \ p|a_i$ **for** $o \leqslant i < n$

but if $p \not| a_n, p^2 \not| a_0$ **then** $f(x)$ **is irreducible in** $\mathbb{Z}[x]$ **which makes it irreducible in** $\mathbb{Q}[x]$**.**
(write $D = \{0, a_n\}$ then the fraction ring $D^{-1}\mathbb{Z}$ has $p\mathbb{Z}$ as prime ideal and $f(x) = x^n + \frac{1}{a_n}(a_{n-1}x^{n-1} + .. + a_0)$ in $D^{-1}\mathbb{Z}$ which satisfies original Eisenstiens criterion.)

for any field F and $0 \neq a \in F$ then
■ $af(x)$ is irreducible over F implies $f(x)$ is irreducible in F
■ $f(ax)$ is irreducible over F implies $f(x)$ is irreducible in F
■ $f(x + a)$ is irreducible over F implies $f(x)$ is irreducible in F

Cyclotomic polynomial : $\Phi_p(x) = \frac{x^p - 1}{x - 1}$ for a prime p is irreducible over $\mathbb{Q}$ (use $\Phi_p(x + 1)$ is irreducible by Eisenstien's criterion.)

$g(x) \in F[x]$ for a field F is such that $g(x) = f_1(x)^{n_1} f_2(x)^{n_2} .. f_k(x)^{n_k}$ be its factorization where $f_i(x)$ are distinct primes then

$$F[x]/(g(x)) \cong F[x]/(f_1(x)^{n_1}) \times F[x]/(f_2(x)^{n_2}) \times .. \times F[x]/(f_k(x)^{n_k}).$$

(use Chinese remainder theorem.)

if $f(x) \in F[x]$ has $a_1, a_2, .. a_k$ as roots in F field then $f(x)$ has $(x - a_1)(x - a_2)..(x - a_k)$ as factors, in particular **a polynomial of degree** n **over** F **has at most** n **roots in** F.

every finite subgroup of multiplicative group of a field is cyclic , in particular $F^* = F - \{0\}$ for F field is a cyclic group (multiplicative).
(use fundamental theorem of finite abelian groups and last point to show subgroup is $\cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times .. \mathbb{Z}/n_k\mathbb{Z}$ so has more than n_k roots for $x^{n_k} - 1$ if $k \geqslant 2$ as for each $d||G|$ cyclic group there are exactly d elements of order dividing d in G, so $k = 1$ i.e. subgroup is $\cong \mathbb{Z}/n_1\mathbb{Z}$ only.)
eg : now as $\mathbb{Z}/p\mathbb{Z}$ is a field for prime p we get $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic group of order $p - 1$ (multiplicative).

$\mathbb{Z}/p^\alpha\mathbb{Z}$ is cyclic group of order $p^{\alpha-1}(p - 1)$ for all odd primes $p, \alpha \geqslant 1$
(use $(1 + p)^{p^{n-1}} \equiv 1 \pmod{p^n}$ but $(1 + p)^{p^{n-2}} \not\equiv 1 \pmod{p^n}$ so Sylow p subgroup is cyclic and homomorphism $\phi : (\mathbb{Z}/p^\alpha\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*$ by $\phi(a) = a \pmod{p}$ then ϕ is serjective so any $p \neq q | p - 1$ is Sylow q subgroup is mapped isomorphically to subgroup of $(\mathbb{Z}/p\mathbb{Z})^*$ which is cyclic so all Sylow subgroups of $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ are cyclic so by direct product and order deduction we have $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ is cyclic.)

10.1 Multivariable Polynomial Rings

For any ring R define inductively the polynomial ring in variables $x_1, x_2, .., x_n$ with coefficients in R denoted by $R[x_1, x_2, .., x_n]$ by

$$R[x_1, x_2, .., x_n] = R[x_1, x_2, .., x_{n-1}][x]$$

i.e. its elements are finite sum of non zero monomial terms like
$a x_1^{d_1} x_2^{d_2} .. x_n^{d_n}$ for $a \in R, d_i's \geqslant 0$.
where a monic term $x_1^{d_1} x_2^{d_2} .. x_n^{d_n}$ is called **monomial**
d_i is degree of x_i, the sum $d = d_1 + d_2 + .. + d_n$ is called the degree of the term and
the ordered n-tuple $(d_1, d_2, .. d_n)$ is called **multidegree** of the term.

11 Matrix Rings

for any non trivial ($\neq \{0\}$) ring R let $M_n(R) = [a_{ij}]$ be set of all $n \times n$ matrices with entries a_{ij} from R with component wise addition and matrix multiplication this $M_n(R)$ forms ring with properties as follows :
■ $M_n(R)$a non commutative ring whenever $R \neq \{0\}$ and $n \geqslant 2$
■ $M_n(R)$ contains a zero divisor whenever $n \geqslant 2$
■ The set of scalar matrices ($a_{ii} = a \forall i$ $a_{ij} = 0$

if $i \neq j$.) in $M_n(R)$ forms a subring isomorphic to R.
■ center of $M_n(R)$ is the set of scalar matrices.
■ if S is a subring of R then $M_n(S)$ is subring of $M_n(R)$

All rings with unity of order p and p^2 are commutative the ring $\left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix}_{s|t} a, b, c \in F_p \text{ field of order } p \right\}$ is a non-commutative ring with unity of order p^3

12 Group Rings

for a commutative ring R with identity $1 \neq 0$ and $G = \{g_1, g_2, .., g_n\}$ be a finite group with group operations written multiplicatively then
RG a group ring is defined to be set of formal sums $a_1g_1 + a_2g_2 + .. + a_ng_n$ for $a_i \in R$ if g_1 is identity then a_1g_1 is simply written as a_1
with addition defined component wise and multiplication defined by $(ag_j)(bg_i) = abg_k$ for $g_ig_j = g_k$ in G and obeying distribution w.r.t. + i.e. if $\alpha = \sum_{i=1}^{n} a_ig_i, \beta = \sum_{j=1}^{n} b_jg_j$ then $\alpha + \beta = \sum_{i=1}^{n}(a_i + b_i)g_i$. and
$\alpha\beta = \sum_{k=i}^{n}(\sum_{g_jg_i=g_k} a_ia_j)g_k$. then these operations make RG a ring with following properties

G $\subset$ RG is subgroup of units of RG (note $1g_1 = g_1 \in RG$)

if $|G| > 1$ then RG has a zero divisor (if $g^m = 1$ in G then $(1-g)(1+g+..+g^{m-1}) = 1-g^m = 0$)

if S is a subring of R then SG is subring of RG.

If $\mathcal{K} = \{k_1, k_2, .., k_n\}$ is one of the conjugacy classes of group G then
$K = k_1 + k_2 + .. + k_n$ is in center of RG
(as $g^{-1}Kg = K \forall g \in G \implies agK = Kag$)

12 References

[1] David S. Dummit, Richard M. Foote : Abstract Algebra, John Wailey & sons, 3, (2004).

[2] Joseph A. Gallian : Contemporary Abstract Algebra, Cengage Learning, 9, (2017).