RING AND FIELDS.

GEORGE SALMAN

Requiements to get richer.

(1) Work hard.
(2) Robbing bank of human knowlegment

Ring. (Denote by R). $R \neq \emptyset$..

- Abelian group for + i.e
  - for all $a, b \in R \to a + b \in R$ unique.
  - There is element which is the $0 \in R$: $0 + a = a$ for all $a \in R$.
  - $a + b = b + a, \forall a, b \in R$.
  - $a + (b + c) = (a + b) + c, \forall a, b, c \in R$.
  - $\forall a \in R$ there is $-a \in R : a + (-a) = 0$.

In order to define ring only, we need it to be Abelian group. In order to define ring with identities we need to add the following properties.

- $a, b \in R \to a \cdot b = ab \in R$.
- There is $1 \in R : 1 \cdot a = a, a \cdot 1 = a, \forall a \in R$.
- $a \cdot (b + c) = a \cdot b + a \cdot c, (a + b) \cdot c = a \cdot c + b \cdot c$

Definition. field is the defined with the same properties of ring with identities also with inverse property i.e $a \cdot a^{-1} = I$.

Remark. We have asscosiatove property in a a ring.

Theorem. *Fermat theorem. If $p \in \mathbb{Z}$ a prime $p = 4n + 1$ then there is $a, b \in \mathbb{Z}$ in which $p = a^2 + b^2$.*

Example. $17 = 4 \cdot 4 + 1$. So there is $a = 4, b = 1$.

Gaussian intergers ring $J[i]$ where its element are $z = a + bi, a, b \in \mathbb{Z}$..

Remainder.

A ring is euclidean where $d : J[i] \backslash \{0\} \to \{0, 1, ...\}$. Using property 2 of eucludean ring $0 \neq z_1, z_2 \in J[i] \Rightarrow d(z_1 z_2) \geq d(z_1), d(z_1 z_2) \geq d(z_2)$. also $z_1 = z_2 z + r$ where $r = 0$ or $d(r) < d(z)$.

Example. In $\mathbb{Z}$ then d is the map defined by $|p|$, and for $\mathbb{F}[x]$ polynomials with field $\mathbb{F}$ then d is the mapd defined by $deg(p(x)) = deg(p(x))$.

Theorem. *The Gaussian integers ring is euclidean ring.*

Proof. First, we need to show that the first property is satisfied i.e., $|z_1 z_2|^2 \geq |z_1|^2$. $|z_1 z_2|^2 = |z_1|^2 |z_2|^2$ and since $|z_1|^2 \geq 1$ we get $|z_1 z_2|^2 > |z_2|^2$.

Example. Given $z_2 = 15+8i$, $z_2 = 3+4i$. we can see that $(15+8i) = (3+4i)\cdot 2+9$. We have a constrain of $c^2+d^2 < 25$ so e.g., if we take 2 as above we get 9 and $9^2 \not< 25$ we can wrire the follows as system of equation $15 = 3a-4b+c, 8 = 4a+3b+d$. We will avoid c, d for little and get the following system of equation $\begin{pmatrix} 3 & -4 \\ 4 & 3 \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 15 \\ 8 \end{pmatrix}$ so we solution is $a = \frac{77}{25}, b = -\frac{36}{25}$ so we can round up those number to a integers and we will get suitable reminder $a = 3, n = -1$.

This example is the direction toward a proof. In general $z_1 = r_1+r_2i, z_2 = s_1+s_2i$ we need to show that ther is $a, b \in \mathbb{Z}$ s.t. $r_1 + r_2i = (s_1+s_2i)\cdot(a+bi)+(c+di)$. So, $r_1 = s_1a - s_2b + \alpha, r_2 = s_2a + s_1b + \beta$. Thus, $\begin{pmatrix} s_1 & -s_2 \\ s_2 & s_1 \end{pmatrix}\begin{pmatrix} \tilde{a} \\ \tilde{b} \end{pmatrix} = \begin{pmatrix} r_1 \\ r_2 \end{pmatrix}$. Using Kremer Theorem, $\tilde{a} = \frac{r_1s_1+r_2s_2}{s_1^2+s_2^2}, \tilde{b} = \frac{r_2s_1-r_2s_2}{s_1^2+s_2^2}$. And we get a, b by rounding up or down so the total sum difference of them is less than 1 from the most close integer to each.

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} r_1 \\ r_2 \end{pmatrix} - \begin{pmatrix} s_1 & -s_2 \\ s_2 & s_1 \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} =$$

$$= \begin{pmatrix} r_1 \\ r_2 \end{pmatrix} - \begin{pmatrix} s_1 & -s_2 \\ s_2 & s_1 \end{pmatrix}\begin{pmatrix} \tilde{a} \\ \tilde{b} \end{pmatrix} + \begin{pmatrix} s_1 & -s_2 \\ s_2 & s_1 \end{pmatrix}\begin{pmatrix} \tilde{a} \\ \tilde{b} \end{pmatrix}$$

$$\overbrace{\begin{pmatrix} 0 \\ 0 \end{pmatrix}}$$

$$- \begin{pmatrix} s_1 & -s_2 \\ s_2 & s_1 \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} s_1 & -s_2 \\ s_2 & s_1 \end{pmatrix}\begin{pmatrix} \tilde{a}-a \\ \tilde{b}-b \end{pmatrix}$$

Therefore,

$$\tilde{a} - a = \delta_1, \tilde{b} - b = \delta_2$$

Hence,

$$\alpha^2 + \beta^2 = (s_1\delta_1 - s_2\delta_2)^2 + (s_2\delta_1 + s_1\delta_2)^2 =$$

$$(s_1^2+s_2^2)(\delta_1^2+\delta_2^2) < s_1^2+s_2^2 \iff \left(\delta_1^2+\delta_2^2\right) < 1$$

So, we need $\delta_1^2+\delta_2^2 < 1$ i.e., the sum of differences we by rounding up and down of $\tilde{a}, \tilde{b}$ is not more than 1. □

How to find primes numbers in Gaussian ring. We start by eliminate prime number from scratch i.e.,

$$2 \quad 3 \quad \cancel{4} \quad 5 \quad \cancel{6} \quad 7 \quad \cancel{8}$$

Lets find the smallest prime number with the smallest d in $J[i]$. In this case $\pm 1, \pm i$ are smallest primes in $J[i]$ with $d = 1$ now in $\mathbb{Z}$ the smallest prime number i.e., startgin from $\pm 1 \pm i$ where $a^2+b^2 = 2$ is 2. So, we can see that we have maximal ideal generated by those elements. We defined earlier that a numer is prime if there is no b, c no invertible in which $a = bc$. So lets check if $1+i$ is a prime.

Lemma. *Assuming $0 < p \in \mathbb{Z}, c \in \mathbb{Z}$ s.t. $gcd(c, p) = \pm 1$ there is $a, b \in \mathbb{Z}$ s.t. $cp = a^2+b^2$.(i.e., c, p are relatively prime) thenp is not prime in $J[i]$.*

Proof. By contradiction, p is prime in $J[i]$. By given, $cp = x^2+y^2 = (x+iy)(x-iy)$ $\Rightarrow p \mid (x+yi)$ or $p \mid (x-yi)$. WLOG $p \mid (x+yi)$ in $J[i] \Rightarrow p(\alpha+\beta i) = (x+yi)$ $\Rightarrow x = \alpha p, y = \beta b \Rightarrow p \mid x-yi$ hence, $p \mid (x+yi)$ and $p \mid (x-yi)$ hence, $p^2 \mid (x-yi)(x+yi) = x^2+y^2 = cp$ i.e., $p \mid c$ which is contradiction to that fact $gcd(p,c) = 1$.

Lemma. *Given that R euclidean $p \in R$ are primes and $p = ab \Rightarrow p \mid a$ or $p \mid b$.*

□

Theorem. *Assuming $0 < p \in \mathbb{Z}, c \in \mathbb{Z}$ s.t. $gcd(c,p) = \pm 1$ there is $a,b \in \mathbb{Z}$ s.t. $cp = a^2+b^2$.(i.e., c,p are relatively prime) $\iff$ $p \nmid c$. then there is $x,y \in \mathbb{Z}$ this case $p = x^2+y^2$.*

Definition. $p \in R$ where R euclidean ring is prime $\iff$ $p = ab$ where a,b not invertible.

Example. $p = 5 = 2^2+1, c = 2, cp = 10 = 3^2+1$.

Definition. R euclidean, and given $a,b \in R$ are relatively prime $\iff$ $gcd(a,b)$ is invertible.

Fermat Theorem. $p \in \mathbb{Z}$ where $p = 4n+1, n \in \mathbb{Z}$, then there is $a,b \in \mathbb{Z}$ s.t. $p = a^2+b^2$.

Proof. Using previous lema p is not prime in $J[i]$ i,e., $p = (a+bi)\left(\tilde{a}+\tilde{b}i\right)$ where $(a+bi), \left(\tilde{a}+\tilde{b}i\right)$ are not invertible in $J[i]$ so $(a+bi) \neq \pm 1, \pm i, \left(\tilde{a}+\tilde{b}i\right) \neq \pm 1, \pm i$. $\Rightarrow p^2 = \left(a^2+b^2\right)\left(\tilde{a}^2+\tilde{b}^2\right)$. Therefore, $a^2+b^2 \mid p^2 \Rightarrow a^2+b^2 \in \left\{1,p,p^2\right\}, \left(\tilde{a}^2+\tilde{b}^2\right) \mid p^2 \Rightarrow \tilde{a}^2+\tilde{b}^2 \in \left\{1,p,p^2\right\}$. Now, the case where $a^2+b^2 = 1, \tilde{a}^2+\tilde{b}^2 = 1$ is eliminted because given that $a+bi$ is not invertible, either $a^2+b^2 = p, \tilde{a}^2+\tilde{b}^2 = p$ is also eliminated, and the only options is $a^2+b^2 = 1, \tilde{a}^2+\tilde{b}^2 = p$ or $a^2+b^2 = p, \tilde{a}^2+\tilde{b}^2 = 1$ so $p = a^2+b^2, \tilde{a}^2+\tilde{b}^2 = p$. □

Main questions of ALGEBRAIC GEORMETRY.. Today, we are going to talk about unique factorization domain. $\{x \in \mathbb{R} : p(x) = 0\}$? $\sim$ Factorization of $p(x)$ where $p(x)$ is polynomial of degree n. Over $\mathbb{C}$: at least one root. i.e., over $\mathbb{C}$, $p(x) = a(x-x_1)^{r_1}...(x-x_s)^{r_s}, r_1+...+r_s = n$. Over $\mathbb{R}$, $p(x) = a(x-x_1)^{r_1}...(x-x_s)^{r_s}Q_1(x)\cdot...\cdot Q_p(x)$ where $Q(x)$ are polynomial of degree 2 without real roots. Given that $p(x) = x^n+a_{n-1}x^{n-1}+...+a_1x+a_0$ when there is a root of multiplicity $\geq 2 \iff$ the is solution for $\{p(x) = 0, p'(x) = 0\}$with condition on $a_0,..,a_{n-1}$. We will define a new term, the resultant between polynimials, $Resultant(p(x),Q(x)) = \{$Parameter: there is common root$\}$, a private case is when $Resultant\,(p(x),p'(x))$. E.g., $p(x) = x^2+a_1x+a_0, p'(x) = 2x+a_1$, we need $p'(x) = 2x+a_1 = 0 \iff x = -\frac{a_1}{2}$, plugging in into $p(x)$ we get $a_0-\frac{a_1^2}{4} = 0$, this is called the discrimant. A critical set is when $\{discrimant = 0\}$, so if the paramters are in the critical set then there is a root. A new terminolgy, we are going to use is a **Path** for example, given $(x-1)\cdots(x-10) = x^{10}+a_9x^9+...a_1x+a_0$, the path is $(a_0t,...,a_9t), t \in [0,1)$. $(a_0,...,a_9) \notin (Discrimant = 0) \to (\tilde{a_0},...,\tilde{a_9}) \notin \{Discrimant = 0\}$, it's not true always, however in $\mathbb{C}$we will show that there is a path.e.g., $p(x) = x^2+2x-5, \phi(t) = x^2+(2+t)x-(5+t)$. in case $\phi(t=0) = p(x)$. E.g., $\forall r \in \mathbb{R}, r = p_1\cdot p_2..\cdot p_s$ where p_i are primes this factorization is unique up tp order, and up to multiplication by invertible elements.

Definition. The ring of unique factorization domain R is intergral domain with 1, and $\forall r \in \mathbb{R}, r = p_1 \cdot p_2 .. \cdot p_s$ where p_i are primes this factorization is unique up tp order, and up to multiplication by invertible elements.

Theorem. *If there is a field $\mathbb{F}$ defines on polynomial with coeffcients i.e., $\mathbb{F}[x_1, ..., x_n]$ is a unique facctorization domain.*

Theorem. *(Hilbert $\approx$ 1930). Any ideal in $\mathbb{F}[x_1, ..., x_n]$ is finitely field generated.*

Remark. The theorem tell us that given a inifnite system of equations

$$\left\{ \begin{array}{c} p_1(x_1, .., x_n) = 0 \\ p_2(x_1, ..., x_n) = 0 \\ \vdots \end{array} \right\}$$

There is $s < \infty$ in which,

$$\left\{ \begin{array}{c} p_1(x_1, .., x_n) = 0 \\ p_2(x_1, .., x_n) = 0 \\ p_3(x_1, ..., x_n) = 0 \\ \vdots \\ p_s(x_1, .., x_n) = 0 \end{array} \right\}$$

Proof. In case $n = 1$ this is a private case of Euclidean ring. For $n \geq 2$ not euclidean ring this stem from the fact that every ideal is one generated. However, for $n \geq 2$ (x_1, x_2) this is not 1 generated ideal but 2. Therefore, this is not eucliedean ring.

Lemma. *If R unique factoriztion domain then $R[x]$ is also unique factorization domain.*

This Lema is so important for the induction assumption, So we can say that

$$\mathbb{F}[x_1, ..., x_n] = (\mathbb{F}[x_1, ..., x_{n-1}])[x_n]$$

$(\mathbb{F}[x_1, ..., x_{n-2}][x_{n-1}])[x_n] = ... = \mathbb{F}[x_1][x_2] \cdots [x_{n-1}]$

Using that fact that for $n = 1$, $\mathbb{F}[x_1]$ is unique factoriztion domain (with multicipity of other ideals). □

Exercise. Given that $f(x) = x^4 + ax^3 + bx^2 + cx + d \in Z[x], a, b, c, d \in 2\mathbb{Z} + 1$ show that f is irrducable in $\mathbb{Z}$.

Solution. For f there is no common factor hence, irrducable hence $f(x) = P(x)Q(x)$ where both are irrducable then $deg(p) = deg(Q) = 2, degP = 1, degQ = 1$. Assume toward contradiction if $degP = degQ = 2$ then $P(x) = x^2 + \alpha x + \beta, Q(x) = x^2 + \gamma x + \delta$, not that

$$1.\beta\delta = d$$
$$2.\alpha\delta + \gamma\beta = c$$
$$3.\beta + \alpha\gamma + \delta = b$$
$$4.\gamma + \alpha = a$$

From equation 4 is odd so one of them is even. Now, $\alpha\gamma$ is odd so $\beta+\alpha\gamma+\delta = b$ is even so contradiction. Now, in case 2, $degP = 1, degQ = 2$ so $P(x) = x+\alpha, Q(x) = x^3 + \beta x^2 + \gamma x + \delta$ in identical way.

Theorem. *Lema of guass. Given $f(x) \in \mathbb{Z}[x]$ non constant, f is irriducable on $\mathbb{Z}$ $\iff$ f is irriducable on Q, and for f coeffcients there is not common term and also f is irrducable on $\mathbb{Z}$.*

Example. $f(x) = x^4 + ax^3 + bx^2 + d$ is irriducable on Z hence on Q.

Exercise. Show that $f(x) = x^3 + 15x^2 + 10x + 15$ is irriducable in $\mathbb{Q}$.

Solution. Its suffcient to show that irriducable in $\mathbb{Z}$.

$$f(x) = (x+\alpha)\left(x^2 + \beta x + \gamma\right)$$

$$= x^3 + (\alpha+\beta)\,x^2 + (\alpha\beta+\gamma)\,x + \alpha\gamma$$

Notice that, $\alpha\gamma = 5 \Rightarrow 5$ divides α, γ. If $5 \mid \alpha$ then $(5 \mid \alpha + \beta = 15 \Rightarrow 5 \mid \beta)$ now $5 \mid \alpha\beta + \gamma = 10 \Rightarrow 5 \mid \gamma$ so contradcition. Case 2, if $5 \mid \gamma$ then $5 \mid \alpha\beta + \gamma \Rightarrow 5 \mid \alpha\beta$ so 5 divides α or β so now $5 \mid \alpha + \beta \Rightarrow 5 \mid \alpha$.

Theorem. *Eisenshtein Criterion. Let R be UDF,*

$$f(x) = a_n x^n + ... + a_1 x + a_0 \in R[x]$$

, and assume that exists $\pi \in R$ is prime s.t.

- $\pi \mid a_i, i = 0, ..., n-1$, $\pi \nmid a_n$.
- $\pi^2 \neq a_0$

Then $f(x)$ is irriducable.

Example. $f(x_1, x_2) = x_1^2 x_2^2 + x_1 x_2^2 + x_2^3 + x_1^2 x_2 + x_1$ irriducable in $\mathbb{Z}[x_1, x_2] = (\mathbb{Z}[x_1])[x_2]$ so we can write

$$f(x_1, x_2) = x_2^3 + (x_1^2 + x_1)x_2^2 + x_1^2 x_2 + x_1 \in (\mathbb{Z}[x_1])[x_2]$$

for $\pi = x_1 \in \mathbb{Z}[x_1]$ is prime then satisfied Eisenshtein Criterion hence irriducable.

Remark. Given that $f(x) \in R[x]$ is irriducable $\iff$ $f(\alpha x + \beta)$ irriducable for all $\alpha, \beta \in R$. Thus, stem from that fact $R[x] \to R[x]$ so $p(x) \to p(\alpha x + \beta)$ isomorphic $f(x) = P(x)Q(x) \to f(\alpha x + \beta) = p(\alpha x + \beta)Q(\alpha x + \beta)$ so $f(x) = p(\frac{x-p}{\alpha})Q(\frac{x-\beta}{\alpha})$.

Example. $x^4 + 4x^3 + 8x^2 + 8x + 9$ so $f(x-1) = x^4 + 2x^2 + 6$ irriducable from Eisenshtein Criterion for $\pi = 2$ so $f(x)$.

Exercise. Given $p(x_1, x_2) = 2 + \lambda x_1^2 + x_1^4 - 2x_2 + x_1^2 x_2 - x_2^2 + x_1^2 x_2^2 + x_2^3$ how can we sketck $\{(x_1, x_2) : P(x_1, x_2) = 0\}$. Moreover, for which λ

Definition. A set $\mathbb{F}$, with two binary operations, addition $(+)$, and multiplication (x). $(\mathbb{F}, +)$ is commutative group i.e., we have

(1) associative property: $(a + b) + c = a + (b + c)$.
(2) Exists 0 element which satisfy. $a + 0 = 0 + a = a$.
(3) Additive inverse $-a$ which satisfy $a + (-a) = (-a) + a = 0$.
(4) Commutativity i.e., $a + b = b + a$.

And $(\mathbb{F}\backslash\{0\}, x)$ a commutative group also, so we have two structures which construct a fields, but what connect this two structures is the distributivity proberty which means,

- $ax(b + c) = axb + axc$.

Example. Some examples. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ used in analysis, physics. $\mathbb{F}_p$ which is used in CS, and many others fields.

Non fields.

(1) For example $\mathbb{Z}, \mathbb{F}[x]$ it satsify all the properties expect the inverse (not for eveery element there is inverse).
(2) The set of all real function $\{f : \mathbb{R} \to \mathbb{R}\}$, $\{f : \mathbb{N} \to \mathbb{R}\}$.
(3) $M_n(\mathbb{F})$ the matrix space - no inverse element also no commutativity.

Remark. Note that each two element $0 \neq a, b \in \mathbb{Z}$ satisfy that $ab \neq 0$. However, in example 2 this is not neccessarily the case, for example take $f = X_{[0,1]} = \left\{ \begin{array}{ll} x \in [0,1], & 1 \\ otherwise & 0 \end{array} \right\}, g = X_{[2,3]} = \left\{ \begin{array}{ll} x \in [2,3], & 1 \\ otherwise & 0 \end{array} \right\}$, satisfy that $fg = 0$ always but both of them are not zero function. This is going to be definition of zero divisor.

Table. In order to understad what is a ring,

We can see that in almost all of the examples, there was all the properties of addition satisfied. Also, in the multplication properties satisfied the assoctiativity, and distributivity. This is going to be our definition to a ring i.e., sets which satisfy this mentioned properties.

Definition. A ring is a set R with binary operations $+$, and multuplication x s.t.

(1) $(R, +)$ is a commutative ring.
(2) x (multuplication) satisfy assoctiativity.
(3) There is distributivity i.e., $a(b + c) = ab + ac, (a + b)c = ac + bc$.

If exists a natural unit 1 element then this is a **ring with unit**.

Application of rings.

(1) In numbers theory: we are going to see a solution $x^2 + y^2 = z^2$ (trouble). Or in general $x^n + y^n = z^n, n \geq 3$, has no solution is the last Theorem of Fermat.
(2) Representation of groups. Given a group G operate on space X, i.e., there is space X which we want to learn, and we can do it using the symmetric

of this space. For example, if (1). X is a graph, or a poker cards so we can look at all the permutation of the cards, or all the symmetries of the graph which keep X in the same place so basically a $\tilde{}$ combinatoric operation. (2). X is a mertic space, so it can be a topological operation for example rotations of the plane, reflections. (3). X is a vector space our operation is $\tilde{}$ linear operation so we can use all what we know about linear algebra. Now, the best sencario is indeed X is a vector space, but many times it's not maybe graph, mertric space, or poker cards (example we saw) so in this case what we can is transforming X into vector space i.e., $X \to$vector space. We know that in the source operation, we used that fact that G has the multiplocation $*$ property $(G, *)$, but now X is a vector space so we can add two vectors, and we want to use this property in G, i.e., we want to take $(G, *)$ and add the addition property $\Rightarrow$ ring.

Example. we want to understand the analysis of the set $\{f : \mathbb{R} \to \mathbb{R}\}$. We can take the function and shigt its graph left and right. This idea of linearity leads to Fourie transfomations.

(3) Find a root to a polynom. We can take a problem, and translate it to finding roots for a polynomials. E.g., finding $x^2 + 1$ where $x \in \mathbb{R}$, lead us to the construction of $\mathbb{C}$.

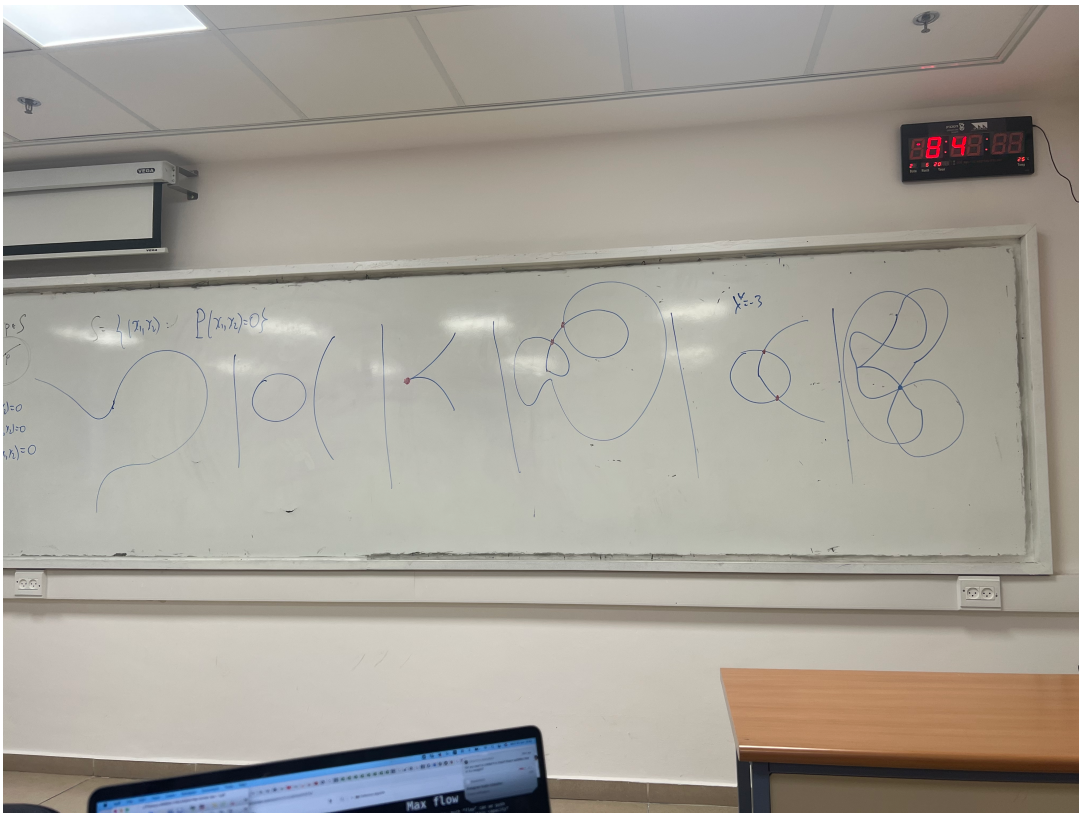
Definition. A $(R, +, \cdot)$ is ring if $(R, +)$ is cummotative ring and the multilication accosiative and there are distributivity.

Claim. Let $(R, +$

Claim. (George). Given $n \in \mathbb{N}$, where $n \, mod \, 10 = 5$. Then $\left\lfloor \frac{n^2}{100} \right\rfloor mod 10 = abmod 10$ where $a = \left\lfloor \frac{n}{10} \right\rfloor, b = a + 1$. Moreover, this can be generalized for all other digits (after the hundred digits to find n^2).

Example. $n = 65$, in this case $\left\lfloor \frac{n^2}{100} \right\rfloor mod 10 = 0$, and $a = 5, b = 6, abmod 10 = 0$.

We are interested to know if $P(x_1, x_2)$ is reducable for λ. We can't check easily. However, we can figure out the graph behaviour of $\{P(x_1, x_2) = 0\}$.



We can locate the singular points which are marked in red. By checking that the *grad* of p locally is 0. We will call them self intersection point, and a knot point. So, we can check is a point p is singular is in the set $\left\{ \begin{array}{c} P(x_1,x_2)=0 \\ \frac{\partial P}{\partial x_1}=0 \\ \frac{\partial P}{\partial x_2}=0 \end{array} \right\}$. A famous problem is to show that there is connection between determining whether P is reducable, and number of components in the graph.

Example. let check the singular points of $P(x_1,x_2)=x_1^2-x_1x_2+\lambda x_1+x_1+1$. We check the set,

$$\left\{ \begin{array}{c} P(x_1,x_2)=0 \\ \frac{\partial P}{\partial x_1}=0 \\ \frac{\partial P}{\partial x_2}=0 \end{array} \right\} = \left\{ \begin{array}{c} x_1^2-x_1x_2+\lambda x_1+x_1+1=0 \\ -x_1+1=0 \\ 2x_1-x_2+\lambda=0 \end{array} \right\}$$

From here we get $x_1=1, x_2=2$. So the polynomial vanish where $1-2-\lambda+\lambda+1+2+\lambda=0.\lambda+2=0$ so $\lambda=-2$ we got singular points.

Our starting point is two fields $\mathbb{F}\subseteq\mathbb{K}$ we can say then that K is a vector space over $\mathbb{K}$ with a dimension (Notation $[\mathbb{K}:\mathbb{F}]$. If the dim is finite then we can say that $\mathbb{K}$ finite exterior of $\mathbb{F}$.

Example. $[\mathbb{C}:\mathbb{R}]=2, [\mathbb{R}:\mathbb{Q}]=\infty$.

Construction of $\mathbb{F} \subset * \subset \mathbb{K}$ *,* $a \in \mathbb{K}$*,* $a \notin \mathbb{F}$*..*

Definition. $\mathbb{F} \subset * \subset \mathbb{K}$, $a \in \mathbb{K}$, $a \notin \mathbb{F}$. Then

$F(a) =$ field of all the fields intersections which are $\subset \mathbb{K}$ and conatin a,$\mathbb{F}$.

$\mathbb{F}(a)$ is minimal which contain a, and $\mathbb{F}$.

Theorem. $\mathbb{F} \subset * \subset \mathbb{K}$ *,* $a \in \mathbb{K}$*,* $a \notin \mathbb{F}$*. given* P *with coffcient in* $\mathbb{F}$*. (one variable) for every polynomials* P, Q *where* $P(a) \in \mathbb{K}, Q(a) \in \mathbb{K}$ *then* $F(a) = \left\{ \frac{P(a)}{Q(a)} \right\} \subseteq \mathbb{K}$.

for example we can take element in $\mathbb{C}$ which is not in $\mathbb{R}$, e.g., i. So $\mathbb{R}[i] = \left\{ \frac{P(i)}{Q(i)} \right\} = \mathbb{C}$. We can take any $z \in \mathbb{C}, z \notin \mathbb{R}$ then $\mathbb{R}[z] = \left\{ \frac{P(z)}{Q(z)} \right\} = \mathbb{C}$.

Theorem. *Given* $\mathbb{F} \subset \mathbb{K} \subset \mathbb{L}$*. then* $[\mathbb{L}, \mathbb{F}] = [\mathbb{L} : \mathbb{K}] \cdot [\mathbb{K} : \mathbb{F}]$.

Corollary. *If* $[\mathbb{L} : \mathbb{F}]$ *is prime then* $\mathbb{K} = \mathbb{F}$ *or* $\mathbb{K} = \mathbb{L}$*. Given,* $a \in \mathbb{K}, a \notin \mathbb{F}$ *also* $\mathbb{F} \subset \mathbb{F}(a) \subseteq \mathbb{K}$*. So if* $[\mathbb{K} : \mathbb{F}]$ *is prime then* $\mathbb{F}(a) = \mathbb{K}$.

Corollary. *Between* $\mathbb{C}$ *and* $\mathbb{R}$ *there are no fields. which contain* $\mathbb{R}$ *and* $\mathbb{C}$ *by the theorem.*

For example, let construct a field between $\mathbb{R}$ and $\mathbb{Q}$. we can take $\sqrt{7} \in \mathbb{R}, \sqrt{7} \notin \mathbb{Q}$, we can construct new field $\mathbb{Q}[\sqrt{7}]$

$$\mathbb{Q}[\sqrt{7}] = \frac{P(\sqrt{7})}{Q(\sqrt{7})} = \frac{q_1 + q_2\sqrt{7} + ... + q_n \left(\sqrt{7}\right)^n}{s_1 + s_2\sqrt{7} + ... + s_n \left(\sqrt{7}\right)^m}$$

where $q_i, s_i \in \mathbb{Q}, \gamma_1, \gamma_2 \in \mathbb{Q}$, so,

$$= \frac{\alpha_1 + \alpha_2\sqrt{7}}{\beta_1 + \beta_2\sqrt{7}} = \left\{ \gamma_1 + \gamma_2\sqrt{7} \right\}$$

Tutorial 1.

Exercise. Let X be a set and let $R = P(X)$ with the following operations,

$$A + B = A \triangle B = (A \backslash B) \cup (B \backslash A)$$

$$A \cdot B = A \cap B$$

Show that $(R, +, \cdot)$ is a accostiave ring with unit.

Solution. Note that $(R, +)$ is abelian group, also

$$A \triangle (B \triangle C) = (A \triangle B) \triangle C$$

- $0 \in R$ is the nutral element $0 = \emptyset$ because,

$$A \triangle \emptyset = (A \backslash \emptyset) \cup (\emptyset \backslash A) = A$$

- The additio inverse $A \in R$ is the set itself,

$$A \triangle A = (A \backslash A) \cup (A \backslash A) = \emptyset$$

  i.e. $-A = A$
- Distributivity, we need to show that,

$$A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$$

  This is true from set theory because,

$$= \{x \mid \text{x belong to exactly one from } A \cap B \text{ or } A \cap C \ \}$$

  for now this is ring.

We need to show accosiative multiplicstion property because intersection of set is accosiative, also cummotative, and exist unit element which is $X \in R$ its implies that $A \cap X = A, \forall A \in R$.

Exercise. Let R be a ring in which $x^2 = x$ for all $x \in R$ (boolean ring becuase as we know $1 + 1 = 0$ and $1 \cdot 1 = 1$)

Example. $(R = P(X), \triangle, \cap)$ we can see that $x \cap x = x$.

(1) show that $x + x = 0$ for all $x \in R$
(2) Show that R is cummotative

Solution. Let start with 1. first we want to know what is

$$x + x$$

and we know that $x^2 = x$ so we know that,

$$x + x = (x + x)^2 = (x + x)(x + x)$$

now we have distributivity,

$$x(x + x) + x(x + x) = x^2 + x^2 + x^2 + x^2 = 4x$$

Since, its abelian group relative to addition (fron definition of ring), so we get,

$$0 = x + x$$

Now, R is cummumutative, let $x, y \in R$ we need to show that $xy = yx$, note that

$$(x + y) = (x + y)(x + y) = x^2 + yx + xy + y^2$$

$$= x + yx + xy + y$$

Since there is inverse to addition $x + y + xy$ we get from section 1 that each element in inverse of it self in the boolean ring hence,

$$xy = yx$$

Exercise. Give a exmaple to a ring with unit in which there is right inverse and not left inverse and vice-versa.

Solution. R is acccosiative with unit, $a \in R$ is not invertible if exists $b \in R$ in which $ab = 1$ so in this case b has no inverse from left and a has inverse from right. We can define $R = \{f : \mathbb{R} \to \mathbb{R}\}$ where multiplication is function composition and addition is function addition $(f+g)(x) = f(x)+g(x)$. Let $R = \{f : V \to V\}$ where V is vector space over $\mathbb{R}$ instead of choosing $\mathbb{R}$. When is $(R, +, \cdot)$ is ring, regarding addition it will be abelian group, now we should treat the distribuitivity property, i.e.,

$$(f \circ (g + h))(x) = f \circ g(x) + f \circ h(x)$$

so what we want is

$$f(g(x) + h(x)) = f(g(x)) + g(h(x))$$

There is no reasson that it will be true for every function but this is true for linear function, so we can take $R = Hom(V, V) = \{T : V \to V |\ \text{T linear}\}$, where V is a vector space. Now, R is ring since $(R, +)$ is abelian, and the addition is

accosiative because V is abelian group, the $0 \in R$ it the constant map 0 and we have distributivity because we have linearity property

$$(f(g+h))(x) = f(g(x)+h(x))$$

and from linearity property we can use now that,

$$f(g(x)+h(x)) = (fg+fh)(x)$$

The unit, is the identity map. Now, found our ring and in this ring exists elements which has inverse from one side, for V which is finite dimensional one side inverse $\iff$ inverse, so we can take $V = \mathbb{R}[x]$ which is infinite dimensional, we want to find $f \in R$ linear map which is injective and not surjective (vise-versa) so we can take

$$f : \mathbb{R}[x] \to \mathbb{R}[x]$$

define by,

$$f(p(x)) \to xp(x)$$

This is injective and not surjective since there is no constant polynomials, and we saw that injective map means that there is left inverse and surjective yields eight inverse, since its injective and not surjective we get a ring as want, however, still need to show that its injective which is easy, take $p_1(x) \neq p_2(x)$ we want to show taht $f(p_1(x)) \neq f(p_2(x))$ where $p_1(x) = \sum a_i x^i, p_2(x) \sum b_i x^i$ i.e.,

$$f(p_1(x)) = x\sum a_i x^i \neq x\sum b_i x^i = f(p_2(x))$$

and the inverse in this case of f is $g : \mathbb{R}[x] \to \mathbb{R}[x]$ defined as follows,

$$g(p(x)) = \frac{1}{x}(p(x) - p(0))$$

we want can see that $g \cdot f = I$.

Example. Take $p(x) = 3x^3 + x^2 + x^2 - \frac{1}{2}x + 17$, so

$$f(p) = 3x^4 + x^3 + x^3 - \frac{1}{2}x^2 + 17x + 0$$

$$g(f(p)) = 3x^3 + x^2 + x^2 - \frac{1}{2}x + 17$$

so we can see that gf is the Id map.

Question 1.3 from HW1. Given tha table we need to fill it

+	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	
d	d	a		

note the at first this is the addition table of a abelian group, so note that, $d+c = b$ i.e.,

+	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

so we got that $a = 0$ and its cycle group respect to addition generated by b since

$$b + a = b, b + b = c, b + c = d, b + d = a$$

i.e, $< R, + >=< b >$ so we may think about it as $Z_4 = \{0, 1, 2, 3\}$, now the mutilication table must look as follow,

*	a	b	c	d
a	0	0	0	0
b	0			
c	0			
d	0			

now b^2 could it be 0? note that $b + b = c$ from the addition table, so

$$c^2 = (b + b)^2 = b^2 + b^2 + b^2 + b^2 = 0$$

but this is a group with order 4 i.e., adding the same element 4 times must give 0 hene, $c^2 = 0$

*	a	b	c	d
a	0	0	0	0
b	0			
c	0		0	
d	0			

note that we could do it as the standard table of Z_4 however, there are lot of options which would give also a table of group, if we assume that $b = 1$ then we get,

*	a	b	c	d
a	0	0	0	0
b	0	b	c	d
c	0	c	0	
d	0	d		

then

$$cd = (b + b)(b + b + b) = 6b^2 = 2b^2 = b + b = c$$

hence,

*	a	b	c	d
a	0	0	0	0
b	0	b	c	d
c	0	c	0	c
d	0	d	c	d

so this is multiplication table of Z_4 other option is when $d = 1$ we will get the same i.e., syysmteric table, so also there is one way to fill the multiplication table and get Z_4 multiplication table.

Remark. We can't choose $c = 1$ or $a = 1$ because we know that $c^2 = 0, a^2 = 0$.

Corollary. *So the main target was given a table of addition to a group, and using the table given we were required to fill the multiplication table so the two tables define a ring, the only way in which we could doit is to fill the table as Z_4 becasue we know that Z_4 is a ring.*

Homomorphisms. Given $\phi : R \to S$ where R, S are rings that imply in which

$$\phi(x+y) = \phi(x) + \phi(y)$$
$$\phi(xy) = \phi(x)\phi(y)$$

Where in the left side $+, \cdot$ is in R and in the right side operations in S.

Exercise. How many homomorphisms there is from $Z_6 \to Z_6$.

Solution. For the addition groups $(Z_6, +)$, every homomorphism ϕ must satisfy, $\phi(x) = ax$ where $a = \phi(1)$ because 1 generate the cycle group respect to addition, for which a value we have that $\phi(x) = ax$ define a homorphism of rings? we need to show that, $\forall x, y$.

$$\phi(xy) = \phi(x)\phi(y) = ax \cdot ay = a^2xy$$

namely for $x = y = 1$ we need so show that satisfied $a^2 = a$ so the options are $a = 0, 1, 2, 3, 4$ for $a = 0$ we get $\phi = 0$ is the trivial, and for $a = 1$ we get $\phi = id$ for $a = 3$ i.e., $\phi(x) = 3x$ from the justification above its homorphism, the same for $a = 4$, we get that $\phi(x) = 4x$ so in total there is 4 homomorphisms.

Exercise. Is there non trivisl homomorphisms from $2Z \to 3Z$.

Solution. NO! Assume there is $\phi : 2Z \to 3z$ we need to show that $\phi = 0$, denote by $a = \phi(2)$ then for all $n \in \mathbb{N}$ we have $\phi(2n) = an$. Namely,

$$a^2 = \phi(2 \cdot 2) = \phi(4) = \phi(2+2) = 2a$$

so $a = 0, 2$ by $2 \notin 3Z$ hence, $a = 0$ so $\phi(0)$.

Definition. integral domain is a nonzero commutative ring in which the product of any two nonzero elements is nonzero.

Exercise. Let $\phi : R \to S$ homomorphism where R, S are integral domains with unit. Assume that $\phi \neq 0$ then $\phi(1_R) = 1_S$.

Remark. In genereal homomorphism doesn't send unit to unit but we will see that if we have intergral domains then this is the case.

Solution. We need to show that $\phi(1_R) = 1_S$ let $x \in R$ s.t. $\phi(x) \neq 0$. Now,

$$\phi(x) = \phi(x \cdot 1_R) = \phi(x) \cdot \phi(1_R)$$

So,

$$\phi(x) - \phi(x)\phi(1_R) = 0$$

$$\iff \phi(x)\left(1_S - \phi(1_R)\right) = 0$$

so by definition of integral domain since S is integral domain then

$$1_S - \phi(1_R) = 0 \Rightarrow 1_S = \phi(1_R)$$

Exercise. Is there no trivial homomorphism from $\mathbb{Q} \to \mathbb{Z}$.

Solution. Toward condiction, let $\phi : \mathbb{Q} \to \mathbb{Z}$ we will show that $\phi = 0$. Denote, $\phi(1) = a$ now that,

$$a = \phi(1) = \phi(1 \cdot 1) = a^2$$

hence, $a = 0, 1$. If $a = 1$ then

$$1 = \phi(1) = \phi(\frac{1}{2} + \frac{1}{2}) = 2\phi(\frac{1}{2})$$

so contradiction, becuase we don't have $\phi(\frac{1}{2}) = y \in \mathbb{Z}$ in which $1 = 2y$. Hence, $a = 0$. Now. for all x we have $\phi(x) = \phi(1)\phi(x) = 0$ i.e., $\phi = 0$.

Remark. if $\phi : \mathbb{Q} \to \mathbb{C}$ is homomorphism then $\phi = 0$, $\phi = id$.

Example. Find all the homomorphisms from $\mathbb{Q}[x] \to \mathbb{C}$.

Solution. Let $\phi : \mathbb{Q}[x] \to \mathbb{C}$ homomorphism, from remark above we have that,

$$\phi|_{\mathbb{Q}} = \left\{ \begin{array}{c} \equiv 0 \\ \equiv id \end{array} \right\}$$

i.e., $\forall q \in \mathbb{Q}$, if $\phi \mid_{\mathbb{Q}} = 0$ then for all $p(x) \in \mathbb{R}$,

$$\phi(p(x)) = \phi\left(\sum a_i x^i\right) = \sum \phi(a_i)\phi(x^i) = 0$$

Otherwise, (its the case where $\phi(a) = a$ for all $a \in \mathbb{Q}$)

$$\phi(p(x)) = \phi\left(\sum p_i x^i\right) = \sum a_i \phi(x^i)$$

denote by $\phi(x) = \zeta \in \mathbb{C}$ then,

$$\phi(p(x)) = \sum_{i \geq 0} a_i \zeta^i = p(\zeta)$$

Corollary. *Each homomorphism $\phi : \mathbb{Q}[x] \to \mathbb{C}$ is in form $\phi \equiv 0$ or $\phi(p(x)) = p(\zeta)$ for all $\zeta \in \mathbb{C}$.*

Exercise. Are the following ring isomorphic?

(1) $\mathbb{Z}_{25}, \mathbb{Z}_5 x \mathbb{Z}_5$
(2) $\mathbb{R}, \mathbb{C}$

Solution. 1. We can see that they are not isomorphic becuase in $\mathbb{Z}_{25}$ there is element in which we add it to it self 24 times which is $\neq 0$ however, in $\mathbb{Z}_5 x \mathbb{Z}_5$ its not the case because it get 0 after 5 times. other approach is tho think about this two rings as groups with addition and i.e., $(\mathbb{Z}_5 x \mathbb{Z}_5, +), (\mathbb{Z}_5, +)$ which are not isomorphicc becuase one of them cyclic and other not,

Theorem. *Every group isomorphic to a cyclic group is also cyclic.*

Proof. Let G be a cyclic group and $f : G \to H$ be an isomorphism to another group H. Let a be a generator for G. We'll show that $f(a)$ is a generator for H. Let y be an element of H, and let x be $f^{-1}(y)$ so that $f(x) = y$ Since a generates G, therefore $x = an$ for some integer n. Then $f(x) = f(a^n) = (f(a))^n$, which shows that y is some power of $f(a)$. Thus, $f(a)$ generates H, and H is also a cyclic group. □

Theorem. $\mathbb{Z}_m x \mathbb{Z}_n \cong \mathbb{Z}_{mn} \iff gcd(m, n) = 1$.

So by theorems above, we can state that $(\mathbb{Z}_5 x \mathbb{Z}_5, +), (\mathbb{Z}_5, +)$ not isomorphic as groups.

Regarding 2, assume toward contradictiton that exists $\phi : \mathbb{C} \to \mathbb{R}$ then, $\phi(1) = 1$ ($\mathbb{C}, \mathbb{R}$ are integral domain) but now, $\phi(i)^2 = \phi(i^2) = \phi(-1) = -1 \in \mathbb{R}$ becuase there is no $x \in \mathbb{R}$ in which $x^2 = -1$.

Definition. Given R ring cummotative with unit, a ideal $I \lhd R$ is a subset which satisfy,

(1) $(I,+) \leq (R,+)$ (subgroup respect to addition)
(2) for $a \in I, x \in R$ then $ax \in I$ i.e., $IR \subseteq I$.

Example. Take all $n\mathbb{Z} \lhd \mathbb{Z}$ for example $2\mathbb{Z} \lhd \mathbb{Z}$ we can see that $2\mathbb{Z}$ is supgroup respect to addition because take $z_1 = 2x_1, z_2 = 2x_2$ then $z_1 - z_2 = 2(x_1 - x_2) \in 2\mathbb{Z}$ so subgroup of $\mathbb{Z}$, also for each element $2k = a \in 2\mathbb{Z}$ we have that for all $x \in \mathbb{Z}$ satisfied $2k \cdot x \in I = 2\mathbb{Z}$.

Example. If we have $a_1, ..., a_n \in R$ then we can look at the ideal generated from the element which is $(a_1, ..., a_n) = \{ax_1 + ... + a_n x_n | x_i \in R\}$ this is again ideal becuase the properties are satisfied.

Exercise. Let $R = \mathbb{Z}[x]$ and define

$$I_1 = \{f \in R | f(1) = 0\}$$

$$I_2 = \{f \in R | f(0) \in 2\mathbb{Z}\}$$

(1) Show that I_1, I_2 are ideals,
(2) Find generators

Solution. We can see that I_1 is a subgroup respect to addittion because $0 \in I_1$ (0 - polynomial), $\forall g, f \in I_1$ we have that $(f-g)(1) = f(1) - g(1) = 0 - 0 = 0$ so $f - g \in I_1$ so first requirment satisfied. Now, for every $f \in I, p \in R$ then $(pf)(1) = p(1)f(1) = p(1) \cdot 0 = 0$ i.e., $pf \in I$ so in total $I_1 \lhd R$. Regarding I_2 again, we have $0 \in I_2$ since 0 polynomial which is even. Now taking $f, g \in I_2$ then $(f-g)(0) = f(0) - g(0) \in 2\mathbb{Z}$. So sungroup of R respect to addition, also let $f \in I_2, p \in R$ then $(f \cdot p)(0) = f(0)p(0) \in 2\mathbb{Z}$ because $f(0)$ is even.

Finding generators. Given that $f(1) = 0$ then there is $p(x) \in \mathbb{R}[x]$ in which $f(x) = (x-1)p(x)$ if we can show that $p \in R$ then it will stem that $f(x) \in (x-1) \lhd R$ i.e., $I_1 \subseteq (x-1)$, note that for

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

then,

$$R \ni f = (x-1)p(x) = (x-1)\sum_{i=0}^{n} a_i x^i$$

$$= a_n x^{n+1} + (a_{n-1} - a_n)x^n + ... + (a_0 - a_1)x - a_0$$

where we know that $f \in R$ so all the coeffceint must be in $\mathbb{Z}$ so all $a_i \in \mathbb{Z}$ i.e., $p \in R$. I.e., we have that $I_1 \subseteq (x-1)$ in the other hand $x - 1 \in I_1$ so the ideal generated by $(x-1) \subseteq I_1$. so $(x-1) = I_1$. Now, general element in I_2 is in form of $p(x) = \sum_{i=1}^{n} a_i x^i + 2a_0$, where $a_i \in \mathbb{Z}$

$p(x) = \sum_{i=1}^{n} a_i x^i + 2a_0 = x \sum_{i=1}^{n} a_i x^{i-1} + 2a_0 \in (x, 2)$ i.e., $I_2 \subseteq (x, 2)$, now we need to show the other direction, let $f(x) \in (x, 2)$ we need to show that $f \in (x, 2)$ take,

$$f = p(x) \cdot x + q(x) \cdot 2 \in (x, 2)$$

$$f(0) = 0 \cdot p(0) + 2 \cdot q(0) \in 2\mathbb{Z}$$

so $f \in I_2$ i,e., $I_2 = (x, 2)$. Could we generate I_2 with less than 2 polynomials? Assume toward contradiction that $I_2 = (p(x))$ i.e., one generated then in this case for all $0 \neq f \in I_2$ we will have that $degp \leq degf$ and we know that $2 \in I_2$ so $deg(p) = 0 \Rightarrow p(x) = \pm 2$ and we can see that $I_2 \neq (\pm 2)$ because for example $x \in I_2$ but $x \notin (\pm 2)$.

Remark. if $\phi : R \to S$ then $ker\phi \lhd R$.

Example. $I_1 = ker(\phi)$ where $\phi : \mathbb{Z}[x] \to \mathbb{Z}$ where $\phi(f) = f(1)$.

Example. $I_2 = ker(\phi)$ where $\phi : \mathbb{Z}[x] \to \mathbb{Z}_2$ where $\phi(f) = f(0)$. where $ker(\phi) = \{f : f(0) =_{mod2} 0\}$

Quontient ring.

Definition. Given $I \lhd R$ then $(R/I, +)$ is a group respect to addition then we can define multiplication $(x + I)(y + I) = xy + I$ (where a general element in the quontien ring is a coset $x + I$ or $y + I$ where x, y are represnetors) defined well, and define on R/I multiplication then its a ring.

Examples.

(1) $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$
(2) $\mathbb{R}[x]/(x) \cong \mathbb{R}$ because for all $p(x)$ satisfied $p(x) - p(0) \in (x)$ i.e., every coset $p(x) + I = p(0) + I$ so $\mathbb{R}[x]/(x) = \{t + (x) : t \in \mathbb{R}\} \cong \mathbb{R}$

In group terminology. Assuming we have a group $\mathbb{Z}$ (also ring) and for it there are infinite infinite ideal already we saw before $n\mathbb{Z}$, we can define the quontint ring $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ for example consider $n = 5$ then we will get 4 different cosets,

$$0 + 5\mathbb{Z}, 1 + 5\mathbb{Z}, 2 + 5\mathbb{Z}, 3 + 5\mathbb{Z}, 4 + 5\mathbb{Z}$$

$$= 0 + I, 1 + I, 2 + I, 3 + I, 4 + I$$

Remark. Element in $0 + 5\mathbb{Z}$ are called trivial in quontient.

note the coset is not a ideal it self however we can see that coset+coset is also coset so we can see that cosets form a ring, then this ring is called quontient ring and written as $\mathbb{Z}/5\mathbb{Z}$. So we can generalize for claim. Note that the ideal here is $n\mathbb{Z}$.

Claim. Let N be an ideal of a ring R. Then the additive cosets of N form a ring R/N with the binary operations defined by $(a + N) + (b + N) = (a + b) + N$ and $(a + N)(b + N) = ab + N$. exa

Proof. By addition and multiplication are well-defined. We know that the additive cosets form an additive group, since ideal N is an additive subgroup of ring R, and so N is a normal subgroup since $< R, + >$ is abelian. Associativity and the distribution laws follow from the same properties in R. □

Exercise. Let $R = P[x_1, x_2] = \left\{ \sum_{i,j} a_{ij} x_1^i x_2^j : a_{ij} \in \mathbb{R} \right\}$ where $I = (x_1 x_2, x_1^2 + x_2^2)$ describe the quontient ring R/I.

Solution. When $p(x_1, x_2) + I = q(x_1, x_2) + I$? $\iff$ $p(x_1, x_2) - q(x_1, x_2) \in I$

Example. (For example in case of $Z/5Z$ if we take $a, b \in \{1 + 5z)$ coset then $a - b \in (1 - 5z)$)

Now, take $p(x_1, x_2) = \sum a_{ij} x_1^i x_2^j$ for all $i, j > 0$ satisfied that $x_1^i x_2^j \in I$ as a multiplication of one of the generators in the idea which is $x_1 x_2$ so,

$$p(x_1, x_2) + I = \sum_{\forall i \text{ where} j=0} a_{i0} x_1^i + \sum_{\forall j \text{where} i=0} a_{0i} x_2^j + I$$

Note that,

$$x_1^3 = \underbrace{(x_1^2 + x_2^2)x_1}_{\in I} - \underbrace{x_2^2 x_1}_{\in I}$$

so $x_1^n, n > 2$ is trivial in the quontient i.e., it gives 0 module $(x_1 x_2, x_1^2 + x_2^2)$ because also,

$$x_1^n = \underbrace{(x_1^2 + x_2^2)x_1^{n-2}}_{\in I} - \underbrace{x_2^2 x_1^{n-2}}_{\in I}$$

the same for x_2^n. so x_1^n, x_2^n are trivial in quontient. moreover, $x_1^2 + I = -x_2^2 + I$ because $x_1^2 + x_2^2 \in I$ so on total in order to define a coset in the quontient ring, we care about monomials in form,

$$\left\{a + bx_1 + cx_1^2 + dx_2 + I : a, b, c \in R\right\}$$

$$= span_R \left\{1 + I, x_1 + I, x_1^2 + I, x_2 + I\right\}$$

Claim. $span_R \left\{1 + I, x_1 + I, x_1^2 + I, x_2 + I\right\}$ is a base because they are linearly independent.

Exercise. Given $R = P(x_1, x_2)$ where $I = (x_1 x_2, x_1^2 + x_2^2)$ we saw that

$$R/I = \left\{a + bx_1 + cx_1^2 + dx_2 + I : a, b, c \in R\right\}$$

because $x_1 x_2 \in I, x_1^n, x_2^m \in I$ for all $n, m > 2$ also $x_1^2 + I = -x_2^2 + I$ i.e., $R/I = span_R \left\{1 + I, x_1 + I, x_1^2 + I, x_2 + I\right\}$ we clim that its a base i.e., the representatiokn $a + bx_1 + cx_2 + dx_1^2 = 0$ i.e., $a + bx_1 + cx_2 + dx_1^2 \in I$ so exists $p, q \in R$ with

$$a + bx_1 + cx_2 + dx_1^2 = p(x_1, x_2)x_1 x_2 + q(x_1, x_2)(x_1^2 + x_2^2)$$

in the right side there is not free coeffctient hence $a = 0$ also there is no coeffctient of $\alpha x_1, \beta x_2$ so $b = 0, c = 0$ now we get that $dx_1^2 = p(x_1, x_2)x_1 x_2 + q(x_1, x_2)(x_1^2 + x_2^2)$

Claim. Each element in R/I could be represented in unique way as $a + bx_1 + cx_2 + dx_1^2$. for multiplication.

Proof. Its enough to show for all the base elements, $\left\{1, x_1, x_2, x_1^2\right\}$, observe that

$$x_1 x_2 = 0$$

becasue $x_1 x_2 \in I$

$$x_1 x_1^2 = x_1^3 = 0$$
$$x_2 x_2 = x_2^2 = -x_1^2$$

$$x_2 x_1^2 = 0$$

$$x_1^2 x_1^2 = 0$$

$$x_1 x_1 = x_1^2$$

Now, take $p(x), q(x) \in R/I$ so,

$$p(x) = a + bx_1 + cx_2 + dx_1^2$$

$$q(x) = a' + b'x_1 + c'x_2 + d'x_1^2$$

So,

$$p(x)q(x) = \left(a + bx_1 + cx_2 + dx_1^2\right)\left(a' + b'x_1 + c'x_2 + d'x_1^2\right)$$

$$= aa' + x_1\left(ab' + a'b\right) + x_2\left(ac' + a'c\right) + \left(ad' + a'd + bb' - cc'\right)x_1^2$$

where $aa', \left(ab' + a'b\right), \left(ac' + a'c\right), \left(ad' + a'd + bb' - cc'\right) \in R$ and $p(x)q(x) \in span\left\{1, x_1, x_2, x_1^2\right\} = R/I$ □

Before discussing next exercise, we are going to discuss euclidean ring,

Definition. A ring R is Euclidean if it is an integral domain (i.e. a commutative ring without zero divisors) and there exists a map $d : R\backslash 0 \to 0, 1, , 2, ...$ such that:

(1) 1. For any$a, b \in R$, $a, b \neq 0$we have $d(a) \leq d(ab)$
(2) 2. For any $a, b \in R$,$a, b \neq 0$there exist $p, r \in R$ such that $b = pa + r$ where either$r = 0$ or $d(r) < d(a)$.

Theorem. *Any non-trivial ideal in an Eucledean ring is 1-generated.*

Exercise. Find generator to $\mathbb{Z} \rhd (123, 36)$.

Solution. We will use Algorithm,

$$123 = 3 \cdot 36 + 15$$

$$36 = 2 \cdot 15 + 6$$

$$15 = 6 \cdot 2 + 3$$

$$6 = 3 \cdot 2 + 0$$

Also, we can write $a \cdot 123 + b \cdot 36 = gcd(123, 36) = 3$ where $a = 5, b = -17$. so each element in

$$a \cdot 123 + b \cdot 36 = gcd(123, 36) = 3$$

is divisible by 3 hence, $(123, 36) \subseteq (3)$ and since $3 = 5 \cdot 123 - 17 \cdot 36$ then $(3) \subseteq (123, 36)$ so we got that $(3) = (123, 36)$.

Exercise. Find generator to $P[x] \rhd (x^2 + 7x + 6, x^2 - 5x - 6)$.

Solution. We will use the euclidean algorithm,

$$x^2 + 7x + 6 = 1 \cdot \left(x^2 - 5x + 6\right) + 12x + 12$$

$$x^2 - 5x - 6 = (12x + 12)\left(\frac{1}{12}x - \frac{1}{2}\right) + 0$$

So $I = (12x + 12) = (x + 1)$ because in genreal $(cp(x)) = (p(x))$ for all $c \in \mathbb{R}$.

Exercise. Find generator for $\mathbb{Z}_5[x] \rhd (x^4+4, x^5+2x^4+4x^2+1)$.

Solution. Euclidean algorithm again,

$$x^5+2x^4+4x^2+1 = (x+2)(x^4+4)+4x^2+x+3$$

$$x^4+4 = \left(4x^2+4x+1\right)\left(4x^2+x+3\right)+2x+1$$

$$4x^2+x+3 = (2x+1)(2x+2)+1$$

$$(2x+1) = 1\cdot(2x+1)+0$$

so $I=(1)=\mathbb{Z}_5[x]$

Theorem. *$R \rhd M$ is maximal $\iff$ R/M field.*

Definition. An ideal $I \subset R$ is called maximal if there are no ideal $\tilde{I} \subset R$ such that $I \subset \tilde{I}$ and $\tilde{I} \neq R$.

Example. Given $I = I_a = \{f : f(a) = 0\}, R = C^0[0,1]$ for $a \in [0,1]$ in homeworks we saw that I_a is maximal we can show that R/I_a is a field (clearly hard task), let use the definiyion, let J be and ideal of $C([0,1])$ s.t., $I \subset J$ so there is $g \in J\backslash I$ (i.e., $g(a) \neq 0$) for every $f \in C([0,1])$ we have that,

$$f = \left(f - \frac{f(1)}{g(1)}g\right) + \frac{f(1)}{g(1)}g \in J$$

since $\left(f-\frac{f(1)}{g(1)}g\right) \in J$, $\frac{f(1)}{g(1)}g \in J$ therefore, $J = C([0,1])$ and I is maximal ideal.

Claim. $R/I_a = \mathbb{R}$.

Proof. let $\phi : R/I_a \to \mathbb{R}$ we will shiw that ϕ is isomorphism$\phi(f+I_a) = f(a)$ its defined well because $f+I_a = g+I_a$ then $f-g \in I_a$ i.e., $(f-g)(a) = 0$ i.e., $f(a) = g(a)$. Homomorphism,

$$\phi(f+g+I_a) = (f+g)(a) = f(a)+g(a)$$

$$= \phi(f+I_a)+\phi(g+I_a)$$

And similar for multiplocation. Note that ϕ is injective becuase if $\phi(f+I_a) = 0$ then $f(a) = 0$ i.e., $f(a) \in I_a$ i.e., $f(a)$ is in the trivial quontient hence, $ker\phi = \{0+I_a\}$. Surjective because for $t \in \mathbb{R}$ for $f \equiv t \in C^0[0,1]$ we get that $\phi(f+I_a) = f(a) = t$ so ϕ is isomorphism □

Exercise. Let $P_1(x) = x^2-1, P_2(x) = x^3+\lambda$ for which $\lambda \in R$ (neccesary and suffcient condition)the ideal generated is maximal?

Solution. In order to ensure that ideal generate is maximal we need first to make sure that the $gcd(p_1,p_2)$ is a prime (irrducible) this will tell us that the ideal is maximal using homeworks exercises, first note that the euclidean algorithm will not work because we have no λ in our hand, instead we know that x^2-1 is reudcable and $x^2-1 = (x-1)(x+1)$ so, we want to find $\lambda \in R$ in which

$$x^3+\lambda = (x-1)(x+1)g(x)$$

where $deg(g(x)) = 1$ recall $g(x) = ax+b$ so,

$$x^3+\lambda = (x-1)(x+1)(ax+b)$$

$= (x^2-1)(ax+b) = ax^3+bx^2-ax-b$

clearly in this case we have that so we get that $b = -\lambda = 0$ and $a = 0$ so no such a λ. Now, suppose that we have $g(x) = ax^2+bx+c$ in which $deg(g(x)) = 2$ s.t.,

$$x^3+\lambda = (x-1)g(x)$$

so we get that,

$$x^3+\lambda = (x-1)\left(ax^2+bx+c\right)$$

$$= ax^3+bx^2+cx-ax^2-bx-c$$

$$= ax^3+(b-a)x^2+(c-b)-c$$

Note that, $a = 1$ and $c = -\lambda$ where $b-1 = 0, c-b = 0$ hence, $a = 1, b = 1, c = 1 = -\lambda \Rightarrow \lambda = -1$. Therefore,

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

which is irriducible in contradiction that g is not irriducalbe then there must be polynomial $ax+b \in \mathbb{R}[x]$ in which $a \neq 0$ s.t $ax+b \mid g$ so we must get that $x = -\frac{b}{a}$ is root but g has no root in R because its means that $g(x) = 0$ i.e., because $g(x) > 0$ we can show that by taking any $x > 1$ $x < -1$ or $0 < x < 1$ if $x > 1$ or $x < -1$ then obvious otherwise $x^2+1 > x$ for all $-1 < x < 1$. Now, again, we need to find $g(x) = ax^2+bx+c$ where $deg(g) = 2$

$$x^3+\lambda = (x+1)(ax^2+bx+c)$$

$$x^3+\lambda = ax^3+(a+b)x^2+(b+c)x+c$$

where $a = 1, a+b = 0, b+c = 0, c = \lambda$ so $b = -1, c = 1$ and $\lambda = 1$ in this case, we have

$$g(x) = x^2-x+1$$

which is irriducable over $\mathbb{R}$ because

$$x^2-x+1 = \frac{1}{4}(2x-1)^2+\frac{3}{4} > 0$$

So, $\lambda = \pm 1$.

Exercise. Show that $\mathbb{Z}_2[x] \rhd (x^2+x+1) = I$ is maximal.

Solution. We will show that R/I is field, by dividing with remainder we get that $R/I = \{a+bx+I | a, b \in \mathbb{Z}_2\}$ because for every $p(x) \in R$ if we write it as $p(x) = q(x)(x^2+x+1)+ax+b$ then $p(x) = I+ax+b$ now we have 4 element that span $R/I = \{1, x, 1+x, 0\}$ we will show that its field, i.e, each element has inverse, note that $x(x+1) = x^2+x = x^2+x+1-1 = 1$ (because $-1 mod 2 = 1$) so $x^{-1} = (1+x), (1+x)^{-1} = x$ so evey element has inverse therefore, x^2+x+1 is maximal.

Theorem. *p is prime if and only if there are no zero divisors in the quotient ring.*

Claim. Every prime is non invertible.

Motivation. Let $R = \mathbb{R}[x]$ consider the ring $\mathbb{R}[x]/(x^3+1)$ the element of this factor are the cosets $\left\{c_1 + c_2x + c_3x^2\right\}, c_1, c_2, c_3 \in \mathbb{R}$. A coset is a zero divisor in $\mathbb{R}[x]/(x^3+1)$ if exists $(d_1, d_2, d_3) \in \mathbb{R}$ where

$$\left(c_1 + c_2x + c_3x^2\right)\left(d_1 + d_2x + d_3x^2\right) = 0 \in \mathbb{R}[x]/(x^3+1)$$

observe that $x^4 = -x, x^3 = -1$ so we will have,

$$(c_1d_1) + (c_1d_2 + c_2d_1)\,x + (c_3d_1 + d_3x_1 + c_2d_2)\,x^2 + (c_2d_3 + c_3d_2)\,x^3 + (c_3d_3)x^4$$
$$= (c_1d_1 - c_2d_3 - c_3d_2) + (c_1d_2 + c_2d_1 - c_3d_3)\,x + (c_3d_1 + d_3c_1 + c_2d_2)\,x^2$$

So, we got,

$$c_1d_1 - c_2d_3 - c_3d_2 = 0$$

$$c_1d_2 + c_2d_1 - c_3d_3 = 0$$

$$c_3d_1 + d_3c_1 + c_2d_2 = 0$$

Equivalent to the following system of equation,

$$\begin{pmatrix} c_1 & -c_3 & -c_2 \\ c_2 & c_1 & -c_3 \\ c_3 & c_2 & c_1 \end{pmatrix}\begin{pmatrix} d_1 \\ d_2 \\ d_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

Therefore $c_1 + c_2x + c_3x^2$ is not a zero divisor in $R[[x]]/(x^3+1)$ if and only if $detA \neq 0$.

Exercise. Consider a coset $c1 + c2x + c3x2 \in R[[x]]/(x^3+1)$. If $c_1 + c_2x + c_3x^2 \in (x+1)$ or $c_1 + c_2x + c_3x^2 \in (x^2 - x + 1)$ then obviously thios coset is a zero divisor in$R[[x]]/(x^3+1)$. Is the converse true?

Solution. Note that $I = (x^3+1)$ and, $R/I = \left\{c_1 + c_2x + c_3x^3 + I \mid c_1, c_2, c_3 \in \mathbb{R}\right\}$. if $p(x) + I$ is zero divisor then exsits $q \neq 0$ in which

$$p(x)q(x) = (x^3+1)r(x) = (x+1)(x^2 - x + 1)r(x)$$

(because zero diviser must obtain the trivial quontient i.e., all the multiplication in $x^3 + 1$)

since $(x+1), (x^2 - x + 1)$ are irriducable from the uniquness of decomposition each if them devide one of $p(x), q(x)$ and note possible both of them divide $q(x)$, $deg(q) \leq 2$ hence one of them divide $p(x)$.

Exercise. Prove that the quotient ring $P[[x1, x2]]/(x_1x_2, x_1^2 + x_2^4)$ is isomorphic to R^6 with a certain multiplication. Let $e_1, ..., e_6$ be the standard basis of R^6.Find $e_i \cdot e_j$ for all $1 \leq i, j \leq 6$.

Solution. Denote $I = \left(x_1x_2, x_1^2 + x_2^4\right)$. Now

$$P[[x_1, x_2]]/I = \{c_1\{1\} + c_2\{x_1\} + c_3\{x_2\} + c_4\{x_1^2\} + c_5\{x_2^2\} + c_6\{x_2^3\} : c_i \in \mathbb{R}\}$$

First notice that for all $i, j \geq 1$ satisfied that $x_1^i x_2^j \in I$. In addition for all $k \geq 3$ satisfied $x_1^k \in I$. Now we will classify polynmials which aer not in I since $I = \{p(x_1, x_2) \cdot x_1x_2 + q(x_1, x_2) \cdot (x_1^2 + x_2^4) : p, q \in P[[x_1, x_2]]$. Notice that $x_1 \notin I$ becuase each term which contain a power of 1 derived from the multiplication $p(x_1, x_2) \cdot x_1x_2$ however it contains x_2. Similarly, we conclude that $1, x_2, x_2^2, x_2^3 \notin I$ we will claim that also $x_1^2 \notin I$ this term could be derived only from $q(x_1, x_2)(x_1^2 + x_2^4)$ for $q \equiv 1$ but this is impossible since $p(x_1, x_2) \cdot x_1x_2 = 0$ in identical wat

$x_2^4 \notin I$. Note that we classified the possible monomylias of x_1, x_2. Notice that sice $x_1^2 + x_2^4 \in I$ implies $\{x_1^2\} = -\{x_2^4\}$ hence, $\{\{c \cdot x_1^2\} : c \in \mathbb{R}\} = \{\{c \cdot x_2^4\} : c \in \mathbb{R}\}$ except this linear combination there is no other linear combination which is in I of monomylians (From similar claim we discussed above) hence each linear combination represnet a differenct coset. (Since if there are two linear combination represent the same coset then the differene is a combanation in I). Lets define isomorphism $\phi : P[[x_1, x_2]]/I \to \mathbb{R}$ by

$$\phi\left(c_1\{1\} + c_2\{x_1\} + c_3\{x_2\}, c_4\{x_1^2\} + c_5\{x_2^2\} + c_6\{x_2^3\}\right) = (c_1, c_2, c_3, c_4, c_5, c_6)$$

We will find e_i, e_j as required, $(i, j) = (2, 3), (2, 5), (2, 6), (3, 4), (4, 5), (4, 6)$ we will get $\phi^{-1}(e_i e_j)$ is a mixede term of powers so in I using the observation in the exercise, I.e., $e_i e_j = 0$ for all (i, j) where $i = 1$ we get

$$e_i e_j = \phi(\{1\}) \cdot \phi(\{p(x)\}) = \phi(\{1\}\{p(x)\}) = \phi(\{p(x)) = e_j$$

Other pairs we can find manually,
$e_2 e_2 = \phi(\{x_1\})\phi(\{x_1\}) = \phi\left(\{x_1^2\}\right) = e_4$
$e_2 e_4 = \phi(\{x_1\})\phi\left(\{x_1^2\}\right) = \phi\left(\{x_1^3\}\right) = \phi(\{0\}) = 0$
$e_3 e_5 = \phi(\{x_2\})\phi\left(\{x_2^2\}\right) = \phi\left(\{x_2^3\}\right) = e_6$
$e_3 e_6 = \phi(\{x_2\})\phi\left(\{x_2^3\}\right) = \phi\left(\{x_2^4\}\right) = -e_4$
$e_4 e_4 = \phi\left(\{x_1^2\}\right)\phi\left(\{x_1^2\}\right) = \phi\left(\{x_1^4\}\right) = \phi(\{0\}) = 0$
$e_5 e_5 = \phi\left(\{x_2^2\}\right)\phi\left(\{x_2^2\}\right) = \phi\left(\{x_2^4\}\right) = -e_4$
$e_5 e_6 = \phi\left(\{x_2^2\}\right)\phi\left(\{x_2^3\}\right) = \phi\left(\{x_2^5\}\right) = \phi(\{0\}) = 0$
$e_6 e_6 = \phi\left(\{x_2^3\}\right)\phi\left(\{x_2^3\}\right) = \phi\left(\{x_2^6\}\right) = \phi(\{0\}) = 0$

Motivation from lecturea. Note that if I ideal is prime then R/I is integral domain, and if I is maximal ideal then R/I is field. A very important observation to know is that not every prime ideal is maximal, however, if ideal is maximal it must be prime. So if I ideal which is not prime then the quontient ring R/I will have zero divisors so R/I is not integral domain. Now, in term of polynomial rings, we could state that R/I has zero divisiorn if $I = (p(x))$ is not prime i.e., reducable. Becuase note that if there is zero divisior then it mean for $p(x)$ exists $q(x) \neq 0 \in R$ where $pq = 0_R$ (where 0_R is the trivial quontient ring i.e., all polynomial $r(x)$ generated by $p(x)$) so $p(x)q(x) = p(x)r(x)$ now if $p(x)$ is reducalbe into $g(x)m(x)$ then each of $g(x), m(x)$ must divide on of p, q so we found a pair p, q where $pq = 0$, this is not the case when p irrducable i.e., prime becuase then we will have no pair p, q which give polynomial in the quontient ring and hencefore no zero divisors.

Exercise. Let $(R^3, \cdot)$ be a cummutative ring with the standard sum and such that(assuming WLOG that identity element is e_1) where $\forall j[3], e_1 \cdot e_j = e_j, e_2^2 = e_3, e_3^2 = e_3 - e_1 - e_2, e_2 e_3 = e_3 - e_1$ where e_1, e_2, e_3 is that standard basis of $\mathbb{R}^3$. Find polynomial $p(x) \in R[x]$ s.t. the ring $(\mathbb{R}^3, \cdot)$ is isomrphic to $R[x]/p(x)$ and find $p(x)$.

Solution. First, denote $p(x) = p_0 + p_1 x + p_2 x^2 + p_3 x^3$ we know that p must be degree 3. Hence, the quontient ring $\mathbb{R}[x]/I = \left\{c_0 + c_1 x + c_2 x^2 \mid c_0, c_1, c_2 \in \mathbb{R}\right\}$ where $I := (p(x))$, define isomorphism $\phi : \mathbb{R}[x]/I \to (R^3, \cdot)$ where we can define,

(1) $\phi(1 + I) = e_1$
(2) $\phi(x + I) = e_2$
(3) $\phi(x^2 + I) = e_3$

Because, $\forall j[3], e_1 \cdot e_j = e_j, e_2^2 = e_3$. Now, following the requirements in the question we will obtain the follows, since $e_3^2 = e_3 - e_2 - e_1$

$$\phi(x^4 + I) =_{Def} \phi(x^2 + I)\phi(x^2 + I) = e_3^2 = e_3 - e_2 - e_1$$

hence,

$$x^4 + I = \phi^{-1}(e_3 - e_2 - e_1) = \phi^{-1}(e_3) - \phi^{-1}(e_2) - \phi^{-1}(e_1) = x^2 - x - 1 + I$$

Now, since, $e_2 e_3 = e_3 - e_1$ we get that,

$$\phi(x^2 + I)\phi(x + I) = \phi(x^3 + I) = e_3 - e_1$$

Therefore,

$$x^3 + I = \phi^{-1}(x^3 + I) = \phi^{-1}(e_3 - e_1) = \phi^{-1}(e_3) - \phi^{-1}(e_1) = x^2 - 1 + I$$

Define

$$p(x) = p_0 + p_1 x + p_2 x^2 + p_3 x^3$$

where we know that,

$$x^3 = x^2 - 1$$

Hence,

$$p(x) = p_0 + p_1 x + p_2 x^2 + p_3(x^2 - 1)$$

$$= (p_0 - p_3) + p_1 x + (p_2 - p_3)x^2$$

Solution. (Other approach).

First

Exercise. Which cosets in the following factor rings are zero divisors? Which cosets are invertible?

(1) $\mathbb{R}[x]/(x^4 + 1)$
(2) $\mathbb{R}[x]/(x_1^2, x_2^2)$ (left as exercise)
(3) $\mathbb{R}[x]/(x_1 x_2)$ (left as exercise)

Solution. (1). Observe that $R[[x]]/(x^4 + 1)$. Denote$I := (x^4 + 1)$. Let us analyze this quotient ring: similarly to earlier exercises, from polynomial division with remainder we obtain that any $p(x) \in R[[x]$ is of the form$p(x) = (x^4+1)\cdot q(x)+r(x)$ where $deg\,(r(x)) < 4$ and so

$$\{p(x)\} = p(x) + (x^4 + 1) = r(x) + (x^4 + 1) = \{r(x)\}$$

The representation is unique because assume that is r_1, r_2 where $deg(r_1), deg(r_2) < 4$ so $deg(r_1 - r_2) < 4$ hence $r_1 - r_2 \notin I$, as we saw any coset is a zero divisor if and only if its not invertible, let us find the zero divisors, assume that $c(x)$ which define cost $\{c(x)\} = \{c_0 + c_1 x + c_2 x^2 + c_3 x^3\}$ then exists $\{d(x)\} = \{d_0 + d_1 x + d_2 x^2 + d_3 x^3\}$ s.t.,

$$c(x)d(x) = (x^4 + 1)q(x)$$

(because zero diviser must obtain the trivial quontient i.e., all the multiplication in $x^4 + 1$) hence,

$$c(x)d(x) = (x^4 + 1)q(x) = (x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1)q(x)$$

and $(x^2 + \sqrt{2}x + 1), (x^2 - \sqrt{2}x + 1)$ do not decompose into linear factors, we conclude from the equation that one of $(x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1)$ divides $c(x)$ (exactly one, since $deg\,(c(x)) \leq 3$). Therefore we obtain that the zero divisors in the

quotient ring are of the form $c(x)$ for $c(x) \in (x^2+\sqrt{2}x+1)$ or $c(x) \in (x^2-\sqrt{2}x+1$. By the proposition we stated earlier, these are exactly the non-invertible elements (the rest are invertible).

Remark. Each $M \lhd R \iff R/M$ field. Also, in ring with unit, every non trivial ideal is contained in maximal ideal (Zorn Lemma)

Observation used in exercise. Given $x \in R$ non invertible $\iff (x) \notin R$ because if invertible then we can get the unit from (x) and then we get all the ring because unit generate all the ring.

Exercise. Given R cummumutaive ring with unit in R there is unique maximal ideal $\iff$ all the non invertible element in R constitute ideal.

Solution. $\Leftarrow$: Let $M \lhd R$ be a maximal ideal we need to show that the set of not invertible elements is ideal, we claim that $M = R\backslash R^*$ where $R^* = \{\text{non invertible elements }\}$, note that $M \subseteq R\backslash R^*$ because M is non trivial ideal i.e., each element in M must be non invertible otherwise (we can get the unit from invertible element which yields $M = R$ which is contradiction because M non trivial). In the other hand, if $x \in R\backslash R^*$ then from uniquness of M we get that $(x) \subseteq M$ so $x \in M$ i.e., $R\backslash R^* \subseteq M$ hence, $R\backslash R^* = M$. In the other direction assume that $R\backslash R^* \lhd R$ then we will show that M is the only maximal ideal i.e., $M \neq R$ but but $I \subseteq M$ for all $I \lhd R$ and indeed $M \neq R$ because $1 \notin M$ and M is maximal becuase there in no ideal $\neq R$ doesn't contain invertible elements.

Example. Let $R = \left\{ \frac{a}{b} | 2 \neq b \right\}$ then each $\alpha \in R$ we can write in form $\alpha = 2^n \cdot \frac{a}{b}$ where $n \geq 0$ and a, b are disjoint (R is ring, we can show it easily). Namely, note that x is invertible $\iff n = 0$ becuase the only thing annoy us from inversing x is dividing in it by 2 but we can't divide in $R/$ hence, $R\backslash R^* = (2)$ i.e., all element generated by 2 are not invertible, hence by exercise (2) is maximal ideal and unique. Also, $\frac{\mathbb{R}}{(2)} \cong \mathbb{Z}_2$. because

Fact. *The ideals in R are,*

$$... \subseteq (2^3) \subseteq (2^2) \subseteq (2^1)$$

Exercise. Let $R = \mathbb{C}[x]/(x^2)$ find zero divisors and invertible elements.

Solution. For polinom $p(x) = \sum_{i=0}^{n} p_i x^i$ so in the quontient $\{p(x)\} = \{p_0 + p_1 x\}$. For each polinom could be represnted as one representor in the quontient with degree 1. Note that if we have two representors the same $\{a + bx\} = \{c + dx\}$ then $(a - c) + (b - d)x = 0$ so $a = c, b = d$. Hence, $R = \{\{a + bx\} | a, b \in \mathbb{C}\}$ and multiplication,

$$\{a + bx\}\{c + dx\} = \{ac + adx + bcx + bdx\}$$

$$= \{ac + \{ad + bc\} x\}$$

if

$$a + bx, c + dx \neq 0$$

and

$$ac + \{ad + bc\} x = 0$$

(i.e., zero divisors) so, $ac = 0, bc + ad = 0$ WLOG $c = 0$ then we assume that $d \neq 0$ so we have zero divisor $' \iff$ in form $\{bx\} = \{dx\}$. Now, to find the invertible elements, assume that $a \neq 0$ is $\{a + bx\}$ invertible? we need to find c, d where

$$ac + (ad + bc) = 1$$

so $ac = 1, ad + bc = 0$ hence $c = \frac{1}{a}, d = -\frac{-b}{d}$ i.e., each element which is not zero divisor is invertible hence,

$$\{a + bx\}^{-1} = \left\{ \frac{1}{a} - \frac{b}{a^2} x \right\}$$

Exercise. Let $R = \mathbb{C}[x]/(x^2)$ and let $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ show that $R \cong S$ where

$$S = \mathbb{C}[A] = \{aI + bA|, a, b \in \mathbb{C}\} \subseteq M_2(\mathbb{C})$$

$$= \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : a, b \in \mathbb{C} \right\}$$

Note that this is group becuase closed to addition and for multiplication,

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \begin{pmatrix} c & d \\ 0 & c \end{pmatrix} = \begin{pmatrix} ac & ad + bc \\ 0 & ac \end{pmatrix}$$

For S there is base as a vector space on $\mathbb{C}$ where $e_1 = A, e_2 = A$ and satisfied,

$$(e_1 + be_2)(ce_1 + de_2) = ace_1 + (ad + bc)e_2$$

i.e., $e_1 \cdot e_1 = e_1, e_2 \cdot e_1 = e_2, e_2 \cdot e_2 = 0$. rom here we get that $S \to R$ which take $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \to \{a + bx\}$ is homomorphism injective and surjective.

Remark. We may think the quontient ring above as homomrphism to all the matrices which give 0 when power 2 those matrices are well known to us - Nilpotent matrices.

Exercise. Given $R = \mathbb{R}[x_1, x_2]/(x_1x_2, x_2^2)$ find zero divisors and invertible elements.

Solution. Let $p(x_1, x_2) = \sum p_i x_1^i x_2^j$ now observe that every $x_1^i x_2^j, i, j > 0$ then $x_1^i x_2^j \in I$ i.e.,

$$\{p(x_1, x_2)\} = \left\{ \sum_i p_{i0} x_1^i + \sum_j p_{0j} x_2^i \right\}$$

note that for all x_2^m where $m > 2$ also $x_2^m \in I$ hence, in total,

$$\{p(x_1, x_2)\} = \left\{ p_{00} + \sum_{i>0} p_{j0} x_1^i + p_{01} x_2 \right\}$$

i.e., $R = \{\{p(x_1) + bx_2\}\}$ where $p(x_1) \in \mathbb{R}[x_1], b \in \mathbb{R}$, (this represnetation is unique because $\left((x_1x_2, x_2^2)\right) \cap \{\{p(x_1) + bx_2\}\} = \{0\}$). I.e., R is a vector space with base

$$\left\{ \{1\}, \{x_1\}, \left\{x_1^2\right\}, ..., \{x_2\} \right\}$$

Note that multiplication in R is defined as,

$$\left(\{p(x_1) + bx_2\} \{q(x_1) + cx_2\}\right)$$

$$= \{p(x_1)q(x_1) + (p_0c + q_0b)\, x_2\}$$

(where $bcx_2^2 \in I$ so its 0), what are the zero dividors? assume that,

$$\{p(x_1) + bx_2\}, \{q(x_1) + cx_2\} \neq 0$$

and,

$$\{p(x_1) + bx_2\}\{q(x_1) + cx_2\} = 0$$

so in this case $p(x_1)q(x_1) = 0$ and $p_0c + q_0b = 0$ from the first constrain either p, q is the 0 polynomial WLOG q is the 0 polynomial in which case $p_0c = 0$ but if $q = 0$ then $c \neq 0$ so $p_0 = 0$ so in total we got zero dividors in form, $\{x_1f(x_1) + ax_2\}, \{0 + dx_2\}$ but $\{0 + dx_2\} \subset \{x_1f(x_1) + ax_2\}$ so in total $\{x_1f(x_1) + ax_2\}$, where $f(x) \in \mathbb{R}[x], a \in \mathbb{R}$. Now, to find invertible elements in the quontient ring, we need to find,

$$\{p(x_1) + bx_2\}\{q(x_1) + cx_2\} = \{1\}$$
$$\Rightarrow \left\{ \begin{array}{c} p(x_1)q(x_1) = 1 \\ p_0x + q_0b = 0 \end{array} \right\}$$

if $p, q \neq 0$ are and in this case $b = -\frac{p_0}{q_0}c$hence, we get

$$\{a + bx_2\}^{-1} = \left\{ \frac{1}{a} - \frac{b}{a^2} \right\}, a \neq 0$$

. Note that there are elements which are not invertible and not zero divisor e.g., $\{x_1 + 1\}$.

Exercise. Let R be cummutative ring with unit, assume that R is also F vector space where $F \subseteq R$ field, $dim_F R < \infty$ then if a not zero divisor $\to a$ invertible.

Solution. Define $f : R \to R$ where $x \to ax$ linear transformation, we claim that f is F linear indeed,

$$f(x + y) = a(x + y) = ax + ay = f(x) + f(y)$$

also,

$$f(\lambda x) = a(\lambda x) =_{Cummutative-Ring} \lambda(ax) = \lambda f(x)$$

Now, note that,

$$kerf = \{x : ax = 0\} = \{0\}$$

since a is not zero divisor hence f is injective and since $dim_F R < \infty$, f is linear map $\Rightarrow f$ is surjective so exsists x s.t. $ax = 1$ i.e., a is invertible.

Exercise. (4.5) Let $R = \mathbb{R}[x]/(x^3 - x^2 - 4x + 4)$ show that $x^2 + x - 1$ is invertible and find the inverse.

Solution. First, we will find the non-invertible element in the quontient ring, observe that,

$$(x^3 - x^2 - 4x + 4) = (x - 1)(x - 2)(x - 2)$$

Namely, for x^2+x-1 there is no common factor hence, not zero divisor (so invertible by claim we showed earlier). Now lets find the inverse, we need to find $p(x) \in \mathbb{R}[x]$ in which $p(x)\left\{x^2 - x - 1\right\} = \{1\}$, i.e., we need to find $q(x) \in \mathbb{R}[x]$ s.t.

$$p(x)(x^2 + x - 1) = q(x)(x^3 - x^2 - 4x + 4) + 1$$

so we will use the euclidean algorithm,

$$(x^3 - x^2 - 4x + 4) = (x - 2)x^2 + x - 1) - x + 2$$

$x^2+x-1=(-x-3)(-x+2)+5$

Therefore,

$$5=(x^2+x-1)+(x+3)(-x+2)$$

$=\left(x^2+x-1\right)+(x+2)\left(\left(x^3-x^2-4x+4\right)-(x-2)(x^2+x-1)\right)$

$=(x-3)(x^3-x^2-4x+4)+(-x^2-x+7)(x^2+x-1)$ And in the quontient, $(x-3)(x^3-x^2-4x+4)=0$ since $(x^3-x^2-4x+4)\in I$

$$\left\{\left(-x^2-x+7\right)\right\}\left\{\left(x^2+x-1\right)\right\}=\{5\}$$

hence,

$$\left\{x^2+x-1\right\}^{-1}=\left\{-\frac{1}{5}x^2-\frac{1}{5}x+\frac{7}{5}\right\}$$

Remark. In general if $\{f(x)\}$ invertible in $\mathbb{F}[x]/(g(x))$ then with euclidean algorithm we will find p,q in which

$$f(x)p(x)+g(x)q(x)\Rightarrow\{f(x)\}^{-1}=\{p(x)\}$$

Obserevation. Let

$$p_1(x)=-\frac{1}{3}(x^2-4)=-\frac{1}{3}(x-2)(x+2)$$

$$p_2(x)=\frac{1}{4}(x^2+x-2)=\frac{1}{4}(x-1)(x+2)$$

$$p_3(x)=\frac{1}{12}\left(x^2-3x+2\right)=\frac{1}{12}\left(x-1\right)\left(x-2\right)$$

Denote by e_i the representor of the polynomial p_i in the quontient ring. Note that e_1,e_2,e_3 is a base for vector space over $\mathbb{R}$. Indeed the transformation matrix from the base $\left\{\{1\},\{x\},\left\{x^2\right\}\right\}$ is given by,

$$\begin{pmatrix} -\frac{1}{3} & 0 & \frac{4}{3} \\ \frac{1}{4} & \frac{1}{4} & -\frac{1}{2} \\ \frac{1}{2} & -\frac{1}{4} & \frac{1}{5} \end{pmatrix}$$

is invertible. And in order to understand the multiplication we need to understand e_i,e_j where for $i\neq j$ we have that $e_ie_j=0$ because each of them is a zero divisor, for

$$e_1^2=p(x)p(x)=\frac{1}{9}(x^4-8x^2+16)$$

$$=\frac{1}{9}(x-1)(x^3-x^2-4x+4)-\frac{1}{3}(x^2-4)=e_1$$

in identical way e_2^2,e_3^2 are found, so the mutiplication is defined as follows,

$$(a_1e_1+a_2e_2+a_3e_3)\cdot(b_1e_1+b_2e_2+b_3e_3)$$

$$=\sum a_ib_ie_i$$

e.g., $e_1+e_2+e_3=\{1\}$. Namely, $\sum a_ie_i$ is invertible $\iff$ $a_1,a_2,a_3\neq 0$ and the inverse is

$$\left(\sum a_ie_i\right)^{-1}=\sum a_i^{-1}e_i$$

for example,

$$x^2+x-1=e_1+5e_2+e_3$$

then the inverse is

$$\left\{x^2+x-1\right\}^{-1} = e_1 + \frac{1}{5}e_2 + e_3 = \left\{-\frac{1}{5}x^2 - \frac{1}{5}x + \frac{7}{5}\right\}$$

So $R \cong \mathbb{R}x\mathbb{R}x\mathbb{R} = \mathbb{R}^3$ where

$$e_i e_j = \delta_{ij} e_i$$

And using the isomorphism

$$\phi : \left(\sum a_i e_i\right) \to (a_1, a_2, a_3)$$

Exercise. Let $\mathbb{F}[x]$ where $p(x) = (x-\alpha_1)(x-\alpha_2)...(x-\alpha_n)$ where $\alpha_i \neq \alpha_j$ for all $i \neq j$. Then $\mathbb{F}[x]/\left(p(x)\right) \cong \mathbb{F}^n$.

Solution. Define map ϕ: $\mathbb{F}[x]/\left(p(x)\right) \to \mathbb{F}^n$ as $\{f(x)\} \to (f(\alpha_1), .., f(\alpha_n))$ we need to show that map is defined well, i.e., homomorphism injective and surjective, taking $f(x) - g(x) \in (p(x))$ then $\forall i$, $(f-g)(\alpha_i) = 0$ because $p(\alpha_i) = 0$ i.e., $f(\alpha_i) = g(\alpha_i)$ hence defined well, homomorphism left as exercise, injective and surjective, note that

$$ker\phi = \{\{f(x)\} \,|\forall i, f(\alpha_i) = 0\}$$

$$= \{\{f(x)\} \,|p(x) \mid f(x)\} = \{\{0\}\}$$

so ϕ injective, and surjetive becuase the discussed is $n - dim$ vector spaces over $\mathbb{F}$ and ϕ linear $\to$ ϕ is surjective.

Exercise. What is the representation matrix of ϕ (from previous exercise) relative to bases $\{(1,0,0....,0), ..., (0,0,....,1)\}\, E, \left\{\{1\}, \{x\}, \left\{x^2\right\}, ..., \left\{x^{n-1}\right\}\right\} = B$.

Solution. As we define ϕ we get that,

$$\{1\} \to_\phi (1,1,....,1)$$

$$\{x\} \to_\phi (\alpha_1, \alpha_2, ..., \alpha_2)$$

$$\vdots$$

$$\{x^{n-1}\} \to_\phi \left(\alpha_1^{n-1}, \alpha_2^{n-1}, ..., \alpha_2^{n-1}\right)$$

Hence,

$$[\phi]_B^E = \begin{pmatrix} 1 & \alpha_1 & & \alpha_1^{n-1} \\ 1 & \alpha_2 & \cdots & \alpha_2^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha_n & & \alpha_n^{n-1} \end{pmatrix}$$

This is the Vandermonde matrix, with determinant of,

$$det = \prod(\alpha_i - \alpha_j) \neq 0$$

Let $\tilde{e_1}, ..., \tilde{e_n}$ *be standard base of* $\mathbb{F}^n$ *and recall*

$$\phi^{-1}(\tilde{e_1}) = e_i = \{p_i(x)\}$$

where $deg(p_i) < n$ *we can classify* p_i *by where* ϕ *defined as* $\phi : \{f(x)\} \to (f(\alpha_1), .., f(\alpha_n))$ *i.e.,*

$$\phi(e_i) = (p_i(\alpha_1), .., p_i(\alpha_n))$$

where $\forall j$ *since we rake as a source to the standrd base the* $p_i(\alpha_j) = \delta_{ij}$ *for example,*

$$[e_i] = [p_i(\alpha_j)]_E = (0, ..., \textit{(i index)}1, .., 0)$$

where ϕ *take the vector which has* 1 *in index* i *and map it to*

$$\phi(e_i) = (p_i(\alpha_1), .., p_i(\alpha_n))$$

so there is only one unique polynomial of degree $< n$ *that imply*

$$p_i(x) = \frac{\prod_{i \neq j}(x - \alpha_j)}{\prod_{j \neq i}(\alpha_i - \alpha_j)}$$

. Therefore, if $p_i(x)$ is polynomial as follows $p_i(x) = \frac{\prod(x-\alpha_j)}{\prod(\alpha_i-\alpha_j)}$, (as defined in the obseervation) then $e_1, ..., e_n$ is base for $\mathbb{F}[x]/\left(p(x)\right)$ and satisfy, $e_{ij} = \delta_{ij}e_i$ i.e.,

$$\left(\sum a_i e_i\right) \cdot \left(\sum b_i e_i\right)$$

$$= \sum a_i b_i e_i$$

and for a polynomial $\{f(x)\} = \sum a_i e_i$ then

$$\{f(x)\} = \phi^{-1}\phi(f(x)) = \phi^{-1}\left((f(\alpha_1), ..., f(\alpha_n)\right)$$

$$= \phi^{-1}(\sum f(\alpha_i)\tilde{e_i}) = \sum f(\alpha_i)e_i$$

i.e., we got the $a_i = f(\alpha_i)$. For example, in the exercise 4.5 we saw that $p(x) = (x^3 - x^2 - 4x + 4) = (x - 1)(x - 2)(x - 2)$ i.e., product of monomials, hence, if we have a polynomial in the quontient ring of $R = \mathbb{R}[x]/(x^3 - x^2 - 4x + 4)$ defined by $e_i = p_i$ uinsg the formla $p_i(x) = \frac{\prod(x-\alpha_j)}{\prod(\alpha_i-\alpha_j)}$, so in this case,

$$p_1(x) = -\frac{1}{3}(x^2 - 4) = -\frac{1}{3}(x - 2)(x + 2) = e_1$$

$$p_2(x) = \frac{1}{4}(x^2 + x - 2) = \frac{1}{4}(x - 1)(x + 2) = e_2$$

$$p_3(x) = \frac{1}{12}\left(x^2 - 3x + 2\right) = \frac{1}{12}\left(x - 1\right)\left(x - 2\right) = e_3$$

then taking a coset

$$\{x^2 + x - 1\} = e_1 + 5e_2 + e_3$$

note that the coeffcient satisfy that for e_1 is plugging in 1 root $\alpha_1 = 1$ in $x^2 + x - 1 = 1 + 1 - 1 = 0$ and for e_2 is equivalent to plug in the root $\alpha_2 = 2$ because note appearing as root in p_2 so we get $2^2 + 2 - 1 = 5$ and for e_3 we plug in $\alpha_3 = -2$ so we get $4 - 2 + -1 = 1$. (So we got a very nice relation for polynmyals and there representation coset in fact we can calculate them with out long division, e.g., take $x^4 + 4$ in the quontient ring $R = \mathbb{R}[x]/(x^3 - x^2 - 4x + 4)$ is equal to plugging in 1

for getting coffcient of e_1 and plugging in 2 for getting coeffcient of e_2 and plug in -2 for getting coeffcient of e_3 so in total

$$x^4 + 4 = 5e_1 + (2^4 + 4)e_2 + ((-2)^4 + 4)e_3$$

$$= 5e_1 + 20e_2 + 20e_3 = ... = 5x^2$$

as same we get in long division.