Notes on Ring Theory

by Avinash Sathaye, Professor of Mathematics
October 27, 2013

Contents

1 Ring axioms and definitions. 2

2 Examples of rings. 6

3 Ideal operations. 10

4 Extending rings. 12

4.1 Adjoining one element to a ring. 12

4.1.1 Adjoining an integral element. 12

4.1.2 Adjoining a general algebraic element. 15

4.2 Inverting a set. 15

5 Important domains. 18

5.1 Euclidean Domains. 18

5.1.1 Properties of euclidean domains. 19

6 Principal Ideal Domains. P.I.D. 23

7 Unique Factorization Domains. U.F.D. 25

8 Fields and Galois Theory. 29

8.1 Splitting field. 32

8.2 Outline of results. 33

8.3 Problems of Galois Theory. 37

1 Ring axioms and definitions.

Definition: Ring We define a ring to be a non empty set R together with **two binary operations** $f, g : R \times R \Rightarrow R$ such that:

1. R is **an abelian group** under the operation f.

2. The operation g is associative, i.e. $g(g(x, y), z) = g(x, g(y, z))$ for all $x, y, z \in R$.

3. The operation g is distributive over f. This means:

   $$g(f(x, y), z) = f(g(x, z), g(y, z))$$

   and

   $$g(x, f(y, z)) = f(g(x, y), g(x, z))$$

   for all $x, y, z \in R$.

Further we define the following natural concepts.

1. **Definition: Commutative ring.** If the operation g is also commutative, then we say that R is a commutative ring.

2. **Definition: Ring with identity.** If the operation g has a two sided identity then we call it the identity of the ring. If it exists, the ring is said to have an identity.

3. **The zero ring.** A trivial example of a ring consists of a single element x with both operations trivial. Such a ring leads to pathologies in many of the concepts discussed below and it is prudent to assume that our ring is not such a singleton ring. It is called the "zero ring", since the unique element is denoted by 0 as per convention below.

   Warning: We shall always assume that our ring under discussion is not a zero ring. However, when we construct a new ring from a given ring, we need to make sure that we have not created the zero ring.

4. **Conventions.** To simplify notation, we write $x + y$ in place of $f(x, y)$. The corresponding identity element is naturally denoted by 0. The operation is simply called the addition operation in the ring.

   We shall also replace $g(x, y)$ by $x \cdot y$ or simply xy, if there is no confusion. We naturally call the resulting operation the multiplication in R.

   The corresponding identity of multiplication, if it exists, is naturally denoted by 1.[1]

[1] Some textbooks make a term "rng" to denote a ring possibly without the unity, whereas the term "ring" is reserved for rings with unity. The idea is that the "i" in the spelling stands for the unity! While cute, this is useless since it is hard to say "rng"!

5. Note that there is a good reason not to make a fuss about the additive identity 0, since it always exists. One sometimes distinguishes the element 1 by calling it the multiplicative identity.

6. It can be shown that for rings with identity, the distributive law forces the operation f to be commutative and hence our assumption of "abelianness" is a natural one. [2]

7. **Definition: Zero divisor** An element $x \in R$ is said to be a zero divisor if $x \neq 0$ and there is some nonzero $y \in R$ such that $xy = 0$ or $yx = 0$. Sometimes people name these two possible cases ($xy = 0$ or $yx = 0$) as conditions for a left or right zero divisors. We shall not emphasize this.

   It is important to **note** that a zero divisor is never zero! [3]

8. A related concept for the identity 1 is:

   Definition: Unit in a ring. An element $x \in R$ is said to be a unit if $xy = yx = 1$ for some $y \in R$.

   The set of units of a ring R is denoted by $R^{\times}$.

   Note that in contrast with the zero divisor concept, the element 1 is counted as a unit.

   It is easily seen the the set $R^{\times}$ is a group under multiplication.

9. **Definition: divisibility in a ring.** We say that an element x of a ring divides y if $y = xz$ for some z in the ring. In symbols we write $x|y$ and we may also say y is divisible by x or that x is a factor of y.

   Thus units clearly divide every element of the ring. In a commutative ring, it is easy to show that every factor of a unit is a unit.

10. Note that the set of units and the set of zero divisors are disjoint.

    To see this, let x be a unit with $xy = yx = 1$. If $xz = 0$ then $yxz = y0 = 0$ but at the same time, $yxz = (1)z = z$. Thus $xz = 0$ implies $z = 0$ and this proves that x is not a zero divisor. The case when $zx = 0$ is similar.

[2] To see this, simply expand $(1 + 1)(x + y)$ in two different ways to get:

$$x + y + x + y = x + x + y + y$$

and deduce $y + x = x + y$ by canceling x from left and y from right.

[3] It is tempting to define a zero divisor as any divisor (or factor) of zero. But then 0 will always be such a zero-divisor and we will need a term "proper zero divisor" to discuss the interesting non zero factors of zero. We have chosen the current definition to avoid adding the word proper every time!

On the other hand, assume that z is a zero divisor, so that $z \neq 0$ and $zw = 0$ for some non zero w. We prove that z is not a unit. If $xz = 1$ for some x, then $xzw = (1)w = w \neq 0$, but $xzw = x(0) = 0$, a contradiction. The case when $wz = 0$ is similar.

11. One of the most useful type of a ring is defined next.

    Definition: Integral domain.

    A ring R is said to be an integral domain if it is **commutative**, **contains $\mathbf{1 \neq 0}$** and has **no zero divisors.** In an integral domain, we have cancellation for multiplication, namely $xy = xz$ implies $x = 0$ of $y = z$. To see this, simply rewrite the equation as $x(y - z) = 0$ and use the condition on zero divisors.

    Definition: Field.

    An integral domain R is said to be a field if its non zero elements are units, i.e. $R^{\times} = R \setminus 0$. Later on we will see how any integral domain can be enlarged to a field called its quotient field.

    Many examples of fields are well known, $\mathbb{Q}$ the field of rational numbers, $\Re$ the field of real numbers, $\mathbb{C}$ the field of complex numbers and $\mathbb{Z}_p$ the finite field with p elements when p is a prime.

    The field $\mathbb{Q}$ is the so-called quotient field of $\mathbb{Z}$.

    Definition: Division ring.

    A ring R is said to be a "division ring" if the condition $R^{\times} = R \setminus 0$ holds. Thus, we can define a field as a commutative division ring.

    One of the best examples of a division ring is the ring of real Hamilton Quaternions:

    $$\mathbb{H} = \{a + bi + cj + dk | a, b, c, d \in \Re\}$$

    where the products are defined by

    $$i^2 = j^2 = k^2 = -1 \text{ and } ij = k = -ji, jk = i = -kj, ki = j = -ik.$$

    Verify that

    $$(a + bi + cj + dk)(a - bi - cj - dk) = a^2 + b^2 + c^2 + d^2$$

    and deduce that we indeed have a division ring!

12. **Definition: Sub-ring.** If R is a ring and $S \subset R$, then S is said to be a sub-ring of R if S is a ring under the operations induced from R. It

will follow that the 0 from R belongs to S, but the identity 1 may or may not belong to S.

Clearly, a sub-ring S forms an additive subgroup of R and has to be closed under multiplication.

Thus the set $3\mathbb{Z} = \{3n|n \in \mathbb{Z}\}$ is a sub-ring of $\mathbb{Z}$ which does not contain the identity. In fact, if a sub-ring of $\mathbb{Z}$ contains 1, then it is obvious that it coincides with $\mathbb{Z}$.

13. For groups, we could use certain subgroups to create quotient groups, namely the normal subgroups. For rings, we can make quotient rings if our sub-rings are "ideal".!

    Definition: Ideal. A subset I of a ring R is said to be a left ideal if

    - I is an additive subgroup of R and
    - for every $a \in I$ and $x \in R$ we have $xa \in I$. This can be shortened as $RI \subset I$.

    A right ideal is defined similarly, where we require $IR \subset I$.

    The subset I is said to be an ideal if it is both a left and a right ideal (or the so-called two-sided ideal). Clearly, for commutative rings, we only need to use the left ideal conditions above.

14. Let R be a ring and I an ideal in R. We define the quotient ring R/I as follows.

    Definition: Quotient ring.

    Consider the set of additive cosets

    $$S = \{x + I|x \in R\}.$$

    Since I is clearly a normal subgroup of the additive group R, we already know that S is a well defined (abelian) quotient group. We define the multiplicative structure on S by:

    $$(x + I)(y + I) = xy + I.$$

    It is easy to check that this is well defined and defines a ring. [4]

[4] The hardest part is to check that this is well defined. Thus, let $x + I = p + I$ and $y + I = q + I$, i.e. $x = p + p_1$ and $y = q + q_1$ where $p_1, q_1 \in I$. Then

$$xy = pq + pq_1 + qp_1 + p_1q_1$$

where we note that the last three terms are in I by definition of an ideal. Hence $xy + I = pq + I$. Note how both left and right conditions on an ideal are used.

The rest of the check is easy.

It is customary to denote this quotient ring as simply R/I without introducing a new symbol S.

15. As in groups, we define a homomorphism or a map which respects the ring structures. All definitions are similar except the the multiplicative structure is also invoked.

    Let $\phi : R \to S$ be a map of rings. We say that ϕ is a (ring-)homomorphism if for all $x, y \in R$:

    - $\phi(x \pm y) = \phi(x) \pm \phi(y)$ and
    - $\phi(xy) = \phi(x)\phi(y)$.

    The image of the homomorphism is the total image $\phi(R) = \{\phi(x) | x \in R\}$ and it is easily seen to be a sub-ring of S.

    The kernel of the homomorphism is the set of all elements mapping to 0, i.e.

    $$Ker(\phi) = \{x \in R | \phi(x) = 0\}.$$

    It is easy to check that $Ker(\phi)$ is a (two-sided) ideal of R.

    Following the terminology in groups, we see that the homomorphism ϕ is injective if and only if $Ker(\phi) = \{0\}$ and it is surjective if an only if $S = \phi(R)$. As before, an isomorphism is a homomorphism which is injective and surjective.

    If we set $I = Ker(\phi)$, then the map $\psi : R/I \to \phi(R)$ defined by $\psi(x + I) = \phi(x)$ is easily seen to be an isomorphism.

    Thus, we have the basic identity

    $$\phi(R) \cong R/Ker(\phi).$$

2 Examples of rings.

We now list several important examples of rings which will be studied in greater details later.

1. **Rings derived from integers.** A lot of insight in the rings comes from the basic ring of integers $\mathbb{Z}$. It is indeed an integral domain with many special properties.

   The finite rings $\mathbb{Z}_n$ derived from $\mathbb{Z}$ give basic examples of finite commutative rings. In fact, in $\mathbb{Z}_n$ the identity 1 is written as $[1]_n$ in our convention and has the property that $r \cdot [1]_n$ or the sum of r terms $[1]_n + [1]_n + \cdots$ is $0 = [0]_n$ exactly when r is a multiple of n.

We make a:

Definition: Characteristic of a ring. A ring R with 1 has characteristic n if n is the first positive integer for which $1+1+\cdots$ n terms $=0$. In case, such an n does not exist, the characteristic is said to be 0.

A simpler description of the characteristic is as follows. Define a homomorphism $\phi : \mathbb{Z} \to R$ by $\phi(1) = 1_R$ where we have made up the notation 1_R for the identity in R. The $Ker(\phi)$ is then an ideal in $\mathbb{Z}$ and it is easy to show that any ideal in $\mathbb{Z}$ is simply of the form $d\mathbb{Z}$ where d is some non negative integer. Indeed, d is simply the GCD of all members of the ideal!

The characteristic of the ring R is n if $Ker(\phi) = n\mathbb{Z}$. It is also clear that the sub-ring $\phi(\mathbb{Z})$ of R is isomorphic to $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$.

2. **Polynomial rings and related costructions.** We shall give a rather general way of constructing rings from base rings which includes the construction of polynomial and power series rings.

   Let G be an abelian group. We say that G is an ordered abelian group if G is a disjoint union of sets denoted as $G_+, G_-, 0$ such that:

   (a) An element $x \in G$ is in G_+ if and only if $-x \in G_-$. In particular, G has no elements x with $x + x = 0$, except 0.

   (b) If $x, y \in G_+$, then $x + y \in G_+$ and similarly, if $x, y \in G_-$ then $x + y \in G_-$. In fact, the condition on G_- can be deduced from the condition on G_+.

   (c) This defines an order on G, namely we define $x < y$ if an only if $y - x \in G_+$.

   An abstract construction.

   Let R be a commutative ring with 1 and consider the set of all functions from G to R denoted by R^G. For any function $f \in R^G$ we shall denote its support by $Supp(f) = \{x \in G | f(x) \neq 0\}$.

   Define $WO(R, G)$ to be the set of all functions in R^G whose support is well ordered (under the given order on G).

   We make $WO(R, G)$ into a ring by defining component-wise addition and multiplication by the Cauchy product defined thus:

   If $f, g \in WO(R, G)$, then the product $fg \in WO(R, G)$ is defined by

$$fg(x) = \sum_{y \in Supp(f), z \in Supp(g), x = y+z} f(y)f(z).$$

Some serious work is involved in proving that the sum has only finitely many terms and the resulting product also has well ordered support.

We shall leave further details of these concepts for private contemplation for now. We only illustrate a few special cases which are fundamental to the ring theory.

- **Polynomial ring.**
  If we take the ordered abelian group as $\mathbb{Z}$ and let S be the set of non negative integers, then we can define the polynomial ring (in one variable over R) as
  $$\{f \in R^{\mathbb{Z}} | Supp(f) \text{ is a finite subset of } S\}.$$
  If we consider a function $h \in R^{\mathbb{Z}}$ defined by $h(1) = 1$ and $h(n) = 0$ if $n \neq 1$ and for convenience denote it by X, then it is easy to see that our ring contains all powers $X, X^2, X^3, \cdots$ and we simply get the set
  $$\{\sum_{i=0}^{m} a_i X^i | \text{ where some } m \in S \text{ and } a_i \in R\}.$$
  This is usually denoted as $R[X]$ where X is identified with the special function. It is called the polynomial ring in one variable over R (or with coefficients in R).
  Having defined a polynomial ring in one variable, we may use it as a base ring and create a polynomial ring in two variables as $R[X][Y]$ which is briefly written as $R[X, Y]$. In general, we can define and use a polynomial ring in several variables $R[X_1, \cdots, X_n]$ or even in infinitely many variables if convenient. [5]
- **Power series.**
  If we use the same setup as above, but drop the condition that the supports of functions is finite, then we get the ring of formal power series with elements of the form
  $$\sum_{i=0}^{\infty} a_i X^i.$$
  The resulting ring is denoted by $R[[X]]$. As before, we can add several variables at a time to make $R[[X_1, \cdots, X_n]]$ or even infinitely many variables.

[5] If we allow infinitely many variables, then we have a choice to allow only finitely many variables at a time in a given element, or allow infinitely many variables to appear in a single element. We get different rings and both can be useful!

- **Generalized polynomial or power series rings.** We may allow the support to be a finite subset of $\mathbb{Z}$ and get a ring denoted as $R[X, X^{-1}]$ where we allow finitely many positive or negative exponents for X. This is called the ring of Laurent polynomials over R.

  A similar construction for power series requires assuming that the support is well ordered and the ring is then denoted as $R((X))$. [6]

3. **Group rings.**

   If G is a finite group (not necessarily abelian) then we can repeat the above abstract construction to make R^G into a ring. This time, we don't worry about the order, since the order is only needed to make sure that the product has only finitely many terms to collect at a time. Since our whole set G is finite, this is not a problem at all.

   The function $f \in R^G$ may be conveniently written as

   $$\sum f(g) \cdot g$$

   where the symbols "g" are simply place holders. This is called the group ring of G over R and is simply denoted as RG.

4. **Matrix rings.** Let n be a natural number and let $M_n(R)$ be the set of $n \times n$ matrices with entries in R. The usual addition and multiplication of matrices makes it into a ring and a rich source of examples of non commutative rings. Note that we need to fix a positive integer n to work with such rings. Sometimes, one defines a ring of infinite matrices whose elements have the shape:

   $$\begin{pmatrix} A & 0 \\ 0 & I \end{pmatrix}$$

   where A is an $n \times n$ matrix for some finite n and I stands for an infinite diagonal matrix with 1's down its diagonal. Here the two 0's are supposed to represent zero matrices of appropriate sizes to fill up an infinite square matrix.

   This ring may be denoted with $M(R)$. If we are working with finitely many matrices of this ring, we can find an n such that all of them can be thought to have a shape with an $n \times n$ part in the top left corner, extended with I and 0's. Then their matrix operations can be essentially worked out in $M_n(R)$ and filled out with I and 0's.

[6] Why do we not write $R[X, X^{-1}]$ as $R(X)$? The reason is that this particular symbol is used for the so-called quotient field (or the total quotient ring) to be defined later.

3 Ideal operations.

Ideals are to be thought of as a natural generalization of integers. In $\mathbb{Z}$ the ring of integers, we know how to work with individual integers, how to factor and divide and otherwise combine them. In arbitrary rings, elements may not have unique or finite factorization and to restore some of the properties of integers, one defined what should ideally behave like numbers, hence the word "ideal".

Given an element r in a ring R, let $a, b \in R$ and note that any (two-sided) ideal containing r must also contain arb. If $1 \in R$, then a, b are allowed to be any integers (or really their images in the ring). If $1 \notin R$ then we can still make perfect sense out of nr as $r + \cdots + r$ - a sum of n terms if $n > 0$ and $-r - \cdots - r$ - a sum of $-n$ terms if $n < 0$. For convenience, we interpret an as na. Thus we shall consider integers multiples of elements of R even though integers themselves may not be in R.

Given a ring R and any subset S, it is easy to see that the set:

$$\{a_1 s_1 b_1 + \cdots + a_m s_m b_m | a_i, b_i \in R \ , \ s_i \in S \text{ and } m \in \mathbb{Z}_+\}$$

is easily seen to be a two-sided ideal in R. It is called the ideal generated by S and is denoted as (S). [7]

Remark.

If the set S is finite, say $S = \{s_1, \cdots, s_m\}$, then it is tempting to write

$$(S) = \{\sum_1^m a_i s_i | a_i \in R\}$$

but this is **wrong** if R does not contain 1. We need to modify it to:

$$(S) = \{\sum_1^m (a_i + d_i) s_i | a_i \in R, d_i \in \mathbb{Z}\}$$

where $d_i s_i$ is defined thus:

- If $d_i > 0$ then $d_i s_i = s_i + s_i + \cdots$ a sum of d_i terms.
- If $d_i < 0$ then $d_i s_i = -(-d_i s_i)$, calculated using the above definition for $-d_i$.
- If $d_i = 0$ then $d_i s_i = 0$.

[7] This is at variance with the "subgroup generated by" notation $< S >$, but is common for ideals. Also, if S is a finite set, then we drop the set notation; for example, we write (s, t) for $(\{s, t\})$.

If the ring is $\mathbb{Z}$ and S is any subset of $\mathbb{Z}$, then we know that $(S) = (d)$ where d is the GCD of all the elements of S. This is the main consequence of the Euclidean algorithm in $\mathbb{Z}$ which says that the GCD of any two integers is a linear combination of the two with integer coefficients. Thus, every ideal in integers is generated by one element, or principle. In general, we shall study rings in which every ideal is finitely generated and these are called Noetherian rings.

We now define a set of operations on ideals and illustrate each by their counterpart in integers. We shall **assume that the ring is commutative,** but the definitions can be suitably interpreted in non commutative rings also, provided extra care is taken and suitable conditions imposed.

1. Given two ideals I, J in R, their sum $I + J$ is defined as the ideal generated by $\{a + b|a \in I, b \in J\}$. It is easy to show that if $I = (S)$ and $J = (T)$, then $I + J = (S \bigcup T)$.

   Since ideals in $\mathbb{Z}$ are principle, we can say that $I = (n), J = (m)$ for some $n, m \geq 0$ and then it is known that $I + J = (n, m) = (d)$, where $d = \text{GCD}(n, m)$.

   More generally, the idea of sum can be extended to even infinite collection of ideals, where we consider elements which belong to the sum of finitely many ideals at a time.

2. Given two ideals I, J in R, their intersection is defined as the usual set theoretic intersection and is easily seen to be an ideal. As before, this extends to an infinite set as well.

   In $\mathbb{Z}$ the ideal $(n) \bigcap (m)$ simply evaluates to $(\text{LCM}(n, m))$. Here an infinite intersection will reduce to the zero ideal unless it is essentially a finite intersection.

3. Given two ideals I, J in R, their product is defined as the ideal generated by $\{rs|r \in I, s \in J\}$. It is denoted as IJ and is really equal to (IJ) in our usual convention for products of sets.

   In $\mathbb{Z}$ we get that $(n)(m) = (nm)$.

4. Given ideals I, J in R we define their quotient $I : J$ to be the set $\{r \in R|rJ \subset I\}$.

   In $\mathbb{Z}$, this gives $(n) : (m) = (n/d)$ where $d = \text{GCD}(n, m)$. Thus, for example, $(6) : (4) = (3)$. For proof, note that $3(4) \subset (12) \subset (6)$ and if $4x$ is divisible by 6, then clearly 3 must divide x.

5. Given an ideal I in R, by its radical, we mean the ideal

$$\{x|x^n \in I \text{ for some positive integer } n\}.$$

The notation for this radical ideal is $\sqrt{I}$.

In $\mathbb{Z}$, the $(\sqrt{n})$ is the ideal (m) where m is obtained from the product of all distinct prime factors of n. Thus $(\sqrt{108}) = (2 \cdot 3) = (6)$.

Remark.

Avoid the confusion with the usual meaning of square root. In ideals the symbol covers all n-th roots!

4 Extending rings.

We now discuss some useful ways of creating new rings out of old ones.

Convention.

For convenience, we shall assume that we have a commutative ring R with 1. The reader may try to generalize the constructions by dropping these conditions.

4.1 Adjoining one element to a ring.

Let R be a ring (with the convention in force, of course) and let $S = R[X]$ a polynomial ring over R. Note that R can be identified as the sub-ring of $R[X]$ consisting of polynomials of degree 0.

We shall do this identification without comment in the future.

4.1.1 Adjoining an integral element.

Definition: Integral element.

An element $x \in A$ is said to be **algebraic** over a sub-ring B if it is the root of some non zero polynomial with coefficients in B. This means:

$$b_0 x^n + b_1 x^{n-1} + \cdots b_n = 0$$

for some $b_0, b_1, \cdots, b_n \in B$ with $b_0 \neq 0$ and $n \geq 1$. The element X is then a root of the polynomial $f(X) = b_0 X^n + b_1 X^{n-1} + \cdots + b_n \in B[X]$.

An element $x \in A$ is said to be **transcendental** over a sub-ring B if it is not algebraic. In this case, it is easy to see that the set

$$B[x] = \{p_0 x^m + \cdots + p_m | p_i \in B, m \text{ is a non negative integer }\}$$

is actually a ring isomorphic to the polynomial ring $B[X]$ under the isomorphism mapping X to x.

A ring A is said to be algebraic over a sub-ring B if every element of A is algebraic over B.

An element $x \in A$ is said to be integral over a sub-ring B if it is a root of a monic polynomial with coefficients in B, i.e.

$$x^n + b_1 x^{n-1} + \cdots + b_n = 0$$

for some $b_1, \cdots, b_n$ in B.

A ring A is said to be integral over B if every element of A is integral over B.

Example. Recall the Newton's Rational Root Theorem: If a rational number r is a root of a polynomial $f(X) = a_0 X^n + \cdots a_n$ of degree n with integer coefficients and if $r = \frac{p}{q}$ in reduced form, then p divides a_n and q divides a_0.

This theorem applied to the case when $f(X)$ is monic (or $a_0 = 1$) gives that r must be an integer factor of a_n.

In particular, it says that a rational root of a monic polynomial is an integer! In other words, a rational number integral over the ring of integers is actually an integer. This explains the term "integral".

A similar argument can be used for $k[X]$, a polynomial ring over a field k. This gives a theorem which says that a rational function (ratio of two polynomials in $k[X]$) is integral over $k[X]$ iff it is in $k[X]$.

Let

$$f(X) = X^n + a_1 X^{n-1} + \cdots + a_n$$

be a monic polynomial of degree n in S so that $a_i \in R$.

Let $I = (f(X))$ the ideal generated by $f(X)$ in S and let $T = S/I$ and let $\phi : S \to T$ be the canonical residue class map $\phi(z) = z + I$.

We claim that

1. ϕ restricted to R is an isomorphism onto $\phi(R)$.

2. $w = \phi(X)$ satisfies $w^n + \phi(a_1) w^{n-1} + \cdots + \phi(a_n) = 0$.

3. **Now we identify** R with $\phi(R)$, so for $r \in R$, we replace $\phi(r)$ by r.

   Then we can simply say that T is a ring containing R and

   $$f(w) = w^n + a_1 w^{n-1} + \cdots + a_n = 0.$$

   In other words, T is an extension of R containing a root w of $f(X)$.

4. The ring T can be described thus:

   $$T = \{r_0 w^{n-1} + r_1 w^{n-2} + \cdots + r_{n-2} w + r_{n-1} | r_i \in R\}.$$

   In other words T consists of expressions $g(w)$ as $g(X)$ varies over all polynomials in X of degree at most $n - 1$ over R. To compute the product $g_1(w) g_2(w)$ we write

   $$g_1(X) g_2(X) = q(X) f(X) + r(X)$$

where $r(X)$ is the remainder of $g_1(X)g_2(X)$ mod $f(X)$ and noting that $f(w) = 0$ we get $g_1(w)g_2(w) = r(w)$.

5. The ring T can be thought of as a ring obtained by adjoining a root of $f(X)$ to R.

PROOF. The first claim is easily checked. As for the second claim, note that $w^n + \phi(a_1)w^{n-1} + \cdots + \phi(a_n) = \phi(f(X))$ and this is zero since $f(X) \in I = Ker(\phi)$.

Given any element $g(X) \in R[X]$ we write $g(X) = q(X)f(X) + r(X)$ by the usual division algorithm and since $\phi(f(X)) = 0$ we see that

$$\phi(g(X)) = g(w) = \phi(r(X)) = r(w).$$

The rest of the claims are now easy to verify.

Example. Let $R = \mathbb{Z}$ and $f(X) = X^2 - D$ for some integer D. The ring $T = \mathbb{Z}[X]/(X^2 - D)$ can then be written as:

$$T = \{aw + b | a, b \in \mathbb{Z}\}$$

where $w = \phi(X)$ satisfies $w^2 - D = 0$, i.e. $w = \sqrt(D)$. Thus T can be thought of as $\mathbb{Z}[w]$ an extension of $\mathbb{Z}$ obtained by adjoining w, a square root of D. It follows that $-w$ is also a square root of D.

Several particular cases are noteworthy.

- If $D = 2$, then we get the ring $\mathbb{Z}[\sqrt{2}]$, the ring obtained by adjoining the square root of 2.

- If we take $D = -1$ so that $f(X) = X^2 + 1$, then we get the usual imaginary square root of -1. Indeed, if we take $R = \Re$ the field of reals and make $\Re[X]/(X^2 + 1)$ then we get the field of complex numbers $\mathbb{C}$.

- **Food for thought.** Notice that we have put no restriction on D. If we take $D = 1$, then we already have two square roots $1, -1$ of D in $\mathbb{Z}$. Our construction produces two more, namely $w, -w$. How can we have four square roots? The problem is that our ring T has zero divisors. Thus we have
$$0 = w^2 - 1 = (w - 1)(w + 1)$$
yet neither $w - 1$ nor $w + 1$ are zero! Thus we need to be careful and restrain our intuition when using this algebraic device!

  We run into such problems only when we allow our $f(X)$ to be reducible.

- Consider $D = 5$. Let $g(X) = X^2 + X - 1$ and let $S = \mathbb{Z}[\omega]$ the ring obtained by adjoining a root ω of $g(X)$.

  Use $\omega^2 + \omega = 1$ and we can see that for $w = 2\omega + 1$ we have

  $$w^2 = (2\omega + 1)^2 = 4\omega^2 + 4\omega + 1 = 4(\omega^2 + \omega) + 1 = 5.$$

  Thus our ring $\mathbb{Z}[\sqrt{5}]$ can be identified with the sub-ring $\mathbb{Z}[2\omega + 1]$ of S.

  It can be shown that whenever $D = 1+4n$ we can use $g(X) = X^2+X-n$ and get

  $$\mathbb{Z}[\sqrt{D}] = \mathbb{Z}[2\omega + 1] \subset \mathbb{Z}[\omega]$$

  where $g(\omega) = 0$.

  The book defines $\mathcal{O}(D)$ to be $\mathbb{Z}[\sqrt{D}]$ if D is a square-free integer congruent to 2 or 3 mod 4 and $\mathcal{O}(D) = \mathbb{Z}[\omega]$ if D is congruent to 1 mod 4.

  This will be discussed in more details later.

4.1.2 Adjoining a general algebraic element.

If we work as above but now allow

$$f(X) = a_0X^n + a_1X^{n-1} + \cdots + a_n$$

where $a_i \in R$ and $a_0 \neq 0$ so $f(X)$ has degree n.

The ring $T = R[X]/(f(X))$ is defined as above, but because of the leading coefficient a_0 not being a unit, we may not be able to carry out the usual division algorithm completely.

Letting ϕ denote the usual canonical homomorphism and $w = \phi(X)$ we still get that w is a root of $f(X)$ after we identify R with $\phi(R)$.

The elements of T can be still expressed as polynomials in w, but we can no longer restrict their degree to less than n.

Example. Let $R = \mathbb{Z}$ and $f(X) = 2X - 1$. Then T is identified with $\mathbb{Z}[\frac{1}{2}]$ since $\frac{1}{2}$ is a unique root of $f(X)$.

With $R = \mathbb{Z}$ we can also consider $f(X) = 4X^2 - 5$ and note that our ring T may be thought of as $\mathbb{Z}[\frac{\sqrt{5}}{2}]$. Note that T contains a subring $\mathbb{Z}[\sqrt{5}]$ already known to us and this subring is integral over $\mathbb{Z}$ but the whole ring T is not.

4.2 Inverting a set.

As we saw above, the result of adjoining a root of $2X - 1$ was to allow the fraction $\frac{1}{2}$ into the ring $\mathbb{Z}$. We now generalize this process for a general ring R, with the continued

Convention: The ring R is assumed to be commutative with 1.

Let S be a subset of R which is multiplicatively closed, which means the product of any two elements of S is again in S.

As **a temporary convenience,** we shall also assume that S contains no zero divisors or zero. We shall drop this convention later.

We now construct a ring A containing R in which every element of S becomes a unit. In principle, we could add the inverse of each element of S but we we can do the whole set in in operation as follows.

1. Start with a set
$$RS = \{(a, s) | a \in R, s \in S\}$$
and define an equivalence relation on RS by $(a, s) \cong (b, t)$ iff there exists $s_1 \in S$ such that
$$s_1(at - bs) = 0.$$
We leave for the reader to check that this is an equivalence relation.

   Now, under our temporary convenient assumption, it follows that s_1 is not needed, since every element of S is non zero and a non zero divisor, so the condition reduces to $at - bs = 0$. We have included it so the construction will work in general.

2. Let the equivalence class of a pair (a, s) be denoted by $[a, s]$. The intention is that this class $[a, s]$ shall represent the intended fraction $\frac{a}{s}$ in our resulting ring A.

   Define
$$A = \{[a, s] | a \in R, s \in S\}.$$
Define ring operations on A by
$$[a, s] + [b, t] = [at + bs, st] \text{ and } [a, s][b, t] = [ab, st].$$
It is straightforward but tedious to check that these are well defined and make a valid ring.

   The set
$$\{[a, 1] | a \in R\}$$

is seen to form a sub-ring isomorphic to R under the correspondence $[a,1] \leftrightarrow a$.

The corresponding elements of S become $[s,1]$ and have the inverse $[1,s] \in A$, thus we have accomplished our task.

3. The ring A is suggestively denoted by $S^{-1}R$ and its elements $[a,s]$ may be denoted as $\frac{a}{s}$ for convenience in actual use.

Examples. We give several illustrations of this construction.

1. Let R be an integral domain and let $S = \{s \in R | s \neq 0\}$. Then $S^{-1}R$ is a field called the quotient field of R or the field of fractions of R.

   We may use the notation $qt(R)$ to denote it.

   Thus $qt(\mathbb{Z}) = \mathbb{Q}$.

2. Let R be still a commutative ring with 1 and take S to be the set of non zero divisors of R. Then the ring $S^{-1}R$ need not be a field but is called the "Total Quotient Ring" of R.

   We will still use the suggestive notation $qt(R)$ for it.

   Consider the ring $R = \mathbb{Q}\ [X,Y]/(XY)$ and for convenience denote by x, y the natural images of X, Y respectively in R.

   It is easy to see that elements of R can be described as $a + xp(x) + yq(y)$ where $p(x)$ and $q(y)$ are polynomial expressions in x, y over R.

   It is not hard to see that $a + xp(x) + yq(y) = 0$ iff $a = 0 = p(x) = q(y)$ and that $a + xp(x) + yq(y)$ is a non zero divisor iff $a \neq 0$. Let

   $$S = \{a + xp(x) + yq(y) \in R | a \neq 0\}$$

   and verify that S is a multiplicatively closed set of non zero divisors as required.

   The ring $S^{-1}R$ is the desired total quotient ring $qt(R)$. It is not a field but its non units are zero divisors, which cannot be units any way!

3. We shall now use the same example R above to illustrate inverting multiplicative sets which contain zero divisors. Thus,**we now drop the convenient convention of avoiding zero divisors in our multiplicative sets.**

   Thus, let

   $$M = \{a + xp(x) \in R | a \neq 0 \text{ or } p(x) \neq 0\}.$$

   The set is multiplicatively closed but does contain the zero divisor x.

Form the ring $A = M^{-1}R$ and consider the map $\psi : R \to A$ defined by $\psi(r) = [r, 1]$. Note that $[y, 1] = [xy, x] = [0, x] = [0, 1]$ from known equivalences of the classes.

Thus, the image of the whole ideal (y) is zero! It is easy to deduce that $Ker(\psi) = (y)$ and hence $\psi(R) \cong R/(y)$.

Now $R/(y)$ can be thought of as $\mathbb{Q}\ [X, Y]/(XY, Y)$ and since the ideal $(XY, Y) = (Y)$ we see that $R/(y) = \mathbb{Q}\ [X, Y]/(Y) \cong \mathbb{Q}\ [X]$.

Thus the ring A contains an isomorphic copy of the ring $\mathbb{Q}\ [X]$ and further calculations show it to be nothing but $qt(\mathbb{Q}\ [X])$. It is customary to denote this field as $\mathbb{Q}\ (X)$.

5 Important domains.

We now begin the study of some important integral domains which appear as fundamental objects for many ring theoretic investigations.

5.1 Euclidean Domains.

The motivation for these domains is the pair of very familiar rings, the ring of integers $\mathbb{Z}$ and the ring of polynomials in one variable $k[X]$.

Both of these domains have a norm and a division algorithm. We explain the meaning of this and give a definition at the same time.

Definition: Norm. Let R be a domain. A norm on R is a map $N : R \to \mathbb{Z}_{\geq 0}$ where $N(0) = 0$. The norm is said to be positive, if $a \neq 0$ implies $N(a) \neq 0$.

Definition: Euclidean Domain. A domain R is said to a "euclidean domain" with respect to a norm N, if given any two elements $a, b \in R$ with $b \neq 0$ we can write $a = qb + r$ for some $q, r \in R$ such that $r = 0$ or $N(r) < N(b)$.

Examples.

- Define a norm in $\mathbb{Z}$ by $N(x) = |x|$. This is a positive norm. Then $\mathbb{Z}$ becomes a euclidean domain since the usual division algorithm works.

- In $k[X]$, let a norm be defined by $N(f(X)) = \deg_X(f(X))$ if $f(X) \neq 0$ and for this discussion, we agree that $N(0) = 0$.

  This is not a positive norm. It can be changed to a positive norm by the simple trick of defining a different function:

$$N^*(f(X)) = 2^{\deg_X(f(X))} \text{ if } f(X) \neq 0 \text{ and } N^*(0) = 0.$$

The division algorithm is defined for the polynomials as well and yields a euclidean domain.

- Another useful example of norm comes from the ring of algebraic integers which we now discuss.

  Define $\mathcal{O}(D)$ to be $\mathbb{Z}[\sqrt{D}]$ if D is a square-free integer congruent to 2 or 3 mod 4 and $\mathcal{O}(D) = \mathbb{Z}[\omega]$ if D is congruent to 1 mod 4. Here the ω is defined to be $\frac{1+\sqrt{D}}{2}$ and satisfies the quadratic equation $X^2 - X - s = 0$ where $D = 1 + 4s$.

  Thus we have two cases:

Case 1 $\mathcal{O}(D) = \mathbb{Z}[X]/(X^2 - D)$ if D is square-free and 2 or 3 modulo 4, while

Case 2 $\mathcal{O}(D) = \mathbb{Z}[X]/(X^2 - X - s)$ when D is square-free of the form $D = 1 + 4s$.

In each case, define α to be the canonical image of X in $\mathcal{O}(D)$ and note that every element of the ring is then of the form $a + b\alpha$ where we are identifying $a, b \in \mathbb{Z}$ with their images in $\mathcal{O}(D)$.

We define the norm when D is square-free negative.

We define the norm by $N(a+b\alpha) = a^2 - b^2D$ in Case 1. Note that this is simply the product of $a + b\alpha$ with its conjugate $a - b\alpha$.

We define the norm to be $N(a+b\alpha) = a^2 + ab - sb^2$ in the second case. Note that this is also a product of the conjugates, but this time, the conjugate of $a + b\alpha$ is $a + b(1 - \alpha)$.

Note that in either case, we need to show that the map is into $\mathbb{Z}_{\geq 0}$ and this is easy to see by the negative discriminant of the quadratic expression.

5.1.1 Properties of euclidean domains.

The main properties of euclidean domains are the following. Let R be a euclidean with norm N.

1. Given any two elements $a, b \in R$ with at least one non zero, then there is a $d \in (a, b)$ such that $a, b \in (d)$. In particular $(d) = (a, b)$.

   Proof. Take $d \neq 0$ to be an element of (a, b) such that $N(d)$ is minimum among all elements of (a, b). Then the division algorithm guarantees that when any element of (a, b) is divided by d then the remainder must be zero. Thus $(a, b) \subset (d)$.

In usual terminology, we can say that d divides both a, b and any common divisor of a, b divides d. Hence $d = \mathrm{GCD}(a, b)$. Moreover, if $d^* \in R$ is any other element satisfying the same conditions, then $(d) = (d^*)$ guarantees that either is a multiple of the other by a unit. For convenience we make a:

Definition: associate elements Two elements of a ring are said to be associates of each other if one of them is a multiple of the other by a unit. Note that associate elements generate the same ideal, but in a ring with zero divisors, two elements generating the same ideal need not be associates.

Remark. Note that in $\mathbb{Z}$ it is customary to make the GCD unique by requiring it to be positive. In integers ±1 are the only units and so this is possible.

2. The above proof also generalizes to any ideal $I \subset R$, since we can still take d as the minimal norm non zero element. Thus every ideal of the ring is generate by one element or is principal.

   We thus make a:

   Definition: Principal Ideal Domain P.I.D. An integral domain is said to be a principal ideal domain (P.I.D. for short) if every ideal in it is principal.

   Note that there is no reason to require the ring to be an integral domain, so we also make a:

   Definition: Principal Ideal Ring. P.I.R. A commutative ring is said to be a principal ideal ring (P.I.R. for short) if every ideal in it is principal.

   Remark. As we note below a P.I.D. is not necessarily a euclidean domain. It is true that a P.I.D. can be shown to be equipped with something called a Dedekind-Hasse norm which we briefly discuss.

   A norm N on a domain S is said to be a Dedekind-Hasse norm if it is positive and has the following property: Given any two elements $a, b \in S$, either $a \in (b)$ or there is some element $0 \neq z \in (a, b)$ such that $0 < N(z) < N(b)$.

   Note that, $z = sa + tb$ for some $s, t \in S$ and this is almost like the division algorithm, except in the usual division algorithm, s is required to be 1.

   Remark. It is known that existence of a Dedekind-Hasse norm is equivalent to the P.I.D. property. It is easy to see why the Dedekind-Hasse norm would imply the P.I.D. property; simply imitate the euclidean proof by taking a non zero least norm element in the ideal and argue that it must generate the ideal. The converse needs properties of unique factorization domains (U.F.D.) developed later.

Remark. In spite of the norm being available, we do not necessarily get a euclidean domain in general. We discuss some special cases below.

1. **The case of D** $= -$**5.**

   We shall show that this ring has non principal ideals and hence is not euclidean.

   Here $\mathcal{O} = \mathbb{Z}[X]/(X^2 + 5)$ and we set α as the canonical image of X. Suppose $0 \neq w = a(b + c\alpha) \in \mathcal{O}$ where $a, b, c \in \mathbb{Z}$ with b, c co-prime.

   First assume that $c \neq 0$.

   Let $I = (w)$ the principal ideal. What is $I \bigcap \mathbb{Z}$, when we identify $\mathbb{Z}$ with its canonical image in $\mathbb{Z}$?

   Here is the calculation. Let $u = w(p + q\alpha) \in \mathbb{Z}$. Then we get

   $$u = a(b + c\alpha)(p + q\alpha) = a(bp - 5cq) + a(bq + cp)\alpha \in \mathbb{Z}.$$

   It follows that $bq + cp = 0$ and because of co-primeness of b, c we see that $(p, q) = \lambda(b, -c)$ for some $\lambda \in \mathbb{Z}$.

   It follows that $u = a(b^2 + 5c^2)\lambda$ and thus $I \bigcap \mathbb{Z} = (a(b + 5c^2))\mathbb{Z}$.

   If $c = 0$ then the calculation gets easier and we see that $u = abp$ so $I \bigcap \mathbb{Z} = (ab)\mathbb{Z}$.

   Thus, in either case, $I \bigcap \mathbb{Z} = (a(b + 5c^2))$.

   We now **claim** that the ideal $(3, 2 + \alpha)$ cannot be principal.

   Proof. Suppose it is generated by some w as above. Then $3 \in (a(b^2 + 5c^2))$. But $|a(b^2 + 5c^2)| \geq 5$, unless $c = 0$. Hence we must have $c = 0$ and $w = ab$, with $3 \in (ab)$. Clearly $ab = \pm 1$ is not an option, since then $I = (1)$, but $\mathcal{O}/I$ is easily seen to be a non zero ring.

   Then we may assume $w = ab = \pm 3$. But then $2 + \alpha \notin (w)$,since 3 does not divide 2, a contradiction.

   Exercise. The reader should work out the general case of intersection of a principal ideal with $\mathbb{Z}$ in the ring $\mathcal{O}$.

2. **Some examples of Euclidean rings.** We describe some $\mathcal{O}(D)$ which are euclidean.

(a) Case of $D = -1, -2$. $\mathcal{O}(D) = \mathbb{Z}[X]/(X^2 - D)$ and we shall write α for the canonical image of X as before. We shall use the norm $N(a + b\alpha) = a^2 - Db^2$.

We now show how the division algorithm works. Given $p + q\alpha \in \mathcal{O}(D)$ and $0 \neq a + b\alpha \in \mathcal{O}(D)$, we let

$$u + v\alpha = \frac{p + q\alpha}{a + b\alpha}$$

where $u, v \in \mathbb{Q}$. Find $r, s \in DZ$ such that

$$|u-r| \leq \frac{1}{2} \geq |v-s| \text{ and hence } N((u-r)+(v-s)\alpha) \leq \frac{1}{4}+\frac{1}{4}(-D).$$

For convenience set $\theta = (u-r)+(v-s)\alpha$ and note that $N(\theta) < 1$ when $D = -1$ or -2.

We have

$$p + q\alpha = (a + b\alpha)(r + s\alpha) + (a + b\alpha)\theta$$

and by multiplicativity of this norm function, the norm of the last term is less than $N(a+b\alpha)$, so $(a+b\alpha)\theta$ has the desired property of the remainder.

(b) Case of $D = -3, -7, -11$. In these cases $\mathcal{O}(D)$ is $\mathbb{Z}[X]/(X^2 - X - s)$ where $s = -1, -2, -3$ respectively. Setting α to the the image of X as before, we have the norm equal to

$$N(a + b\alpha) = a^2 + ab - sb^2 = (a + \frac{b}{2})^2 - (s + \frac{1}{4})b^2.$$

Noting that $D = 1 + 4s$ we note that the last term simplifies to $-(\frac{D}{4})b^2$.

We imitate the above proof by writing

$$u + v\alpha = \frac{p + q\alpha}{a + b\alpha}$$

where $u, v \in \mathbb{Q}$.

Find $r, s \in \mathbb{Z}$ such that

$$|v - s| \leq \frac{1}{2} \geq |(u + \frac{v}{2}) - (r + \frac{s}{2})| = |(u - r) + \frac{v - s}{2}|.$$

Let as before $\theta = (u - r) + (v - s)\alpha$ and note that

$$N(\theta) = \left((u - r) + \frac{v - s}{2}\right)^2 - \frac{D}{4}(v - s)^2.$$

Thus when $D = -3, -7$ or -11

$$N(\theta) \leq \frac{1}{4} + \frac{|D|}{16} = \frac{4 + |D|}{16} < 1.$$

The rest of the proof follows as before giving $(a + b\alpha)\theta$ as a valid remainder.

3. **A domain which is a P.I.D. but not euclidean.** The ring $\mathcal{O}(-19)$ is very special. It is shown to be non euclidean under **any possible** norm and yet unlike the non euclidean ring $\mathcal{O}(-5)$ it is a P.I.D. - i.e. a domain in which every ideal is principal!

   Even though elementary, the proof is somewhat long and we leave it as an assignment to look it up and digest.

6 Principal Ideal Domains. P.I.D.

We now discuss some useful properties of PID or more generally of PIR (principal ideal ring).

1. **Stability of an increasing sequence of principal ideals.**

   Let R be a principal ideal ring (PIR) and if $(x_1, x_2, \cdots, x_n, \cdots)$ is a sequence of elements in R, such that x_{n+1} divides x_n for all $n \geq 1$. (In other words, $x_n \in (x_{n+1})$ = the ideal generated by x_{n+1}.)

   Then the sequence of ideals (I_n) stabilizes for $n >> 0$, which means there is some sufficiently large N such that $I_N = I_n$ for all $n \geq N$.

   Proof. The ideal generated by all the x_i is generated by some x, since R is a PIR. Thus $x = \sum_1^N a_i x_i$ for some N where $a_N \neq 0$. From the given divisibility, we see that $x \in x_N$. Since $x_N \in (x)$ we see that $(x) = (x_N)$. It follows that for any $n > N$, we have $I_N = (x_N) \subset (x_n) = I_n$ from hypothesis, while $I_n \subset (x) = (x_N) = I_N$ from construction.

   Hence $I_n = I_N$ for all $n \geq N$.

2. **Definition: Irreducible/reducible element** An element x in a domain R is said to be reducible if $x = yz$ for some $y, z \in R$ such that x is not an associate of either y or z. Equivalently, we could also state the condition as neither y nor z is a unit.

   Yet another way of stating the condition is to write $x = yz$ for some $y, z \in R$ such that $(x) \neq (y)$ and $(x) \neq (z)$.

   An element x in a domain is said to be irreducible if it is not reducible.

Note that units are irreducible under this definition and so is the zero element.

Remark. If the ring is not an integral domain, then the different formulations are not necessarily equivalent and we leave the generalizations to the reader's imagination at this point.

3. **Factorization in a PID.** We now prove that every element of a PID can be written as a product of finitely many irreducible elements.

   Proof. Suppose if possible we have a non empty collection of elements which cannot be written as a product of finitely many irreducible elements. For convenience, let us call them "bad" elements. Any element which is a product of finitely many irreducibles will be called good. Note that product of finitely many good elements is obviously a product of finitely many irreducibles and hence good.

   Consider the set

   $$S = \{(x) | x \in R \text{ and } x \text{ is bad.}\}$$

   Note that a bad element x must be factor-able as $x = yz$ such that at least one of y, z is again bad and x is not an associate of either y or z.

   For proof of this, note that x being bad, must be reducible, otherwise it is a singleton product of irreducibles. Also, we already know that if y, z were good then so would be x, a contradiction.

   Thus, if y is bad then we get $(x) \subsetneq (y)$ where $(x), (y)$ both belong to S. Repeating this process, we can get an infinite sequence of principal ideals generated by bad elements:

   $$(x_1) \subsetneq (x_2) \subsetneq \cdots \subsetneq (x_n) \cdots \text{ with } (x_n) \in S \text{ for all } n = 1, 2, \cdots .$$

   This is a contradiction to the stability of an increasing sequence of ideals that we established.

4. Uniqueness of expression. Now that we have established existence of factorization of elements as products of irreducibles, we investigate the uniqueness of such an expression.

   First we need a Lemma.

   Lemma. Irreducible is prime in a PID. If x is an irreducible element in a PID R, then the ideal (x) is a prime ideal.

   Proof. Suppose that $yz \in (x)$ where $y, z \in R$ and $y \notin (x)$. We wish to show that $z \in (x)$.

Set the ideal $I = (x, y)$ and assume that $I = (w)$ for some w. Clearly, we can write $w = ax + by$ for some $a, b \in R$. Note that $x, y \in (w)$. Since x is irreducible, either w is a unit or $(w) = (x)$. Clearly, if $(w) = (x)$ then we get $y \in (w) = (x)$ a contradiction.

Hence w is a unit. Now $wz = axz + byz \in (x)$, since $yz \in (x)$. Since w is a unit, $z \in (x)$ as we needed.

■

Now we shall prove the uniqueness of the factorizations. Here is the statement:

Given any non zero element $x \in R$ where R is a PID, there is a finite set of prime ideals $P(x) = \{(p_1), \cdots, (p_n)\}$, and a set of non negative integers $\{a_1, \cdots, a_n\}$ such that x is an associate of $\prod_1^n p_i^{a_i}$.

The set of prime ideals $P(x)$ is uniquely determined by x and for each $(p_i) \in P(x)$, the corresponding exponent a_i is also uniquely determined by x.

Proof. First we shall establish the uniqueness of $P(x)$. So suppose, if possible

$$x = \epsilon \prod_{i=1}^{n} p_i^{a_i} = \tau \prod_{j=1}^{m} q_i^{b_i}$$

where ϵ, τ are units in R. Consider the corresonding sets of primes $S = \{(p_i)\}_1^n$ and $T = \{(q_j)\}_1^m$ where we are naturally assuming that $\{(p_i)\}$ are distinct primes and similarly $\{(q_j)\}$ are distinct primes.

Since q_j divides x, it is clear that it divides one of $p_1, \cdots, p_n$ and if q_j divides p_i, we must have $(q_j) = (p_i)$, since p_i is irreducible. Thus we see that every member of T is in S. Similarly every member of S is in T and thus $S = T$ and this common set of prime ideals is the $P(x)$ which is thus uniquely determined by x.

The only remaining thing to prove is the uniqueness of exponents. Suppose if possible we have an example of non uniqueness:

$$x = \epsilon \prod_{i=1}^{n} p_i^{a_i} = \tau \prod_{i=1}^{n} p_i^{b_i}$$

where ϵ, τ are units. Moreover, all a_i are non negative and some $a_i \neq b_i$.

Without loss of generality we may assume that $0 < a_1 < b_1$. Clearly $x \in (p_1^{a_1})$ and write $x = yp_1^{a_1}$. Then we see that

$$y = \epsilon \prod_{i=2}^{n} p_i^{a_i} = \tau p_1^{b_1 - a_1} \prod_{i=2}^{n} p_i^{b_i}.$$

Here the first expression for y is not divisible by p_1, while the second one is divisible by p_1 since $b_1 - a_1 > 0$. This is a contradiction and we have the uniqueness established.

7 Unique Factorization Domains. U.F.D.

Remark. What we have proved above is actually more general. We did not really use the PID property, but used the following two properties:

1. R is a domain in which every element is a finite product of irreducible elements times a unit. In notation this means:

$$x = \epsilon \prod_{1}^{n} p_i^{a_i}$$

where p_i is irreducible and ϵ is a unit.

2. Every irreducible element p is prime, which means it generates a prime ideal (p).

What we concluded is that then every element $x \in R$ has an expression as a unit times a finite product of prime elements:

$$x = \epsilon \prod_{i=1}^{n} p_i^{a_i}$$

where ϵ is a unit in R and the set of prime ideals $\{(p_i)\}$ is completely determined by x and is denoted as $P(x)$. For every $(p) \in P(x)$ the exponent of p in the factorization is well defined and in this sense, the product expression is unique up to rearrangement and choice of generators of prime ideals in $P(x)$.

Integral domains r in which such unique product expressions occur are called **unique factorization domains** of **U.F.D.** for short.

Thus, the result of the previous section can now be summarized by saying that a P.I.D. is a U.F.D.

It would be convenient to make a notation $\text{ord}_{(p)}(x)$ where (p) is any principle prime ideal in a U.F.D. R and x is any non zero element of R.

We define $\text{ord}_{(p)}(x) = 0$ if $x \notin (p)$. If $x \in (p)$, then we can find a largest r such that $x \in (p^r)$ and thus $x \notin (p^{r+1})$.

We define $\text{ord}_{(p)}(x) = r$. It is easy to see that if we have a factorization:

$$x = \epsilon \prod_{1}^{n} p_i^{a_i}$$

then $\mathrm{ord}_{(p_i)}(x) = a_i$ for $i = 1, \cdots, n$ and $\mathrm{ord}_(p)(x) = 0$ if $p \notin P(x)$.

A basic result about U.F.D. gives a large set of examples of U.F.D.s.

Theorem. Let R be a domain and $S \subset R$ multiplicatively generated by a set of non zero prime elements and all units of R. Suppose that the ring $S^{-1}R$ is a U.F.D.

Finiteness Assumption. Also assume that a non zero element $x \in R$ can always be written as $x = sy$ where $s \in S$ and y is not divisible by any prime element in S. For convenience, we may call this **a convenient factorization** of x.[8]

Then R is a U.F.D.

Conversely, if R is a U.F.D., then so is $S^{-1}R$.

Proof. Let $B = S^{-1}R$ and note that B is evidently a domain. The natural map of R into B given by $r \to \frac{r}{1}$ is injective and we naturally identify R with its image. Thus we will simply assume that R is a sub-ring of B, which, in turn is contained in the quotient field of R.

Let $x = \frac{a}{s} \in B$ be a non zero element where $a \in R$ and $s \in S$. We write $x = \frac{s_1 a_1}{s}$ where, $s_1 a_1$ is a convenient factorization of a.

We may further assume that s, s_1 don't have any common factors, since we could simply drop them off first.

We claim that $\frac{a}{s}$ is an irreducible non unit in B if and only if a_1 is an irreducible non unit in R.

For proof, note that, if a_1 is a unit in R, then clearly x is a unit in B, contrary to the hypothesis. Suppose, if possible a_1 is reducible in R, say $a_1 = uv$, where u, v are non units in R outside S. Then clearly $x = \frac{s_1 u}{s} \frac{v}{1}$ and x becomes reducible in B contrary to the hypothesis. Thus an irreducible element of B is simply an irreducible element a_1 of R multiplied by a unit $\frac{s_1}{s}$ in B.

Let r be any irreducible non unit element of R. If $r \in S$, then it must be a prime element of R by our hypothesis.

If $r \notin S$, then it is not divisible by any element of S and we claim that it is an irreducible element of B. Suppose if possible $r = \frac{u_1}{s_1} \frac{u_2}{s_2}$ is a factorization into non units in B.

Then we see that $s_1 s_2 r = u_1 u_2$. Since S is generated by prime elements, the element $s_1 s_2$ can be canceled from both sides leaving a new factorization $r = v_1 v_2$ where each v_i is equal to u_i divided by suitable elements of S.

Since r is irreducible in R, one of $\{v_i\}$ must be a unit, i.e. the corresponding u_i must be a unit in B, a contradiction!

Now we claim that an irreducible $r \in R$ is a prime element in R. As before, if $r \in S$ then we are done by hypothesis. If not, we know that $r = \frac{r}{1}$ is prime in B. Thus if $r = xy$ is a factorization into non units in R, then r

[8] It may be shown that this is essentially unique, except for unit multipliers.

divides one of x, y in B.

Without loss of generality, assume $x = r\frac{z}{s}$, where $z \in R$ and $s \in S$. Thus $sx = rz$ and no factors of s divide r. Therefor s divides z, i.e. $z = sz_1$ with $z_1 \in R$. Then $x = rz_1$, proving primeness of r.

Now we have everything we need to prove that R is a U.F.D.

Any $x \in R$ can be written as a product of prime elements times a unit in B. Clearing denominators and using the above analysis, we see that

$$sx = t \prod_i u_i$$

where $s, t \in S$ and u_i are irreducible elements of R which are not in S. Note that the product is allowed to be empty.

Using primeness of factors of R and description of $\{u_i\}$ we see that $t = sw$ for some $w \in S$ and we have the factorization

$$x = \left(\prod_j w_j\right)\left(\prod_i u_i\right)$$

where we have split up w into its prime factors (all in S).

The uniqueness follows from the primeness of the factors as above.

The converse part is evident.

Remark. The finiteness condition is necessary as shown by the following example.

Let K be any field and let A be the polynomial ring in two variables $K[X, Y]$.

Pick any sequence of non zero irreducible polynomials $y_1, y_2, \cdots$ in $K[Y]$. Let

$$R = K[X, Y, \frac{X}{y_1}, \frac{X}{y_1 y_2}, \cdots, \frac{X}{y_1 y_2 \cdots y_n}, \cdots].$$

Let S be the multiplicative set generated by units of R and the polynomials $y_1, \cdots, y_n, \cdot$.

Then it can be shown that R is not a UFD since the element X in R is divisible by $y_1 y_2 \cdots y_n$ for every n.

The ring $S^{-1}R$ is however a localization of $K(Y)[X]$ and hence is a U.F.D.

Thus, it is necessary to assume the finiteness condition.

8 Fields and Galois Theory.

We present a quick overview of Galois Theory of fields, with details to be filled in as we go on.

1. Let F be a field and L an over-field. The field L is naturally a vector space over F. The extension L/F is said to be finite if the $\dim_F(L)$ is finite and we shall denote this dimension by the suggestive notation $[L : F]$.

2. The simplest example of a finite field extension is as follows. Let $f(X) = X^n + a_1 X^{n-1} + \cdots + a_n \in F[X]$ be an irreducible polynomial. Then we know that $I = (f(X)) \in F[X]$ is a maximal ideal and hence $F[X]/I$ is a field.

   The field $L = F[X]/I$ can be described more explicitly as follows. Set $\alpha = \overline{X}$ the image of X modulo I. Let $\overline{F}$ denote the set of elements of F modulo I. We first note that the natural residue map $F \to \overline{F}$ is a homomorphism, and since F is a field and the map is not the zero map, it is an isomorphism. Thus, we can and almost always do, replace the residue class $\overline{a}$ by a when $a \in F$.

   Thus, without further explanation, we declare that $F \subset L$ when in reality only an isomorphic copy $\overline{F} \subset L$.

   Now L can be described as the set of all possible residue classes of polynomials modulo I. Clearly, for any polynomial $g(X)$ we see that $g(X) \equiv r(X) \mod (I)$ if $r(X)$ is the remainder of $g(X)$ when divided by $f(X)$. Using that $\overline{X} = \alpha$ we see that

   $$L = \{r_{n-1}\alpha^{n-1} + \cdots + r_0 \mid r_i \in F\}.$$

   Moreover, it is easy to see that $1, \alpha, \cdots, \alpha^{n-1}$ is a basis of L over F and thus we have the theorem that $[L : F] = n$. We can, and do, write $L = F[\alpha] = F(\alpha)$. [9]

3. **Field Polynomials.** Let z be any element of L and let ϕ_z denote the multiplication map by z. This is clearly a linear transformation of the vector space L over F and we can make equations

   $$\phi_z(v_i) = zv_i = \sum_{j=1}^{n} a_{ij} v_j$$

[9] There is a subtle but important point here. As described, L is really the set of all polynomials in α over F and hence $F[\alpha]$ is an appropriate notation. However, since it is a field, it is equal to its quotient field, or the same as the field of all rational functions in α. The second notation brings this fact out. In general, for an arbitrary element α these notations make sense and are different entities.

where $v_1 = 1, v_2 = \alpha, \cdots, v_n = \alpha^{n-1}$ is a natural basis of L/F.

This gives a natural matrix equation:

$$(z\mathcal{I} - A)V = 0$$

where V is the column vector formed by the basis elements and A is the matrix formed by the (a_{ij}).

By Cramer's Rule, we see that

$$\det((z\mathcal{I} - A))v_i = 0 \text{ for all } i = 1, \cdots, n.$$

In particular, noting that $v_1 = 1$ we get the polynomial equation $H(X) = \det((X\mathcal{I} - A)) = 0$, satisfied by z.

Thus, we have proved that every element of L satisfies a polynomial equation over F of degree at most $n = [L : F]$.

Remark. The above calculation can be extended by replacing ϕ_z by any linear transformation of a vector space to itself and gives among other things, the famous Cayley-Hamilton theorem and concepts of determinants and traces of linear transformations. This is an important technique in linear algebra.

4. Two facts may be noted about the above argument.

   Working over a ring F. The above calculation can be redone by assuming F to be only a ring and we can argue that F is still isomorphic to its image $\overline{F}$ in $F[X]/I$. We simply need the fact that no multiple of the monic polynomial $f(X)$ can be a constant in F except for 0. Indeed, the only reason we assumed monicness above was to make this come out for the ring case.

   The element α then is an integral element over F, where we use:

   Definition: An element is said to be integral over a ring R if it is the root of a monic polynomial over R.

   Now, the argument with Cramer's rule made any random element z of $F[\alpha]$ to satisfy the corresponding polynomial equation $H(X) = 0$ where $H(X)$ is visibly monic! Thus we have proved the

   Theorem If α is integral over F, then so is every element of the ring $L[\alpha]$. Thus, it makes sense to say that $L[\alpha]/F$ is an integral extension. This gives a natural definition of one ring being integral over another.

   Definition: Integral extension. A ring S is said to be integral over a ring R if every element of S is integral over R. This can also be descibed by saying that S is integral over R.

The ring S would be said to be an integral extension of R if $R \subset S$ and S is integral over R.

Naturally, we also make a:

Definition: Integrally closed. A ring R is said to be integrally closed in S if every element of S integral over R is already in R. A domain is said to be integrally closed or normal if it is integrally closed in its quotient field.

If we take a polynomial $g(X)$ whose image is the element z discussed above, then we note that the resulting polynomial $H(X)$ and in particular its constant term is completely defined by the two polynomials $f(X), g(X)$. In particular the constant term $H(0)$ evaluates to $(-1)^n \det(A)$ and is of special significance. It is $(-1)^n$ times the resultant of the polynomials $f(X)$ and $g(X)$ and in this form, it is called the **Bezout resultant.** In practice the sign is normalized by people in certain ways, since it clearly depends on the order of the basis.

If F is only a ring (and not a field), then the division by a monic polynomial still keeps the remainders with coefficients in the ring and we see that our resultant is a robust object defined over any base ring when one of the polynomials is monic.

There is a version of the resultant which even lets go of the monicness hypothesis and is called the **Sylvester resultant.** We don't need to worry about it at this point, except to note that it is far more convenient to write and may be used in practice, since it avoids the division algorithm altogether, at the cost of enlarging the size of the determinant to $(n+m) \times (n+m)$.

5. **Another free bonus.** Let us generalize our calculations even further.

   Thus let L/F be any finite field extension with $[L : F] = n$. Let $w = (w_1, \cdots, w_n)$ be any basis of L over F. We can do the same calculations as above for any given $z \in L$ and produce a monic polynomial $H(X)$ of degree n such that $H(z) = 0$.

   With a little analysis of the change of basis formula, it is easy to show that the polynomial is independent of choice of the basis. [10]

   Thus we may make a notation $H_z^{L/F}(X)$ for our polynomial and it is called the field polynomial of z for the extension L/F.

[10] Show that if another basis is given as wP where P is an invertible $n \times n$ matrix, then the resulting matrix for the new basis is similar to the old, conjugated by the transpose of P. Thus, the determinant is the same!

If we consider the field $F(z)$ generated by the element z, then it makes sense to compare the two field polynomials

$$H_z^{L/F}(X) \text{ and } H_z^{F(z)/F}(X).$$

By a suitable choice of basis, it can be shown that the first is a power of the second by the field degree $[L : F(z)]$. Thus, this polynomial contains lot of information about the field extension $F(z)$. [11]

6. The constant term $H_z^{L/F}(0)$ of the field polynomial is important and we have studied it before. It used to be called the field norm $N_{L/F}(z)$. We, of course, did not mention the fields earlier, since they were fixed.

   The comparison of field polnomials above gives a very useful result for the norms, namely:

$$N_{L/F}(z) = N_{F(z)/F}(z)^{[L:F(z)]}.$$

8.1 Splitting field.

Let us fix a monic polynomial

$$f(X) = X^n + a_1X^{n-1} + \cdots a_n \text{ where } F \text{ is a field with } a_i \in F.$$

We wish to find an over-field L such that $f(X)$ factors completely into linear factors over L. We also wish to show that the smallest subfield of L over which the factorization occurs is unique up to isomorphism.

First, we prove existence of a field L by induction on n.

It is obvious that for $n = 1$, we have nothing to prove since $f(X)$ is already linear.

If $g(X)$ is a monic irreducible factor of $f(X)$, then we know that $L_1 = F[X]/(g(X))$ is a field containing an isomorphic copy of F and having a root of $g(X)$. Identifying F with its image in L_1 we see that over L_1 we have a factorization: $f(X) = (X - \alpha)f^*(X)$ where $X = \alpha$ is a root of the factor $g(X)$ of $f(X)$ in L_1. Since the degree of $f^*(X)$ is $n - 1$, we know that by induction, there is a field L containing L_1 over which $f^*(X)$ factors completely into linear factors.

Thus over L we have a complete factorization:

$$f(X) = \prod_1^n (X - \alpha_i)$$

[11] Pick a basis of $L/F(z)$ as $1 = w_1, \cdots, w_r$ and pick a basis of $F(z)/F$ as $1 = t_1, \cdots, t_s$. Then it is not hard to see that a basis of L/F is obtained by $(w_1t_1, \cdots, w_1t_s, w_2t_1, \cdots, w_2t_s, \cdots, w_rt_1, \cdots, w_rt_s)$ and with respect to this basis, the matrix of the transformation ϕ_z has r identical blocks down the diagonal. Thus its determinant is the determinant of the first block raised to the r-th power as required.

where $\alpha = \alpha_1, \cdots, \alpha_n$ are all the roots of $f(X)$ in L.

A smallest subfield of L over which $f(X)$ factors completely may be described as $F(\alpha_1, \cdots, \alpha_n)$ which can be described as fields obtained by successively adjoining one of these at a time.

We make a

Definition: Splitting field. The field $F(\alpha_1, \cdots, \alpha_n)$ is said to be a splitting field of $f(X)$ over F.

We shall now show that any two splitting fields of the same polynomial $f(X)$ are F-isomorphic, meaning, there is an isomorphism between them which is identity on the field F.

It would be more convenient to prove the following more general

Theorem. Let $\sigma : F_1 \to F_2$ be two fields with an isomorphism σ between them. Let σ be naturally extended to polynomial rings $\sigma : F_1[X] \to F_2[X]$ by defining $\sigma(X) = X$.

Let $L_1 = F_1(\alpha_1, \cdots, \alpha_n)$ and $L_2 = F_2(\beta_1, \cdots, \beta_n)$ be corresponding splitting fields for $f_1(X) = f(X)$ and $f_2(X) = \sigma(f(X))$. Note that the roots are repeated if necessary to match respective multiplicities.

Then $L_1 \cong L_2$.

Proof.

Again we shall make induction on $n = \deg_X(f(X))$ and note that the result is obvious for $n = 1$.

Assume that $g_1(X)$ is an irreducible monic factor of $f_1(X)$ with root α_1. By renumbering, if necessary, assume that β_1 is a root of $g_2(X) = \sigma(f_1(X))$.

then clearly, we have:

$$F_1(\alpha_1) \cong F_1[X]/(g_1(X)) \cong F_2[X]/(g_2(X)) \cong F_2(\beta_1)$$

where the middle isomorphism comes from σ. Set $K_1 = F_1(\alpha_1)$ and $K_2 = F_2(\beta_1)$. Note that we have an isomorphism σ^* from K_1 to K_2 which takes α_1 to β_1.

Note that we have a factorization $f_1(X) = (X - \alpha_1)f_1^*(X)$ over K_1 and $f_2(X) = (X - \beta_1)f_2^*(X)$ over K_2.

Moreover, L_1, L_2 are easily seen to be splitting fields for the polynomials $f_1^*(X)$ over K_1 and for $f_2^*(X)$ over K_2 with $\sigma^*(f_1^*(X)) = f_2^*(X)$.

It is then clear that the inductive hypothesis applying to the polynomials $f_1^*(X)$ and $f_2^*(X)$ gives the result.

8.2 Outline of results.

We now present the outline of results to be proved.

1. **Primitive Element Theorem (PET).** Let L/F be a finite field extension. Then L can be clearly generated by adjoining a finite sequence

of elements successively to F, i.e. $L = F(x_1, \cdots, x_m)$ for a finite sequence of algebraic elements. [12]

It is very useful to be able to prove that $L = F(x)$ for a single element x and we say that x is a primitive element of the extension L/F. We express this by saying L is a simple extension of F.

One necessary and sufficient condition for L/F to be simple is that there are only a finitely many fields between F and L.

2. Of course, this condition can be difficult to check, but a simpler sufficient condition is as follows.

   Definition: Separable. A polynomial $f(X) \in F[x]$ is said to be separable if it has no multiple roots or equivalently, the GCD of $f(X)$ and $f'(X)$ is 1. Note that in characteristic $p > 0$ we can have $f(X)$ with degree bigger than 1 such that $f'(X) = 0$ as a polynomial. In this case the GCD is $f(X)$ and the polynomial is not separable. This is also stated as "the polynomial is inseparable".

   An element $x \in L$ is said to be separable if the minimum polynomial satisfied by x over F is separable.

   The whole field extension L/F is separable if every element of L is separable over F. It can be easily seen that it is enough that L is generated by separable elements.

   Remark. There is a definition of separability which is valid when L/F is not even algebraic, but we postpone it to future.

   An easier to check sufficient condition for simplicity of L/F is that L/F is a finite separable extension.

3. **Galois extension.** An finite extension L/F is said to be Galois if it is the splitting field of some separable polynomial over F.

   Using the PET, we can deduce that $L = F(x)$ for some x. Moreover, it can be shown that the minimum polynomial $f(X)$ of x over F is separable and splits completely into linear factors in L, so L is indeed also the splitting field of $f(X)$.

   The Galois group $Gal(L/F)$ is abstractly defined as $Aut(L/F)$ the group of automorphisms of L which fix F element-wise.

   It can be shown that F is exactly the set of elements fixed by all elements of $Aut(L/F)$ and in turn, this property can be used as another characterization of a finite Galois extension.

[12] Note that every element of a finite field extension satisfies a polynomial equation (even a monic polynomial equation) over F as we have already shown.

Using that a Galois extension L of F is equal to $F(x)$ we can deduce the following. The minimum separable polynomial of x can be assumed to be

$$f(X) = X^n + a_1X^{n-1} + \cdots + a_n \text{ with } a_i \in F.$$

If $x = x_1, \cdots, x_n$ are all the distinct roots of $f(X)$ then we know that for each $i = 1, \cdots, n$ there are uniquely defined automorphisms $\sigma_i \in Aut(L/F)$ such that $\sigma(x) = x_i$. Moreover, the automorphism group consists of exactly these n elements.

In particular,

$$|Aut(L/F)| = [L : F] = n = \deg_X(f(X)).$$

4. **Fundamental Theorem of Galois Theory.** Let L/F be a finite Galois extension and let $G = Aut(L/F) = Gal(L/F)$ be its Galois group.

   For convenience, we shall assume $L = F(x)$ and set $f(X) = X^n + a_1X^{n-1} + \cdots + a_n \in F[X]$.

   Let H be any subgroup of G. Let $S_H = \{i|\sigma_i \in H\}$. Then clearly the polynomial

   $$f_H(X) = \prod_{i \in S_H} (X - x_i)$$

   is easily seen to be invariant under action of all elements of H (extended by sending X to itself) and thus all its coefficients are fixed by every element of H.

   We define the fixed field of H by:

   $$Fix(H) = \{u \in L|\sigma(u) = u \ \forall \sigma \in H\}$$

   It is easy to show that $Fix(H)$ is generated by all the coefficients of $F_H(X)$ over F and $L/Fix(H)$ is a Galois extension with Galois group H.

   Conversely, for any intermediate field $F \subset K \subset L$ we can factor $f(X)$ over K and take the irreducible factor of $f(X)$ which is divisible by $X - x_1$ over L.

   Denote it by ${}_Kf(X)$.

   It can be shown that

   $$\{\sigma_i|X - x_i \text{ divides } {}_Kf(X) \text{ over } L\}.$$

is a subgroup of G and its fixed field is K. We shall denote this subgroup by G_K.

Thus we get a one to one correspondence between subgroups of G and intermediate fields K.

5. Actually, the above description is unusual when compared to the standard descriptions. We are using the special structure of our Galois group using the fact that L is generated by x which is being permuted among conjugate roots.

   Here is how the usual definition goes.

   Consider the set

   $$G_K = \{\sigma \in G | \sigma(a) = a \ \forall a \in K\}.$$

   Then we can show that G_K is a subgroup of G and its fixed field $Fix(G_K)$ is equal to K.

   As a result, the field L can be thought of as a Galois extension of K with Galois group G_K. We note that $L = F(x)$ implies $L = K(x)$ and it is clearly the splitting field of ${}_Kf(X)$ over K. This is why the alternate description works.

6. In general, the field extension K/F is not Galois for an intermediate field K. There is a simple group theoretic test for this.

   The field extension K/F is Galois iff the corresponding subgroup G_K is normal in G.

7. **Connection with solvability.**

   This is crucial in the analysis of the solvability of an equation by radicals. A radical over a field is an m-th roots of an element of the field for some natural number m. A radical extension of a field F is a field $F(\alpha)$ where α is a radical over F. An iterated radical extension is a tower of successive radical extensions. It can be shown that extending further, if necessary, we can write an iterated radical extension as succession of Galois extensions with cyclic Galois groups. Thus, its Galois group is cyclic.

   Thus, if our equations is solvable by radicals, then its Galois group is seen to be a quotient of a solvable group, hence solvable by itself!

   For polynomials of degrees $2, 3, 4$, the classical formulas for roots can be interpreted as consequences of the fact that the resulting Galois groups are indeed solvable (being subgroups of S_n for $n \leq 4$.)

On the other hand, we can construct equations whose Galois groups are alternating or full symmetric groups of any desired degree (i.e. A_n or S_n) and from group theory, we know that these are not solvable as groups.

This solved the fundamental problem of proving that an equation of degree 5 or bigger cannot be solved by adjoining iterated radicals. This is the genesis of the fame of Galois and his theory and one of the main reason for continued activity in this field.

8.3 Problems of Galois Theory.

We list some problems that we can solve, some we may be able to solve in due time and some which are not yet solved!

1. What are the possible Galois groups $Gal(L/F)$ when F is a finite field. **Answer.** The Galois group is always cyclic and if $|F| = q = p^r$ for some r, then it is generated by the Frobenius σ_q defined by $\sigma_q(x) = x^q$.

2. What are the possible Galois groups for splitting fields of polynomials of small degrees?

   Answer. For polynomials of degrees $2, 3, 4$ such groups are subgroups of S_2, S_3, S_4 respectively and there are explicit tests which will describe what the groups are.

3. Galois Theory also answered old geometric problems attempted by Greek geometers by showing that the equations to be solved give Galois groups which cannot be created by the allowed constructions using ruler and compass.

   This was another spectacular success.

4. An unsolved problem is the Dream of Kronecker, to show that every finite group is the Galois group of some polynomial over $\mathbb{Q}$.

   The solution of this for A_n and S_n goes back to Hilbert. Many special groups have been constructed by various mathematicians and have led to advances in group theory or algebraic geometry.

   Shafarevich is reputed to have proved that every solvable group is a Galois group. This old theorem had acquired a possible flaw in it some years back, the latest verdict needs to be checked.

5. The Above problem is completely known if we ask the question over $\mathbb{C}\ (t)$ rather than $\mathbb{Q}$. But it needs the full power of Riemann surfaces.

6. In general, Galois groups over $F(t)$ where F is a finite field or the algebraic closure of a finite field was studied by Abhyankar and he gave some necessary conditions on the Galois groups. Only in last few years, these were shown to be sufficient.

   His main condition was that the Galois group has to be quasi-p which means it is generated by its p-sylow subgroups. One of the simplest way to satisfy this condition is if the group is simple! Since one of the recent successes of Group Theory is to classify all finite simple groups, it becomes a natural research problem to construct equations with given simple Galois groups over a characteristic p field. Abhyankar and his several collaborators have solved this problems for many well known simple groups, the problem is not quite finished; except for the fact that the existence of such Galois groups has been established. Thus, this has been a fertile research area over last few years and has led to advances in Group theory as well as algebraic geometry.

7. We shall study several techniques to analyze the Galois group of a given small degree polynomial over $\mathbb{Q}$ or some suitable field.

8. One important tool in all of the above is to start with a monic polynomial over $\mathbb{Z}$ and reduce it modulo various primes. Since the Galois group is known to be cyclic after reduction, we can deduce existence of elements of certain type in the original Galois group. This combined with group theory can often lead to deduce what the original Galois group must be.

To be continued ...

Index

algebraic element, 12

division algorithm, 18
division ring, 4

euclidean domain, 18
- norm, 18

field, 4
field extension, 29
- finite, 29

field of fractions, 17
field polynomial, 29

Galois extension, 34
Galois group, 34
group
- ordered abelian, 7

ideal, 5
- colon of, 11
- generated by a set, 11
- intersection of, 11
- principle, 11
- product of, 11
- radical of, 12
- sum of, 11

identity in a ring, 2
inseparable, 34
integral domain, 4
integral element, 13, 30
integral extension, 30

norm
- Dedekind-Hasse, 20
- euclidean domain, 18

P.I.D., 20, 23
P.I.R., 20
primitive element, 34
primitive element theorem, 33
principal ideal domain, 20, 23
principal ideal ring, 20

quotient field, 17

resultant
- Bezout, 31
- Sylvester, 31

ring
- addition in, 2
- associate elements, 20
- characteristic of, 7
- commutative, 2
- definition of, 2
- divisibility, 3
- division ring, 4
- group ring, 9
- homomorphism, 6
  - image of, 6
  - kernel of, 6
- ideal, 5
- identity of, 2
- integral domain, 4
- integral over a subring, 13
- integrally closed., 31
- irreducible element, 23
- multiplication in, 2
- multiplicatively closed set, 16
- noetherian, 11
- normal, 31
- polynomial ring, 8
- power series ring, 8
- quotient ring, 5
- reducible element, 23
- subring, 4
- unit in, 3
- zero divisor in, 3
- zero ring, 2

ring of algebraic integers, 18
ring of quadratic integers, 15

separable, 34
    element, 34
    extension, 34
    polynomial, 34
simple extension, 34
splitting field, 33

total quotient ring, 17
transcendental, 12

U.F.D., 26
    order with respect to a principle prime, 26
unique factorization domain, 26
unit in a ring, 3