

Groups and Rings

Kexing Ying

May 15, 2020

1 Rings

1.1 Recap

We shall omit ring axioms but note that we will in general refer to rings without the multiplicative identity unless it is prefixed with **unital**. Simply put,

Definition 0.1 (Unital Ring). *An unital ring is a triplet $(R, +, \times)$ such that $(R, +)$ forms an additive abelian group and (R, \times) forms a multiplicative monoid such that \times distributes over $+$.*

Definition 0.2 (Ring). *A ring is a unital ring without the necessary condition of the multiplicative identity.*

Some obvious properties can be deduced right away.

Theorem 1. *Let R be a ring,*

- (Zero annihilates) $0x = x0 = 0$;
- (Negation distributes) $-xy = (-x)y = x(-y)$.

Proof. Omitted. □

Definition 1.1 (Unit). *Let R be a ring. We say $x \in R$ is a unit if and only if it has an multiplicative inverse. We write $U(R) := \{x \in R \mid \exists x^{-1} \in R, xx^{-1} = 1_R = x^{-1}x\}$.*

Proposition 1.1 (Unit Group). *Let R be an unital ring, then $U(R)$ is a multiplicative group and we call it the unit group.*

Furthermore, a lot of obvious definitions common to all algebraic structures are exactly what they sound like. These include **subring**, **ring homomorphism**, and **unital ring homomorphism**.

Theorem 2. *Let $\phi : R \rightarrow S$ be an ring homomorphism. Then $\phi(0_R) = 0_S$ and $\forall x \in R$, $\phi(-x) = -\phi(x)$. Furthermore, if ϕ is an unital ring homomorphism, then $\forall x \in U(R)$, $\phi(x) \in U(S)$ and $\phi(x^{-1}) = \phi(x)^{-1}$.*

Proof. First two property follows from R and S being additive groups while the last follows from the properties of the unit group. \square

From this theorem, we see that $\phi(U(R)) \leq U(S)$.

Given an abelian group $(G, +)$, we can construct a trivial ring structure by extending it with the binary operation $\times : G \rightarrow G \rightarrow G : a, b \mapsto 0_G$. We call this a **trivial multiplicative structure**. We call a ring **trivial** if it only contains one element, thus $0 = 1$ if the ring is unital. In fact, the reverse is also true; an unital ring contains only one element (so trivial) if $0 = 1$ as $\forall x \in R, x = x \times 1_R = x \times 0_R = 0_R$.

1.2 Integral Domains & Polynomial Rings

Definition 2.1 (Zero divisor). *Let R be a ring and $x \in R$. We say x is a left zero divisor if there is some $y \in R^* = R \setminus \{0_R\}$ such that $xy = 0_R$. Similar definition for the right zero divisor.*

The ring $M_2(\mathbb{F})$ has zero divisors for any field \mathbb{F} while $\mathbb{Z}/p\mathbb{Z}$ does not have any zero divisors for p a prime. We say a ring R is an integral domain if it is a non-trivial commutative unital ring with no zero divisors.

Theorem 3. *Let R be an integral domain. Then $\forall x \in R^*, y, z \in R, xy = xz \implies y = z$.*

Proof. Fix x, y, z and suppose $y \neq z$, then $y + (-z) \neq 0$ and so $x(y + (-z)) \neq 0$ as x is not a zero divisor. $\#$ \square

Theorem 4. *If R is a finite integral domain, then it is a field.*

Proof. We need to show $U(R) \supseteq R^*$. Let $a \in R^*$, then by the previous theorem, the map $x \mapsto ax$ is injective. As R is finite, the map is also surjective. \square

A similar argument can be used to show that given an integral domain R that is a finite vector space over some field F , R is a field.

Let R be a commutative unital ring, we define

$$R[X] := \left\{ \sum_{i=0}^n a_i X^i \mid a_i \in R, n \in \mathbb{N} \right\},$$

the set of R -polynomials. $R[X]$ forms a commutative ring with the obvious operations.

The following statements are equivalent:

1. R is an integral domain;
2. $R[X]$ is a integral domain;
3. for every $p, q \in R[X]^*$, $\deg pq = \deg p + \deg q$;
4. for every $p \in R[X]^*$, p has at most $\deg p$ number of roots.

where R is a non-trivial commutative unital ring.

Proof. $2 \implies 1$ trivially and $3 \implies 2$ by contrapositive. We will now show that $1 \implies 3$, $4 \implies 1$ and $1 \implies 4$.

Suppose R is an integral domain, $p, q \in R[X]^*$ such that $p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$ and $q(x) = b_m x^m + b_{m-1} x^{m-1} + \dots + b_0$ where $a_n \neq 0_R \neq b_m$ (so $\deg p = n$ and $\deg q = m$).

So, we have

$$(pq)(x) = \left(\sum_{i=0}^n a_i x^i \right) \left(\sum_{j=0}^m b_j x^j \right) = \sum_{i=0}^n \sum_{j=0}^m a_i b_j x^{i+j},$$

i.e. $\deg pq \leq n + m$. Now, as the coefficient of x^{n+m} is $a_n b_m$, both of which are non-zero, as R is an integral domain, $a_n b_m \neq 0_R$, thus, $\deg pq = n + m$.

We will prove $4 \implies 1$ by contrapositive. Suppose R is not an integral domain, i.e. there exist $a, b \in R^*$ such that $ab = 0_R$. Consider the polynomial $R[X]^* \ni p = x \mapsto ax$. While $\deg p = 1$, p has two roots, 0_R and b respectively, contradicting 4.

Lastly, we show $1 \implies 4$ by induction on the degrees. Let $p \in R[X]$, if $\deg p = 0$ then there exists some $a \in R^*$, $p = x \mapsto a$ which does not have any roots since $a \neq 0_R$. Now, suppose $\deg p = n + 1$ and let λ be a root. Then

$$p(x) = p(x) - p(\lambda) = \sum_{i=0}^{n+1} a_i (x^i - \lambda^i) = (x - \lambda) \sum_{i=0}^{n+1} a_i (x^{n-1} + \dots + \lambda x^{n-1}) = (x - \lambda)q(x),$$

for some $q \in R[X]$ with degrees less than or equal to n . Now, by the inductive hypothesis, q has at most n roots so let us define the set

$$r := \{x \mid x = \lambda \vee q(x) = 0_R\}.$$

It is obvious that all elements of r are roots of p and $|r| \leq n + 1$ so it suffices to show that these are the only roots. Let $\mu \in R \setminus r$, then $x - \mu \neq 0_R \neq q(\mu)$ and hence $p(\mu) = (x - \mu)q(\mu) \neq 0_R$ as by assumption, R is an integral domain. \square

A direct corollary of the above, specifically $1 \iff 2$ means $U(R[X])$ is the set of constant polynomials $p = x \mapsto a \in R$ where $a \in U(R)$. This means that $U(R) \cong U(R[X])$ by the homomorphism $i = a \mapsto (x \mapsto a)$.

Definition 4.1 (Nilpotent). *Given some ring R , $x \in R$, x is called nilpotent if and only if there exists some $d \in \mathbb{N}$ such that $x^d = 0_R$.*

Given some integral domain R , we can construct a field $\text{Frac}(R)$. Let $\text{Frac}(R)$ be the equivalence classes of $R \times R^*$ by the relation $(a, b) \sim (a', b') \iff ab' = a'b$. Then $\text{Frac}(R)$ is a field by equipping it with

$$+ = (a, b), (a', b') \mapsto (ab' + a'b, bb'),$$

and

$$\times = (a, b), (a', b') \mapsto (aa', bb').$$

By checking using the definition above, with ι being an injective unital homomorphism, we see that for all fields \mathbb{F} , if there exist some ϕ such that $\phi : R \rightarrow \mathbb{F}$ is an injective unital

ring homomorphism, then there exists a unique homomorphism ψ such that the following diagram commutes.

$$\begin{array}{ccc} R & \xrightarrow{\iota} & \text{Frac}(R) \\ & \searrow \phi & \downarrow \psi \\ & & \mathbb{F} \end{array}$$

1.3 Ideals & Quotients

Definition 4.2 (Ideal). *Given R a ring, we say I is an ideal if it is an additive subgroup of R and for all $r \in R$, $x \in I$, $rx, rx \in I$. We denote this by $I \triangleleft R$.*

The relation between a ring and its ideals is similar to that of normal subgroups and groups. A ring has two trivial ideals, the zero ideal and itself, so the only ring with less than two ideals is the trivial ring $\{0\}$. Also, given some ring homomorphism $\phi : R \rightarrow S$, $\ker \phi \triangleleft R$.

By some easy checking, we see that ideals are closed under finite sum and intersections, i.e. if $(I_i)_{i=1}^n$ is a sequence of ideals, so is $\sum_{i=1}^n I_i$, and if \mathcal{I} is a non-empty family of ideals, $\bigcap \mathcal{I}$ is also an ideal. The second point is important as it allows us to talk about ideals generated by sets. We write $\langle r_1, \dots, r_n \rangle$ for the ideal generated by $(r_i)_{i=1}^n \subseteq R$ and $\langle S \rangle$ for the ideal generated by the set $S \subseteq R$.

It is easy to see that; given some ring R , for all $S \subseteq R$, $I \triangleleft R$, $S \subseteq I \implies \langle S \rangle \leq_{Gp} I$ and $1_R \in S \implies \langle S \rangle = R$.

Theorem 5. *Let R be a non-trivial unital commutative ring, then R is a field if and only if the only ideals in R are $\{0_R\}$ and R itself.*

Proof. Forward direction follows as 1_R is in any non-trivial ideals, while the backwards direction follows by considering $xR = R$ for all $x \in R$. \square

From this we see that any ring homomorphisms from a field \mathbb{F} to a ring R , $\phi : \mathbb{F} \rightarrow R$ is either $x \mapsto 0_R$ or injective. With this we can see that the sequence of rings

$$\mathbb{Z} \hookrightarrow \mathbb{Q} \hookrightarrow \mathbb{R} \hookrightarrow \mathbb{C},$$

while has forward injective ring homomorphisms with the inclusion map has only the zero ring homomorphisms backwards.

Theorem 6. *Let R be a unital ring with ideal $I \triangleleft R$, then $R/I := \{r + I \mid r \in R\}$ is a ring with the operations $(a + I) \hat{+} (b + I) = (a + b) + I$ and $(a + I)(b + I) = ab + I$.*

Definition 6.1 (Quotient Map). *Given ring R , and $I \triangleleft R$, we define the quotient map $q : R \rightarrow R/I : x \mapsto x + I$. q is a surjective unital ring homomorphism with the kernel I .*

We again meet the first isomorphism theorem this time with regards to rings.

Theorem 7. Let R, S be unital rings and $\phi : R \rightarrow S$ a unital ring homomorphism, then the map

$$\psi : R/\ker \phi \rightarrow S : x + \ker \phi \mapsto \phi(x)$$

is a well-defined injective unital ring homomorphism such that the following diagram commute.

$$\begin{array}{ccc} R & \xrightarrow{q} & R/\ker \phi \\ & \searrow \phi & \downarrow \psi \\ & & S \end{array}$$

Note that this is equivalent to $R/\ker \phi \cong S$ whenever ϕ is surjective.

Similarly, we also meet the *correspondence theorem* again.

Theorem 8. Let R be a ring and $I \triangleleft R$, then the map between the set of ideals greater than I is order isomorphic to the set of ideals of R/I .

Proof. Use the map

$$\mathcal{Q} : \{I' \triangleleft R \mid I \subseteq I'\} \rightarrow \{J \triangleleft R/I\} : I' \mapsto q(I').$$

\mathcal{Q} is well-defined as for $I' \triangleleft R$, $I \subseteq I'$, $q(I') \triangleleft R/I$ since for all $a, b \in I'$, $a + b \in I'$ so $(a + I) + (b + I) \in q(I')$ and for all $r \in R$, $a \in I'$, $ra, ar \in I'$ so $(r + I)(a + I) = ra + I \in q(I')$ and $(a + I)(r + I) = ar + I \in q(I')$. \square

Here is a funny exercise. Suppose there exists a proper non-trivial ideal I in \mathbb{Z} greater than $\langle p \rangle$ for some prime p , then, there is some $x \in (I)$, $x \notin \langle p \rangle$, so $\gcd(x, p) = 1$. By Bezout's lemma, there is some $a, b \in \mathbb{Z}$ such that $1 = ax + bp \in I + \langle p \rangle \subseteq I$, so $I = \mathbb{Z}$. So by the correspondence theorem, $\mathbb{Z}/\langle p \rangle$ has no non-trivial proper ideal. In fact this can be seen by the fact that $\mathbb{Z}/\langle p \rangle = \mathbb{F}_p$ which is a field.

1.4 Product Structure on Rings

Let $(R_i)_{i \in I}$ be a family of unital rings, then there is a natural product ring structure on the Cartesian product $\prod_{i \in I} R_i$ such that $U(\prod_{i \in I} R_i) = \prod_{i \in I} U(R_i)$ and the projection map $\pi_j : \prod_{i \in I} R_i \rightarrow R_j : x \mapsto x_j$ is an unital ring homomorphism.

Note that the inclusion map $\iota_j : R_j \rightarrow \prod_{i \in I} R_i$ is a ring homomorphism not necessarily of an unital one. Also, the product ring does not preserve integral domain, i.e. for all $i \in I$, R_i is an integral domain does **not** imply $\prod_{i \in I} R_i$ is also an integral domain.

We call ideals $I, J \triangleleft R$ **coprime** if $I + J = R$. This terminology is used as $\langle x \rangle + \langle y \rangle = \mathbb{Z}$ if and only if x, y are coprime in \mathbb{Z} .

Lemma 1. Let R be a ring and $I_1, I_2 \triangleleft R$ such that I_1, I_2 are coprime, then for all $a, b \in R$,

$$(a + I_1) + (b + I_2) = R.$$

Proof. Let $r \in R$, then, as I_1, I_2 are coprime, there exists $x \in I_1, y \in I_2$ such that $x + y = r + (-a) + (-b)$ so $(a + x) + (b + y) = r$. \square

Theorem 9. Let R be ring and $I_1, I_2 \triangleleft R$ such that I_1, I_2 are coprime. Then

$$R/(I_1 \cap I_2) \cong R/I_1 \times R/I_2.$$

Proof. Consider the mapping $\psi : R \rightarrow R/I_1 \times R/I_2 : r \mapsto (r + I_1, r + I_2)$. By checking, we find ψ to be a ring homomorphism with kernel $I_1 \cap I_2$. So, it suffices to prove that ψ is surjective by the first isomorphism theorem.

Let $(a + I_1, b + I_2) \in R/I_1 \times R/I_2$, then by the previous lemma, $(a + I_1) + ((-b) + I_2) = R$, so there exist $x \in a + I_1, y \in (-b) + I_2$ such that $x + y = 0_R$, i.e. $x = -y$. Now, as $x \in a + I_1, y \in (-b) + I_2$, we have $x - a \in I_1$ and $y + b \in I_2$. So, by considering $\psi(x) = (x + I_1, x + I_2) = (x + I_1, -y + I_2) = (a + (x - a) + I_1, b + -(y + b) + I_2) = (a + I_1, b + I_2)$ by the fact that $\alpha + I_1 = I_1 \iff \alpha \in I_1$. \square

The theorem above is normally referred to as the *Chinese remainder theorem* and we that, by induction, we can easily extend it to any finite number of ideals that are pairwise coprime, i.e.

Theorem 10. Let R be ring and $(I_i)_{i=1}^n$ be a finite sequence of ideals in R such that I_i, I_j are pairwise coprime for $i \neq j$. Then

$$\frac{R}{\left(\bigcap_{i=1}^n I_i\right)} \cong \prod_{i=1}^n R/I_i.$$

1.5 The Ring Structure of the Integers

The integers is the typical example that comes into mind when discussing rings and luckily it has many nice properties.

Definition 10.1 (Principle Ideal). We call an ideal $I \triangleleft R$ principle if and only if it is generated by one element.

Theorem 11. Every ideal in \mathbb{Z} is principle.

Proof. It is easy to show that every ideal in \mathbb{Z} is of the form $\langle n \rangle$. \square

Theorem 12. Suppose R is a unital ring. Then there is a unique unital ring homomorphism $\phi : \mathbb{Z} \rightarrow R$ such that,

$$\phi(k) = \begin{cases} 0_R, & k = 0 \\ \phi(k-1) + 1_R, & k > 0 \\ -\phi(-k), & k < 0 \end{cases}$$

By denoting the above unique ring homomorphism by χ_R given any unital ring R , we have by previous results $\ker \chi_R \triangleleft \mathbb{Z}$. Now, as \mathbb{Z} is principle, there exists some n , $\langle n \rangle = \ker \chi_R$. If we restrict this n to be non-negative, we find that n to be unique as if $\langle x \rangle = \langle y \rangle$ then $x \mid y$ and $y \mid x$, so $x = \pm y$.

Definition 12.1 (Characteristic). Given a unital ring R , the characteristic of R is the unique $n \in \mathbb{N}$ such that $\langle n \rangle = \ker \chi_R$.

By considering the inclusion map of \mathbb{Z} to \mathbb{Z} , \mathbb{Q} , \mathbb{R} , and \mathbb{C} , we find these rings all have characteristics 0.

Lemma 2. *Let \mathbb{F} be a field, R a ring and $\phi : \mathbb{F} \rightarrow R$ an ring homomorphism. Then there is a induced vector space of R over \mathbb{F} using the scalar multiplication $\times : \mathbb{F} \times R \rightarrow R : (f, r) \mapsto \phi(f)r$.*

From this we can deduce,

Theorem 13. *Suppose R be an integral domain of non-zero characteristic, then R has prime characteristic p and is a vector space over \mathbb{F}_p .*

Proof. The first part of the statement is trivial so it suffices to find some ring homomorphism from $\mathbb{F}_p \rightarrow R$ which is provided by the first isomorphism theorem. \square

1.6 Prime and Maximal Ideals

Definition 13.1 (Prime). *We call an ideal $I \triangleleft R$ prime if and only if it is proper and for all $a, b \in R$, $ab \in I$ implies $a \in I$ or $b \in I$.*

Straight away, we see that 0_R is prime in R if and only if R is an integral domain. Another example of a prime ideal is that, if R is an integral domain, then $\langle X \rangle$ is prime in $R[X]$. This is true by considering $p \in \langle X \rangle \iff p(0) = 0$, or alternatively, deduced straight away by the following theorem.

Theorem 14. *Let R be a commutative unital ring and $I \triangleleft R$ be a proper ideal. Then I is prime if and only if R/I is an integral domain.*

Proof. Straightforward contrapositive both ways. \square

Definition 14.1 (Maximal Ideal). *Let R be a ring and $I \triangleleft R$ is proper, we say I is maximal if and only if for all $J \triangleleft R$, $I \subseteq J \implies I = J$ or $J = R$.*

Theorem 15. *Let R be a commutative unital ring and $I \triangleleft R$ be a proper ideal. Then I is maximal if and only if R/I is a field.*

Proof. Follows directly from the fact that R/I is a field if and only if it has no proper non-trivial ideals. \square

Since a field is an integral domain, it follows that every maximal ideal is also prime.

It is not at all obvious that all rings have a maximal ideal, but this nice property turns out to be true using *Zorn's lemma*.

Theorem 16. *Let (X, \leq) be a non-empty poset. If each chain C in X has an upper bound in X , then X has a maximal element.*

Theorem 17. *Every unital ring $R \neq \{0_R\}$ has a maximal ideal.*

Proof. Let P to be the set of proper ideals. Then P, \subseteq is a poset by lifting the partial order from sets. Thus, by Zorn's lemma, it suffices to show that every chain in P has an upper bound in P . Let C be a chain in P , then by checking, we find $\bigcup C$ is a element of P so an upper bound of C in P . \square

Definition 17.1 (Prime). *Let $x \in R$, where R is a ring. We say x is prime if and only if $\langle x \rangle$ is a prime ideal in R .*

In a commutative unital ring R , we have $\langle x \rangle = \{xr \mid r \in R\}$ for elements of $x \in R$. We sometimes write xR for this ideal. It should be noted that the unital condition is significant as while $2\mathbb{Z}$ is commutative, $\langle 2 \in 2\mathbb{Z} \rangle \neq \{2r \mid r \in 2\mathbb{Z}\}$ as the latter does not contain 2.

Commutative unital rings have a notion of divisibility. Given $a, b \in R$, we say $a \mid b$ if one of the following equivalent properties hold,

- $b \in \langle a \rangle$;
- $\langle b \rangle \subseteq \langle a \rangle$;
- $\exists x \in R, b = xa$.

Definition 17.2 (Irreducible). *We say $x \in R^*$ is irreducible if $\langle x \rangle$ is maximal among the set of proper principle ideals.*

We immediately see that 1_R is not irreducible as it generates the entire ring so $\langle 1_R \rangle$ is not proper.

Theorem 18. *$a \in R$ is irreducible if and only if whenever $x \mid a$, $\langle x \rangle = \langle a \rangle \vee \langle x \rangle = R$.*

Theorem 19. *$a \in R$ is not irreducible if and only if there exists $x, y \in R^*$ $x, y \neq 1_R$ such that $a = xy$.*

Lemma 3. *Let R be an integral domain, then*

- $\langle a \rangle = \langle b \rangle$ if and only if there is some $x \in U(R)$ such that $a = xb$;
- $a \in R^*$ is irreducible if and only if $a = xy$ implies $\langle x \rangle = R$ or $\langle y \rangle = R$;
- $a \in R^*$ is irreducible if and only if $a = xy$ implies $\langle x \rangle = \langle a \rangle$ or $\langle y \rangle = \langle a \rangle$;
- if $a \in R^*$ is prime, then it is irreducible.

Proof. The first part is by following your nose while the rest follows directly from it. \square

One common question that is often asked is to show some number to be irreducible in $\mathbb{Z}[\theta]$ for some algebraic number θ . This type of questions can be approached using a single method.

Suppose we would like to show that $2, 3, 1 + \sqrt{-5}$ are irreducible in $\mathbb{Z}[\sqrt{-5}]$. We will first define the function $\phi : \mathbb{Z}[\sqrt{-5}] \rightarrow \mathbb{Z} : a + b\sqrt{-5} \mapsto a^2 + 5b^2$. By checking, we find ϕ preserves product and thus, divisibility. Furthermore, we see that $\alpha \in \mathbb{Z}[\sqrt{-5}]$ is a unit if and only if $\phi(\alpha) = 1$. Now, suppose for a contradiction $1 + \sqrt{-5}$ is reducible. Then by theorem 19, there is some $a, b \in \mathbb{Z}[\sqrt{-5}]$ such that $1 + \sqrt{-5} = ab$, so Wlog. $\phi(a) = 2$ and $\phi(b) = 3$ which is not possible $\#$. The similar is true for showing 2 and 3 being irreducible.

Lemma 4. *Let R be a ring, then R is an integral domain if and only if $\langle 0_R \rangle$ is prime in R .*

Theorem 20. *Let R be a non-trivial commutative unital ring such that every proper ideal is prime, then R is a field.*

Proof. Let $r \in R^*$, then Wlog. $\langle r \rangle \neq R$ so $\langle r \rangle$ is prime. Now, consider the ideal generated by r^2 . Trivially, by primeness, $r \in \langle r^2 \rangle$ so there exists $a \in R$, $r = ar^2 \implies 0_R = ar^2 - r = r(ar - 1)$. Now, as $\langle 0_R \rangle$ is prime, R is an integral domain, so $ar = 1$. \square

1.7 Principle Ideal Domain

Definition 20.1 (Principle Ideal Domain). *We call an integral domain R to be a principle ideal domain if and only if for all $I \triangleleft R$, I is principle. We sometimes write R is a PID.*

As every ideals of \mathbb{Z} is of the form $\langle k \rangle$ for some $k \in \mathbb{Z}$, \mathbb{Z} is a PID.

Theorem 21. *Let R be a PID and $x \in R^*$. Then x is irreducible if and only if $R/\langle x \rangle$ is a field. Furthermore, any non-zero prime ideal is maximal.*

Proof. Follows directly from the fact that R/I is a field if and only if I is maximal for any $I \triangleleft R$. \square

A powerful result of the above theorem is that we have just classified the finite fields \mathbb{F}_p . $\mathbb{F}_p = \mathbb{Z}/\langle p \rangle$ is a field if and only if p is prime (in the ideal sense as well as in the integer sense).

Theorem 22. *Let \mathbb{F} be a field. Then $\mathbb{F}[X]$ is a principle ideal domain.*

Proof. Let $I \triangleleft \mathbb{F}[X]$ and Wlog. suppose I is proper and non-trivial. Thus, by the well-ordering principle, there is some $p \in I$ with minimal degree d_p . For contradiction, suppose $I \neq \langle p \rangle$, then there is some $q \in I \setminus \langle p \rangle$ with minimal degree d_q . By construction, we have $d_p \leq d_q$ so $r(X) := q(X) - c_p(X)X^{d_q-d_p} \in I$, where $c = c_q c_p^{-1}$ and c_f is the coefficient of f of the term $X^{\deg f}$. We see that, by construction, $\deg r < \deg q$ so, by the minimum degree assumption of q , $r \in \langle p \rangle$ implying $q \in \langle p \rangle$. $\#$ \square

While the proof above is neat, it turns out that polynomial over fields forms what it's called a *Euclidean Domain* which are principle ideal domains. We will come back to this definition later.

The reverse of the above theorem is also true.

Theorem 23. *If $R[X]$ is a PID, then R is a field.*

Proof. As $\langle X \rangle$ is irreducible in $R[X]$, we find that $R[X]/\langle X \rangle$ is a field by theorem 21. Now, as $R[X]/\langle X \rangle \cong R$ by considering the first isomorphism theorem and the ring homomorphism that maps each polynomial to its constant coefficient, we find that R is a field. \square

Theorem 24. *Let S denote the set of maximal ideals of some ring R , then*

$$\bigcup S = R \setminus U(R).$$

1.8 Fields and Adjunction of Elements

We say a field \mathbb{F} is a *subfield* of a field \mathbb{K} or that \mathbb{K} is a *field extension* of \mathbb{F} if and only if \mathbb{F} is a unital subring of \mathbb{K} . If so, then \mathbb{K} forms a \mathbb{F} -vector space and we call its dimension the *degree* of the field extension, this is denoted by $[\mathbb{K} : \mathbb{F}]$.

We will come back to this later.

1.9 More on Polynomial Rings.

Suppose $\phi : R \rightarrow S$ is a unital ring homomorphism between two integral domains, then the mapping

$$\hat{\phi} : R[X] \rightarrow S[X] : \sum_{i=0}^n r_i X^i \mapsto \sum_{i=0}^n \phi(r_i) X^i$$

is also a unital ring homomorphism. This can be used to examine irreducibility in $S[X]$ and $R[X]$ through each other.

Definition 24.1 (Primitive). *We call $f \in \mathbb{Z}[X]$ primitive if and only if there is no prime p dividing all of the coefficients of f .*

Theorem 25. *A non-constant polynomial $f \in \mathbb{Z}[X]$ is irreducible in $\mathbb{Z}[X]$ if and only if it is primitive and irreducible in $\mathbb{Q}[X]$.*