LOVELY
PROFESSIONAL
UNIVERSITY

ABSTRACT ALGEBRA II

Edited By
Richa Nandra

Printed by
EXCEL BOOKS PRIVATE LIMITED
A-45, Naraina, Phase-I,
New Delhi-110028
for
Lovely Professional University
Phagwara

CONTENT

SYLLABUS

Abstract AlgebraII

Objectives:

- To learn about the structure as group, ring and field.
- To gain knowledge about homomorphisms, isomorphisms, cosets, quotient groups, and the isomorphism theorems, rings, ideals, ring homeomorphisms, isomorphisms and its theorems.
- To learn about fields, quotient fields and field extensions Galois Theory also.

Sr. No.	Content
1	Polynomial rings,The field of quotients Euclidean domains, Principal Ideal Domains, Unique factorization domain
2	Prime fields, finite and algebraic extensions, Roots of a polynomial
3	splitting fields; existence and uniqueness, Separable extensions, Finite fields; the structure, the existence of GF (pn)
4	Galois theory :Normal extensions, Galois groups
5	Symmetric functions, fundamental theorem, Constructible polygons, Solvability by radicals

Richa Nandra, Lovely Professional University

Unit 1 : The Field of Quotient Euclidean Domains

CONTENTS

Objectives

After studying this unit, you will be able to:

- Discuss whether an algebraic system is an integral domain or not
- Define and identify prime ideals and maximal ideals
- Prove and use simple properties of integral domains and fields
- Construct or identify the field of quotients of an integral domain

Introduction

Finally, we shall see how to construct the smallest field that contains a given integral domain. This is essentially the way that Q is constructed from Z. We call such a field the field of quotients of the corresponding integral domain.

In this unit, we have tried to introduce you to a lot of new concepts. You may need some time to grasp them. Take as much time as you need. But by the time you finish it, make sure that you have attained the knowledge of following topics.

1 .1 Prime and Maximal Ideals

In 'Z' we know that if p is a prime number and p divides the product of two integers a and b, then either p divides a or p divides b. In other words, if $ab \in pZ$, then either $a \in pZ$ or $b \in pZ$. Because of this property we say that pZ is a prime ideal, a term we will define now.

Definition: A proper ideal P of a ring R is called a prime ideal of R if whenever $ab \in P$ for $a, b \in R$, then either $a \in P$ or $b \in P$.

You can see that {0} is a prime ideal of Z because $ab \in \{0\} \Rightarrow a \in \{0\}$ or $b \in \{0\}$, where $a,b \in Z$.

Another example of a prime ideal is

Example: Let R be an integral domain. Show that I = ((0, x) | x ∈ R) is a prime ideal of R x R.

Solution: Firstly, you know that I is an ideal of R x R. Next, it is a proper ideal since I ≠ R x R. Now, let us check if I is a prime ideal or not. For this let (a_1, b_1), (a_2, b_2) ∈ R x R such that (a_1, b_1) (a_2, b_2) ∈ I. Then (a_1a_2, b_1b_2) = (0, x) for some x ∈ R

∴ $a_1a_2 = 0$, i.e., a, = 0 or $a_2 = 0$, since R is a domain. Therefore, (a, b_1) ∈ I or (a_2, b_2) ∈ I. Thus, I is a prime ideal.

Now we will, prove the relationship between integral domains and prime ideals.

Theorem 1: An ideal P of a ring R with identity is a prime ideal of R if and only if the quotient ring R/P is an integral domain.

Proof: Let us first assume that P is a prime ideal of R. Since R has identity, so has R/P. Now, let a + P and b + P be in R/P such that (ai – P) (b + P) = P, the zero element of R/P. Then ab+P = P, i.e., ab ∈ P. As P is a prime ideal of R either a ∈ P or b ∈ P. So either a + P = P or b+P = P.

Thus, R/P has no zero divisors.

Hence, R/P is an integral domain.

Conversely, assume that R/P is an integral domain. Let a, b ∈ R such that ab ∈ P. Then ab + P = P in R/P, i.e., (a + P) (b + P) = P in R/P. As R/P is an integral domain, either a + P = P or b + P = P, i.e., either a E P or b ∈ P. This shows that P is a prime ideal of R.

An ideal mZ of Z is prime iff m is a prime number. Can we generalise this relationship between prime numbers and prime ideals in Z to any integral domain? To answer this let us first try and suitably generalise the concepts of divisibility and prime elements.

Definition: In a ring R, we say that an elements divides an element b if b = ra for some r ∈ R. In this case we also say that a is a factor of b, or a is a divisor of b.

Thus, $\overline{3}$ divides 6 in Z_7, since $\overline{3}.\overline{2} = \overline{6}$.

Now let us see what a prime element is.

Definition: A non-zero element p of an integral domain R is called n prime element if

(i) p does not have a multiplicative inverse, and

(ii) whenever a, b ∈ R and p | ab, then p | a or p | b.

Can you say what the prime elements of Z are? They are precisely the prime numbers and their negatives.

Now that we know what a prime element is, let us see if we can relate prime ideals and prime elements in an integral domain.

Theorem 2: Let R be an integral domain. A non-zero element p ∈ R is n prime element if and only if Rp is a prime ideal of R.

Proof: Let us first assume that p is a prime element in R. Since p does not have a multiplicative inverse, 1 ∉ Rp. Thus, Rp is a proper ideal of R. Now let a, b ∈ R such that ab ∈ Rp. Then ab = rp for some r ∈ R

⇒ p | a or p | b, since p is a prime element.

⇒ a = xp or b = xp for some x ∈ R.

⇒ a ∈ p or b ∈ Rp .

Thus ab ∈ Rp ⇒ either a ∈ Rp or b G ∈ Rp, i.e., Rp is a prime ideal of R.

Note $x \in R$ has a multiplicative inverse iff $Rx = R$.

Conversely, assume that Rp is a prime ideal. Then $Rp \neq R$, Thus, $1 \notin Rp$, and hence, p does not have a multiplicative inverse. Now suppose p divides ab, where $a, b \in R$. Then $ab = rp$ far some $r \in R$, i.e., $ab \in Rp$.

As Rp is a prime ideal, either $a \in Rp$ or $b \in Rp$. Hence, either $p \mid a$ or $p \mid b$. Thus, p is a prime element in R.

Theorem 2 is very useful for checking whether an element is a prime element or not, or for finding out when a principal ideal is a prime ideal.

Prime ideals have several useful properties.

Now consider the ideal 22 in Z. Suppose the ideal nZ in Z is such that $2Z \subseteq nZ \subseteq Z$. Then $n \mid 2$. $\therefore$ $n= \pm 1$or $n = \pm 2$. $\therefore$ $nZ = Z$ or $nZ = 2Z$.

This shows that no ideal can lie between 2Z and Z. That is, 22 is maximal among the proper ideals of Z that contain it. So we say that it is a "maximal ideal". Let us define this expression.

Definition: A proper ideal M of a ring R is called a maximal ideal if whenever I is an ideal of R such that $M \subseteq I \subseteq R$, then either $I = M$ or $I = R$.

Thus, a proper ideal M is a maximal ideal if there is no proper ideal of R which contains it. An example that comes to mind immediately is the zero ideal in any field F. This is maximal because you know that the only other ideal of F is F itself.

To generate more examples of maximal ideals, we can use the following characterisation of such ideals.

Theorem 3: Let R be a ring with identity. An ideal M in R is maximal if and only if R/M is a field.

Proof: Let us first assume that M is a maximal ideal of R. We want to prove that R/M is a field. For this, it is enough to prove that R/M has no non-zero proper ideals. So, let I be an ideal of R/M. Consider the canonical homomorphism $\eta : R \to R/M : \eta\,(r) = r + M$. Then, you know that η^{-1} (I) is an ideal of R containing M, the kernel of η. Since M is a maximal ideal of R. $\eta^{-1}(I) = M$ or $\eta^{-1}(I) = R$. Therefore, $I = \eta(\eta^{-1}\,(I))$ is either η(M) or η(R). That is, $I = \{\bar{0}\}$ or $I = R/M$, where; = O +M = M. Thus, R/M is a field.

Conversely, let M be an ideal of R such that R/M is a field. Then the only ideals of R/M are $\{\bar{0}\}$ and R/M. Let I be an ideal of R containing M. Then, as above $\eta(1) = \{\bar{0}\}$ or, $\eta(I) = R/M$.

$\therefore$ $I = \eta^{-1}(\eta(1))$ is M or R. Therefore, M is a maximal ideal of R.

Corollary: Every maximal ideal of a ring with identity is a prime ideal.

Now, the corollary is a one-way statement. What about the converse? That is, is every prime ideal maximal? What about the zero ideal in Z? Since Z is a domain but not a field and $Z \simeq Z/\{0\}$, $Z/\{0\}$ is a domain but not a field. Thus. (0) is a prime ideal but not a maximal ideal of Z.

Example: Show that an ideal mZ of Z is maximal iff m is a prime number.

Solution: You know that Z,,, is a field iff m is a prime number. You also know that $Z/mZ = Z_m$. $Z \mid mZ$ is a field iff m is prime. Hence, mZ is maximal in Z iff m is a prime number.

Example: Show that $\bar{2}Z_{12}$ is a maximal ideal of Z_{12}, whereas $(\bar{0},\bar{4},\bar{8})$ is not.

Solution: You know that Z_{12} = Z/12Z and $\bar{2}Z_{12}$ = 2Z/12Z. We see that $Z_{12}/\bar{2}Z_{12}$ = (Z/12Z)/(2Z/12Z) = Z_2, which is a field. Therefore, $\bar{2}Z_{12} = \{\bar{0},\bar{2},\bar{4},\bar{6},\bar{8},\overline{10}\}$ is maximal in Z_{12}.

Now $\{\bar{0},\bar{4},\bar{8}\} = \bar{4}Z_{12} \underline{\not\subset} \bar{2}Z_{12} \underline{\not\subset} Z_{12}$.

Therefore, $\{\bar{0},\bar{4},\bar{8}\}$ is not maximal in Z_{12}.

We first introduced you to a special ideal of a ring, called a prime ideal. Its speciality lies in the fact that the quotient ring corresponding to it is an integral domain.

Then we discussed a special kind of prime ideal, i.e., a maximal ideal.

1.2 Field of Quotients

Consider Z and Q. You know that every element of Q is of the form $\frac{a}{b}$, where a ∈ Z and b ∈ Z*.

Actually, we can also denote $\frac{a}{b}$ by the ordered pair (a, b) ∈ Z × Z*. Now, in Q we know that

$\frac{a}{b} = \frac{c}{d}$ = - iff ad = bc. Let us put a similar relation on the elements of Z × Z*

Now, we also know that the operations on Q are given by

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \text{and} \frac{a}{b}.\frac{c}{d} = \frac{a}{b}\frac{c}{d} \forall \frac{a}{b}, \frac{c}{d} \in Q.$$

Keeping these in mind we can define operations on Z × Z*. Then we can suitably define an equivalence relation on Z × Z* to get a field isomorphic to Q.

We can generalise this procedure to obtain a field from any integral domain. So, take an integral domain R. Let K be the following set of ordered pairs:

K= {(a,b)) a , b ∈ R and b ≠ 0)

We define a relation ~ in K by

(a, b) ~ (c, d) if ad = bc.

We claim that ~ is an equivalence relation. Let us see if this is so.

(i) (a, b) ~ (a, b) ∀ (a, b) ∈ K, since R is commutative. Thus, ~ is reflexive.

(ii) Let (a, b), (c, d) ∈ K such that (a, b) ~ (c, d). Then ad = bc, i.e., cb = da. Therefore, (c, d) ~ (a, b). Thus, ~ is symmetric.

(iii) Finally, let (a,b), (c,d), (u, v) ∈ K such that (a,b) – (c,d) and (c,d) ~ (u,v). Then ad = bc and cv = du. Therefore, (ad) v = (bc)v = bdu, i.e., avd =bud. Thus, by the cancellation law for multiplication (which is valid for a domain), we get av = bu, i.e., (a,b) – (u,v). Thus, – is transitive.

Hence, ~ is an equivalence relation.

Let us denote the equivalence class that contains (a,b) by [a,b]. Thus,

$[a,b] = \{(c,d) \mid c,d \in R,\ d \neq 0 \text{ and } ad = bc\}$.

Let F be the set of all equivalence classes of K with respect to ~.

Let us define + and in F as follows. (It might help you to keep in mind the rules for adding and multiplying rational numbers.)

$[a,b] + [c,d] = [ad+bc,bd]$ and

$[a,b].[c,d] = [ac,bd]$.

Do you think + and · are binary operations on F?

Note b # 0 and d # 0 in the integral domain R imply bd # 0. So, the right-hand sides of the equations given above are well defined equivalence classes. Thus, the sum and product of two elements in F is again an element in F.

We must make sure that these operations are well defined.

So, let $[a,b] = [a',b']$ and $[c,d] = [c',d']$. We have to show that $[a,b] + [c,d] = [a',b'] + [c',d']$, i.e., $[ad+bc,bd] = [a'd'+b'c',b'd']$.

Now, $(ad+bc)\, b'd' - (a'd' + b'c')\, bd$

$= ab'dd', + cd'bb' - a'bdd' - cdbb'$

$= (ab' - a'b)dd' + (cd' - c'd)\, bb'$

$= (0)\, dd' + (0)bb'$, since $(a,b) - (a', b')$ and $(c,d) \sim (c',d')$.

$= 0$

Hence, $[ad+bc,bd] = [a'\, d' + b'c',brd']$, i.e., + is well defined.

Now, let us show that $[a,b]\ .\ [c,d] = [a',br]\ .\ [c',d']$,

i.e., $[ac,bd] = [a'c'\ b'd']$.

Consider $(ac)\,(b'd') - (bd)\,(a'c')$

$= ab'cd' - ba'dc' = ba'cd' - ba'\, cd'$, since $ab' = bar$ and $cd' = dc'$

$= 0$

Therefore, $[ac,bd] = [a'c',b'd']$. Hence,. is well defined.

We will now prove that F is a field.

(i) + is associative : For [a,b], [c,d], [u,v] E F,

$$\begin{aligned}([a,b] + [c,d]) + [u,v] &= [ad+bc,bd] + [u,v]\\ &= [(ad+bc)v + ubd,\ Wv]\\ &= [adv + b(cv+ud),\ bdv]\\ &= [a,b] + [cv+ud,dv]\\ &= [a,b] + ([c,d]+ [u,v])\end{aligned}$$

(ii) + is commutative :.For [a,b], [c,d] $\in$ F,

[a,b] + [c,d] = [ad+bc,bd] = [cb+da,db] = [c,d] + [a,b]

(iii) [0,1] is the additive identity for F : For [a,b] $\in$ F,

[0,1] + [a,b] = [0.b+l.a, l.b] = [a,b]

(iv) The additive inverse of [a,b] $\in$ F is [–a,b] :

[a,b] + [–a,b] = [ab-ab,b^2] = [0,b^2] = [0,1], since 0.1 = 0.b^2.

We would like you to prove the rest of the requirements for F to be a field.

So we have put our heads together and proved that F is a field.

Now, let us define f : R $\rightarrow$ F : f(.a) = [a,1]. We want to show that f is a monomorphism.

Firstly, for a, b $\in$ R,

f(a+b) = [a+b,1] = [a,]] + [b,l].

= f(a) + f(b), and

Thus, f is a ring homomorphism.

Next, let a,b $\in$ R such that f(a) = f(b). Then [a,1] = [b,l], i.e., a = b. Therefore, f is 1–1.

Thus, f is a monomorphism.

So, Im f = (R) is a subring of F which is isomorphic to R.

As you know, isomorphic structures are algebraically identical.

So, we can identify R with f(R), and think of R as a subring of F. Now, any element of F is of the form [a,b] = [a,1] [l,b] = [a,l] [b,l]$^{-1}$ = f(a) f(b)$^{-1}$, where b $\neq$ 0. Thus, identifying x $\in$ R with f(x) $\in$ f(R), we can say that any element of F is of the form ab^{-1}, where a,b $\in$ R, b $\neq$ 0.

All that we have discussed adds up to the proof of the following theorem.

Theorem 4: Let R be an integral domain. Then R can be embedded in a field F such that every element of F has the form ab^{-1} for a, b $\in$ R, b $\neq$ 0.

The field F whose existence we have just proved is called the field of quotients (or the field of fraction) of R.

Thus, Q is the field of quotient of Z. What is the field of quotients of R? The following theorem answers this question.

Theorem 5: Iff : R $\rightarrow$ K is a monomorphism of an integral domain R into a field K, then there exists a monomorphism g : F $\rightarrow$ K : g([a,1]) = f(a), where F is the field of quotients of R.

It says that the-field of quotients of an integral domain is the smallest field containing it. Thus, the field of quotients of any field is the field itself.

So, the field of quotients of R is R and of Z_p is Z_p, where p is a prime number.

Self Assessment

1. An ideal P of a ring R is called a/an .... ideal of R. If whenever ab $\in$ P for a, b $\in$ R, then either a $\in$ P or b $\in$ P.

(a) prime ideal (b) odd ideal

(c) even ideal (d) integer ideal

2. An ideal P of a ring R with identity is a prime ideal of R. If and only if the .... R/P is an integral domain.

   (a) polynomial ring
   (b) subring
   (c) quotient ring
   (d) ideal ring

3. If x ∈ R, it has multiplicative inverse iff RX = ...

   (a) R
   (b) RX^{-1}
   (c) XR
   (d) X

4. A proper ideal m of a ring R is called maximal ideal of whenever I is an ideal of R such that m .... I .... R then either I = m or I = R.

   (a) $\cap, \cap$
   (b) $\supset, \cap$
   (c) $\subseteq, \subseteq$
   (d) $\supseteq, \supseteq$

5. If R be a ring with identity. An ideal M in R is maximal if and only if .... is a field.

   (a) R.M
   (b) R/M
   (c) M/R
   (d) R+M

1.3 Summary

- The characteristic of any domain or field is either zero or a prime number.
- The definition and examples of prime and maximal ideals.
- The proof and use of the fact that a proper ideal I of a ring R with identity is prime (or maximal) iff R/I is an integral domain (or a field).
- Every maximal ideal is a prime ideal.
- An element p of an integral domain R is prime iff the principal ideal pR is a prime ideal of R.
- Z, is a field iff n is a prime number.
- The construction of the field of quotients of an integral domain.

1.4 Keywords

Prime Ideal: A ideal P of a ring R is called a prime ideal of R if whenever ab ∈ P for a, b ∈ R, then either a ∈ P or b ∈ P.

Proper Ideal: A proper ideal M of a ring R is called a maximal ideal if whenever I is an ideal of R such that $M \subseteq I \subseteq R$, then either I = M or I = R.

Maximal Ideal: Every maximal ideal of a ring with identity is a prime ideal.

1.5 Review Questions

1. Let F be a field. Show that F, with the Euclidean valuation d defined by d(a) = 1 ∀ a ∈ F/{0}, is a Euclidean domain.

2. Let F be a field. Define the function

   $d : F(x)\backslash\{0\} \to N \cup \{0\} : d(f(x)) = \deg f(x).$

   Show that d is a Euclidean valuation on F[x], and hence, F[x] is a Euclidean domain.

3. Find all the units in

   (a) Z (b) Z_6 (c) Z/5Z (d) Z + IZ

4. Let R be an integral domain. Show that

   (a) u is a unit in R iff u | 1.

   (b) for a, b $\in$ R, a | b and b | a iff a and b are associates in R.

5. Which of the following polynomials is irreducible? Give reasons for your choice.

   (a) $x^2 - 2x + 1 \in R[x]$ (b) $x^2 + x + 1 \in C[x]$

   (c) $x - i \in C[x]$ (d) $x^3 - 3x^2 + 2x + 5 \in R[x]$.

Answers: Self Assessment

1. (a) 2. (c) 3. (a) 4. (c) 5. (b)

1.6 Further Readings

Books

Dan Saracino: Abstract Algebra; A First Course.

Mitchell and Mitchell: An Introduction to Abstract Algebra.

John B. Fraleigh: An Introduction to Abstract Algebra (Relevant Portion).

Online links

www.jmilne.org/math/CourseNotes/

www.math.niu.edu

www.maths.tcd.ie/

archives.math.utk.edu

Unit 2 : Principal Ideal Domains

CONTENTS

Objectives

After studying this unit, you will be able to:

- Discuss the Principal Ideal Domains
- Describe theorem related to Principal Ideal Domains

Introduction

In the last unit, you have studied about field and integer domain. In this unit, you will study about Principal Ideal Domains.

2.1 Euclidean Domain

In earlier classes you have seen that **Z** and F[x] satisfy a division algorithm. There are many other domains that have this property. Here we will introduce you to them and discuss some of their properties. Let us start with a definition.

Definition: Let R be an integral domain. We say that a function $d : R \setminus (0) \rightarrow NU\ (0)$ is a Euclidean valuation on R if the following conditions are satisfied:

(i) $d(a) \leq d\ (ab)\ \ \forall\ \ a, b \in R \setminus \{0\}$, and

(ii) for any $a, b \in k$, $b \neq 0\ 3\ q, r \in R$ such that

$a = bq+r$, where $r = 0$ or $d(r) < d(b)$.

And then R is called a Euclidean domain.

Thus, a domain on which we can define a Euclidean valuation is a Euclidean domain.

Let us consider an example.

Example: Show that Z is a Euclidean domain.

Solution: Define, $d : Z \rightarrow N \cup \{0\} : d(n) = |n|$.

Then, for any $a,b \in Z \setminus \{O]$,

$d(ab)= |ab| = |a|\ |b| \geq |a|$ (since $|\ b| \geq |$ for $b \neq 0$)

$= d(a).$

i.e., $d(a) \leq d(ab)$.

Further, the division algorithm in Z says that if $a, b \in Z, b \neq 0$, then 3 q, $r \in Z$ such that

$a = bq + r$, where $r = 0$ or $0 < |r| < |b|$.

i.e:, $a = bq+r$, where $r = 0$ or $d(r) < d(b)$.

Hence, d is a Euclidean valuation and Z is a Euclidean domain.

Let us now discuss some properties of Euclidean domains. The first property involves the concept of units. So let us define this concept. Note that this definition is valid for any integral domain.

Definition: Let R be an integral domain. An element $a \in R$ is called a unit (or an invertible element) in R, if we can find an element $b \in R$, such that $ab = 1$, i.e., if a has a multiplicative inverse.

For example, both 1 and -1 are units in Z since 1.1 = 1 and (-1).(-1) = 1.

Caution The difference between a unit in R and the unity in R. The unity is the identity with respect to multiplication and is certainly a unit. But a ring can have other units ton, as you have just seen in the case of Z.

Now, can we obtain all the units in a domain? You know that every non-zero element in a field F is invertible. Thus, the set of units of F′ is $F \setminus \{0\}$. Let us look at some examples.

Example: Obtain all the units in F[x], where F is a field.

Solution: Let $f(x) \in P[x]$ be a unit, Then $\exists\ g(x) \in F[x]$ such that $f(x) g(x) = 1$. Therefore,

deg f(x) g(x)) = deg(1) = 0, i.e.,

deg f(x) + deg g(x) = 0

Since deg f(x) and deg g(x) are non-negative integers, this equation can hold only if deg f(x) = 0 = deg g(x). Thus, f(x) must be a non-zero constant, i.e., an element of $F\setminus \{0\}$. Thus, the units of F[x] are the non-zero elements of F. That is, the units of F and F[x] coincide.

Example: Find all the units in R = $\left(a + b\sqrt{-5} \mid a, b \in Z\right)$.

Solution: Let $a + b\sqrt{-5}$ be a unit in R. Then there exists

$c + d\sqrt{-5} \in R$ such that

$\left(a + b\sqrt{-5}\right)\left(c + d\sqrt{-5}\right) = 1$

$\Rightarrow (ac - 5bd) + (bc + ad)\sqrt{-5} = 1$

$\Rightarrow\ ac - 5bd = 1$ and $bc+ad = 0$

$\Rightarrow abc - 5b^2d = b$ and $bc+ad = 0$

$\Rightarrow a(-ad) - 5b^2d = b$, substituting $bc = -ad$.

So, if $b \neq 0$, then $(a^2 + 5b^2) \mid b$, which is not possible.

$\therefore \qquad b = 0.$

Thus, the only units of R are the invertible elements of Z.

Theorem 1: Let R be a Euclidean domain with Euclidean valuation d. Then, for any $a \in R \setminus \{0\}$, $d(a) = d(l)$ iff a is a unit in K.

Proof: Let us first assume that $a \in R\setminus \{0]$ with $d(a) = d(1)$.

By the division algorithm in R, $\exists\ q, r \in R$ such that $1 = aq+r$,

where $r = 0$ or $d(r) < d(a) = d(1)$.

Now, if $r \neq 0$, $d(r) = d(r.1) \geq d(1)$. Thus, $d(r) < d(1)$ can't happen.

Thus, the only possibility for r is $r = 0$,

Therefore, $1 = aq$, so that a is a unit.

Conversely, assume that a is a unit in R. Let $b \in R$ such that $ab = 1$. Then $d(a) \leq d(ab) = d(1)$. But we know that $d(a) = d(a.1) \geq d(1)$. So, we must have $d(a) = d(1)$.

Using this theorem, we can immediately solve Example, since f(x) is a unit in F[x] iff deg f(x) = deg (1) = 0.

Now let us look at the ideals of a Euclidean domain.

Theorem 2: Let R be a Euclidean domain with Euclidean valuation d. Then every ideal I % of R is of the form $I = Ra$ for some $a \in R$.

Proof: If $I = (01$, then $I = Ka$, where $a = 0$. So let us assume that $I \neq \{0\}$. Then $I\setminus \{0\}$ is non-empty. Consider the set $\{d(a) \mid a \in I \setminus\{0\})$. The well ordering principle this set has a minimal element. Let this be d(b), where b e $I \setminus \{0\}$. We will show that $I = Rb$.

Since $b \in 1$ and I is an ideal of R,

$Rb \subseteq I.$ ...(1)

Now take any $a \in I$. Since $I \subseteq R$ and R is a Euclidean domain, we can find $q, r \in R$ such that

$a = bq + r$, where $r = 0$ or $d(r) < d(b)$.

Now, $b \in I \Rightarrow bq \in I$. Also, $a \in I$. Therefore, $r = a - bq \in I$.

But $r = 0$ or $d(r) < d(b)$, The way we have chosen d(b), $d(r) < d(b)$ is not possible.

Therefore, $r = 0$, and hence, $a = bq \in Rb$.

Thus, $I \subseteq Rb$. ...(2)

From (1) and (2) we get

$I = Rb$.

Thus, every ideal I of a Euclidean domain R with Euclidean valuation d is principal, and is generated by $a \in I$, where d(a) is a minimal element of the set $\{d(x) \mid x \in I \setminus (0)\ \}$.

Tasks

1. Show that every ideal of F[x] is principal, where F is a field.
2. Using Z as an example, show that the set
3. $S = (a \in R\setminus (0) \mid d(a) > d(1)\ \} \cup (0)$ is not an ideal of the Euclidean domain R with Euclidean valuation d.

2.2 Principal Ideal Domain (PID)

In the previous section you have proved that every ideal of F[x] is principal, where F is a field. There are several other integral domains, apart from Euclidean domains, which have this property. We give such rings a very appropriate name.

Definition: We call an integral domain R a principal ideal domain (PID, in short) if every ideal in R is a principal ideal.

Note Every Euclidean domain is a PID

Thus, Z is a PID. Can you think of another example of a PID? What about Q and Q[x]? In fact, by Theorem 2 all Euclidean domains are PIDs. But, the converse is not true. That is, every principal ideal domain is not a Euclidean domain.

For example, the ring of all complex numbers of the form $a+\frac{b}{2}\left(1+i\sqrt{19}\right)$, where a, b $\in$ Z, is a principal ideal domain, but not a Euclidean domain.

Now let us look at an example of an integral domain that is not a PID.

Example: Show that Z[x] is not a PID,

Solution: You know that Z[x] is a domain, since Z is one. We will show that all its ideals are not principal. Consider the ideal of Z[x] generated by 2 and x, i.e., < 2,x>. We want to show that < 2, x > $\neq$ <f(x)> for any f(x) $\in$ Z[X].

On the contrary, suppose that 3 f(x) $\in$ Z[x] such that < 2, x > = < f(x) >. Clearly, f(x) $\neq$ 0.

Also, 3 g(x), h(x) $\in$ Z[x] such that

2 = f(x) g(x) and x = f(x) h(x).

Thus, deg f(x) + deg g(x) = deg 2 = 0 ...(1)

and deg f(x)+deg h(x) = deg x = 1 ...(2)

(I) shows that deg f(x) = 0, i.e., f(x) $\in$ Z, say f(x) = n.

Then (2) shows that deg h(x) = 1. Let h(x) = ax+b with a,b $\in$ Z.

Then x =f(x) h(x) = n(ax+b).

Comparing the coefficients on either side of this equation, we see that na = 1 and nb = 0. Thus, n is a unit in Z, that is, n = If I.

Therefore, 1 $\in$ < f(x) > = < x,2 >. Thus, we can write

I = x (a_0 +a_1x+ ...+$a_r x^r$) + 2(b_0+b_1x+ .... +$b_s x^s$), where a_i,b_j $\in$ Z $\forall$ i = 0, l,.. ...., r and j = 0, 1,...,s.

Now, on comparing the constant term on either side we see that 1 = 2b_0. This can't be true, since 2 is not invertible in Z. So we reach a contradiction.

Thus, < x,2 > is not a principal ideal.

Thus, Z[x] is not a P.I.D.

We will now discuss some properties of divisibility in PIDs. If R is a ring and $a,b \in R$, with $a \neq 0$, then a divides b if there exists $c \in R$ such that $b = ac$.

Definition: Given two elements a and b in a ring. R, we say that $c \in R$ is a common divisor of a and b if $c \mid a$ and $c \mid b$.

An element $d \in R$ is a greatest common divisor (g.c.d, in short) of $a, b \in R$ if

(i) $d \mid a$ and $d \mid b$, and

(ii) for any common divisor c of a and b, $c \mid d$.

For example, in Z a g.c.d of 5 and 15 is 5 , and a g.c.d of 5 and 7 is 1.

We will show you that if the g.c.d of two elements exists, it is unique up to units, i.e., if d and d are two g.c.ds of a and b, then $d=ud'$, for some unit u.

So now let us prove the following result.

Theorem 3: Let R be an integral domain and $a, b \in R$. If a g.c.d of a and b exists, then it is unique up to units.

Proof: So, let d and d′ be two g.c.ds of a and b. Since d is a common divisor and d′ is a g.c.d, we get $d \mid d'$. Similarly, we get $d' \mid d$. Thus, we see that d and d′ are associates in R. Thus, the g.c.d of a and b is unique up to units.

Theorem 3 allows us to say the g.c.d instead of a g.c.d. We denote the g.c.d of a and b by (a,b). (This notation is also used for elements of R × R. But there should be no cause for confusion. The context will clarify what we are using the notation for.

How do we obtain the g.c.d of two elements in practice? How did we do it in Z? We looked at the common factors of the two elements and their product turned out to be the required g.c.d. We will use the same method in the following example.

Example: In Q[x] find the g.c.d of

$p(x) = x^2 + 3x - 10$ and

$q(x) = 6x^2 - 10x - 4$

Solution: By the quadratic formula, we know that the roots of p(x) are 2 and –5, and the roots of q(x) are 2 and –1/3.

Therefore, $p(x) = (x - 2)(x + 5)$ and $q(x) = 2(x - 2)(3x + 1)$.

The g.c.d of p(x) and q(x) is the product of the common factors of p(x) and q(x), which is $(x - 2)$.

Let us consider the g.c.d of elements in a PD.

Theorem 4: Let R be a PID and $a, b \in R$. Then (a, b) exists and is of the form $ax + by$ for some $x,y \in R$.

Proof: Consider the ideal $<a, b>$. Since R is a PID, this ideal must be principal also. Let $d \in R$ such that $<a, b> = <d>$. We will show that the g.c,d of a and b is d.

Since $a \in <d>$, $d \mid a$, Similarly, $d \mid b$.

Now suppose $c \in R$ such that $c \mid a$ and $c \mid b$.

Since d E <a,b>, 3 x, $y \in R$ such that $d = ax+by$.

Since $c \mid a$ and $c \mid b$, $c \mid (ax+by)$, i.e., $c \mid d$.

Thus, we have shown that $d = (a,b)$, and $d= ax+by$ for some $x.y \in R$.

The fact that F[x] is a PID gives-us the following corollary to Theorem 4.

Corollary: Let F be a field. Then any two polynomials f(x) and g(x) in F[x] have a g.c.d which is of the form $a(x)f(x)+b(x)g(x)$ for some $a(x), b(x) \in F[x]$.

For example, (c), $(x–1) = \frac{1}{5}(x^3 – 2x^2 + 6x – 5) + \frac{(-x)}{5}(x^2 – 2x + 1)$.

Now you can use Theorem 4 to prove the following exercise about relatively prime elements in a PID, i.e., pairs of elements whose g.c.d is 1.

Let us now discuss a concept related to that of a prime element of a domain.

Definition: Let R be an integral domain. We say that an element $x \in R$ is irreducible if

(i) x is not a unit, and

(ii) if $x = ab$ with $a,b \in R$, then a is a unit or b is a unit.

Thus, an element is irreducible if it cannot be factored in a non-trivial way, i.e., its only factors are its associates and the units in the ring.

So, for example, the irreducible elements of Z are the prime numbers and their associates. This means that an element in Z is prime iff it is irreducible.

Another domain in which we can find several examples is F[x], where F is a field. Let us look at the irreducible elements in R[x] and C[x], i.e., the irreducible polynomials over R and C. Consider the following important theorem about polynomials in C[x]. You have already come across this in the Linear Algebra course.

Theorem 5 (Fundamental Theorem of Algebra): Any non-constant polynomial in C[x] has a root in C.

Does this tell us anything about the irreducible polynomials over C? Yes. In fact, we can also write it as:

Theorem 5: A polynomial is irreducible in C[x] iff it is linear.

A corollary to this result is:

Theorem 6: Any irreducible polynomial in R[x] has degree 1 or degree 2.

We will not prove these results here but we will use them often when discussing polynomials over R or C. You can use them to solve the following exercise.

Let us now discuss the relationship between prime and irreducible elements in a PID.

Theorem 7: In a PID an element is prime iff it is irreducible.

Proof: Let R be a PID and $x \in R$ be irreducible. Let $x \mid ab$, where $a, b \in R$. Suppose $x \nmid a$.

Then $(x,a) = 1$, since the only factor of x is itself, up to units. Thus, xb, Thus, x is prime.

Task Let R be a domain and $p \in R$ be a prime element. Show that p is irreducible. (Hint: Suppose $p = ab$. Then $p \mid ab$. If $p \mid a$, then show that b must be a unit.)

Now, why do you think we have said that Theorem, 7 is true for a PID only? You can see that one way is true for any domain. Is the other way true for any domain? That is, is every irreducible element of a domain prime? You will get an answer to this question.

Example: Just now we will look at some uses of Theorem 7.

Theorem 7 allows us to give a lot of examples of prime elements of F[x]. For example, any linear polynomial over F is irreducible, and hence prime. In the next unit we will particularly consider irreducibility (and hence primeness) over Q[x].

Now we would like to prove a further analogy between prime elements in a PID and prime numbers, namely, a result analogous. For this we will first show g very interesting property of the ideals of a PID. This property called the ascending chain condition, says that any increasing chain of ideals in a PID must stop after a finite number of steps.

Theorem 8: Let R be a PID and I_1,I_2,.. .. .. be an infinite sequence of ideals of R satisfying.

$1_1 \subseteq 1_2 \subseteq$....

Then 3 m ∈ N such that I, = I_{m+1} = I_{m+2} = ...

Proof: Consider the set I = I, ∪ I_2 ∪ ... = $\bigcup_{m=1}^{\infty} I_n$. We will prove that I is an ideal of R.

Firstly, I ≠ ϕ, since I_1 ≠ ϕ and I_1 ⊆ I.

Secondly, if a,b ∈ I, then a ∈ I, and b ∈ I_s for some r,s ∈ N.

Assume r ≥ s. Then I_s ⊆ I,. Therefore, a, b ∈ I,. Since I, is an ideal of R, a–b ∈ I, ⊆ I. Thus,

a–b ∈ I ∀ a, b ∈ I.

Finally, let x ∈ R and a ∈ I. Then a ∈ I, for some r ∈ N.

∴ xa ∈ I, ⊆ I. Thus, whenever x ∈ R and a ∈ I, xa ∈ I.

Thus, I is an ideal of R. Since R is a PID, I = <a> for some a ∈ R. Since a ∈ I, a ∈ I, for some m ∈ N.

Then I ⊆ I,. But I, ⊆ I. So we. see that I = I_m.

Now, I, ⊆ I_{m+1} ⊆ I_m. Therefore, I, = I_{m+1}

Similarly, I, = I_{m+2} and so on. Thus, Im = I_{m+1} = I_{m+2} = ...

Now, for a moment let us go back, where we discussed prime ideals. Over there we said that an element p ∈ R is prime iff < p > is a prime ideal of R. If R is a PID, we shall use Theorem 7 to make a stronger statement.

Theorem 9: Let R be a PID. An ideal < a > is a maximal ideal of R iff a is a prime element of R.

Proof: If < a > is a maximal ideal of R, then it is a prime ideal of R. Therefore, a is a prime element of R.

Conversely, let a be prime and let I be an ideal of R such that < a > ⊄ I. Since R is a PID, I = < b > for some b ∈ R. We will show that b is a unit in R.

< b > = R, i.e., I = R.

Now, < a > ⊆ < b > ⇒ a = bc for some c ∈ R. Since a is irreducible, either b is an associate of a or b is a unit in R. But if b is an associate of a, then <b> = <a>, a contradiction. Therefore, b is a unit in R. Therefore, I = R.

Thus, <a> is a maximal ideal of R.

What Theorem 9 says is that the prime ideals and maximal Ideals coincide in a PID.

Now, take any integer n. Then we can have n = 0, or n = ± 1, or n has a prime factor. This property of integers is true for the elements of any PID, as you will see now.

Theorem 10: Let R be a PID and a be a non-zero non-invertible element of R. Then there is some prime element p in R such that a.

Proof: If a is prime, take p = a. Otherwise, we can write a =albl, where neither a, nor b_1 is an associate of a. Then < a > $\not\subseteq$ < a_1 >. If a_1 is prime, take p = a_1. Otherwise, we can write a_1 = a_2b_2, where neither a_2 nor b_2 is an associate of a,. Then <a_1> $\not\subseteq$ < a_2 >. Continuing in this way we get an increasing chain

<a> $\not\subseteq$ <a_1> $\not\subseteq$ <a_2> $\not\subseteq$ ...

By Theorem 8, this chain stops with some < a, >. Then a, will be prime, since it doesn't have any non-trivial factors. Take p = a,, and the theorem is proved.

And now we are in a position to prove that any non-zero non-invertible element of a PID can be uniquely written as a finite product of prime elements (i.e., irreducible elements).

Theorem 11: Let Rt be a PID. Let a ∈ R such that a ≠ 0 and a is not a unit. Then a = p_1, p_2....p_r, where p_1,p_2.... p_r, are prime elements of R.

Proof: If a is a prime element, there is nothing to prove. If not, then P_1 | a, for some prime p_1 in R, by Theorem 10. Let a = p_1a_l. If p_1a_1. If a_1 is a prime, we are through. Otherwise P_2 | a, for some prime p_2 in R. Let a_1, = p_2a_2. Then a = $p_1p_2a_2$. If a_2 is a prime, we are through. Otherwise we continue the process. Note that since al is a non-trivial factor of a, <a> $\not\subseteq$ <a_1>. Similarly, <a_1> $\not\subseteq$ < a_2 >. So, as the process continues we get an increasing chain of ideals,

<a> $\not\subseteq$ <a_1> $\not\subseteq$ <a_2> $\not\subseteq$ ...

in the PID R. Just as in the proof of Theorem 10, this chain ends at < a, > for some m ∈ N, and a, is irreducible.

Hence, the process stops after m steps, i.e., we can write a = p_1p_2 ... p_m, where p_i is a prime element of R ∀ i = 1, ... m.

Thus, any non-zero non-invertible element in a PID can be factorised into a product of primes. What is interesting about this factorisation is the following result that you have already proved for Z in Unit 1.

Theorem 12: Let R be a PID and a ≠ 0 be non-invertible in R. Let a = p_1p_2....p_n = q_1q_2....q_m, where p_i and q_j are prime elements of R. Then n = m and each p_i is an associate of some q_j for $1 \le i$ | n, $1 \le j$ | m.

Before going into the proof of this result, we ask you to prove a property of prime elements that you will need in the proof.

Task Use induction on n to prove that if p is a prime element in an integral domain R and if p | a_1a_2 ... a, (where a_1, a_2,.. .., a, ∈ R), then p | a_i, for some i = 1, 2. .... n.

Now let us start the proof of Theorem 12.

Proof: Since $p_1p_2, ...p, = q_1q_2 ... ,.q_m, p_1 \mid q_1q_2. ... q_m,.$

Thus, $p_1 \mid q_j$ for some j = 1. .... ..,m. By changing the order of the q_i, if necessary, we can assume that j = 1, i.e., $p_1 \mid q$. Let $q_1 = p_1u_l$. Since q_1 is irreducible, u_1 must be a unit in R. So p_1 and q_1 are associates. Now we have

$p_1p_2 = P_n (p_1u_1)q_2....q_m.$

Cancelling p_1 from both sides, we get

$p_2p_3...p_n = u_1q_2...,q_m.$

Now, if m > n, we can apply the same process to p_2, p_3, and so on.

Then we will get

$1 = u_1u_2 .... u_n q_{n+1} .... q_m.$

This shows that q_{n+1} is a unit. But this contradicts the fact that q_{n+1} is irreducible.

Thus, $m \leq n$.

Interchanging the roles of the ps and qs and by using a similar argument, we get $n \leq m$.

Thus, n = m.

During the proof we have also shown that each pi is an associate of some q_j, and vice versa.

What Theorem 12 says is that any two prime factorisations of an element in a PID are identical, apart from the order in which the factors appear and apart from replacement of the factors by their associates.

Thus, Theorems 11 and 12 say that every non-zero element in a PID R, which is not a unit, can be expressed uniquely (up to associates) as a product of a finite number of prime elements.

For example, $x^2 – 1 \in R[x]$ can be written as (x-1)(x+1) or (x-1) (x-1) or [2(x-tl)] [2(x-1)] in R[x].

The property that we have shown for a PID in Theorems 11 and 12 is true for several other domains also. Let us discuss such rings now.

Self Assessment

1. An integral domains R a .... if every ideal in R is a principle ideal.

   (a) principle ideal domain (b) unique ideal domain

   (c) special ideal domain (d) range ideal domain

2. g.c.d. represent ....

   (a) greatest common divisor (b) greatest common dividend

   (c) greatest common domain (d) greatest commutated domain

3. Let R be .... and a, b ∈ R, if a g.c.d. of a and b exists, then it is unique up to unit.

   (a) domain and range (b) integral domain

   (c) UID (d) SID

4. PID stands for ....

   (a) principal integral domain (b) pair ideal domain

   (c) principle ideal domain (d) principle ideal divisor

5. Any irreducible polynomials R[x] has degree 1 or define ....

   (a) n   (b) 2

   (c) 4   (d) 5

2.3 Summary

- The definition and examples of a Euclidean domain.
- Z any field and any polynomial ring over a field are Euclidean domains.
- Units, associates, factors, the g.c.d. of two elements, prime elements and irreducible elements in an integral domain.
- The definition and examples of a principal ideal domain (PID).
- Every Euclidean domain is a PID, but the converse is not true.

  Thus, Z, F and F[x] are PIDs, for any field F.
- The g.c.d. of any two elements a and b in a PID R exists and is of the form ax + by for some x, y ∈ R.
- The Fundamental Theorem of Algebra: Any non-constant polynomial over C has all its roots in C.

2.4 Keywords

Euclidean Domain: An integral domain D is called a **Euclidean domain** if for each non-zero element x in D there is assigned a non-negative integer δ(x) such that

(i) (ab) (b) for all non-zero a,b in D, and

(ii) for any non-zero elements a,b in D there exist q,r in D such that a = bq + r, where either r = 0 or δ(r) < δ(b).

UID: Let R be a commutative ring with identity. A non-zero element p of R is said to be **irreducible** if

(i) p is not a unit of R, and

(ii) if p = ab for a,b in R, then either a or b is a unit of R.

Any principal ideal domain is a unique factorization domain.

2.5 Review Questions

1. Show that a subring of a PID need not be PID.
2. Will any quotient ring of a PID be a PID? Why? Remember that a PID must be an integral domain.
3. Let R be an integral domain. Show that

   (a) u is a unit in R iff u | 1.

   (b) for a, b ∈ R, a | b and b | a iff a and b are associates in R.

Notes

4. Find the g.c.d. of

   (a) $\overline{2}$ and $\overline{6}$ in $Z/<8>$, (b) $x^2 + 8x + 15$ and $x^2 + 12x + 35$ in $Z[x]$,

   (c) $x^3 - 2x^2 + 6x - 5$ and $x^2 - 2x + 1$ in $Q[x]$.

5. Let R be a PID and a, b, c $\in$ R such that a (bc. Show that if (a, b) = 1, then a | c.

   (Hint: By Theorem 4, $\exists$ x, y $\in$ R such that ax + b = 1.)

Answers: Self Assessment

1. (a) 2. (a) 3. (b) 4. (c) 5. (b)

2.6 Further Readings

Books

Dan Saracino: Abstract Algebra; A First Course.

Mitchell and Mitchell: An Introduction to Abstract Algebra.

John B. Fraleigh: An Introduction to Abstract Algebra (Relevant Portion).

Online links

www.jmilne.org/math/CourseNotes/

www.math.niu.edu

www.maths.tcd.ie/

archives.math.utk.edu

Unit 3 : Unique Factorization Domains

Notes

CONTENTS

Objectives

After studying this unit, you will be able to:

- Discuss unique factorization domains
- Explain theorems of UID

Introduction

In this unit, we shall look at special kinds of integral domains. These domains were mainly studied with a view to develop number theory. Let us say a few introductory sentences about them.

You saw that the division algorithm holds for F[x], where F is a field. You saw that it holds for Z. Such integral domains are called Euclidean domains.

We shall look at some domains which are algebraically very similar to Z. These are the principal ideal domains, so called because every ideal in them is principal.

Finally, we shall discuss domains in which every non-zero non-invertible element can be uniquely factorised in a particular way. Such domains are very appropriately called unique factorisation domains. While discussing them, we shall introduce you to irreducible elements of a domain.

While going through the unit, you will also see the relationship between Euclidean domains, principal ideal domains and unique factorisation domains.

3.1 Unique Factorisation Domain (UFD)

Here we shall look at some details of a class of domains that include PDs.

Definition: We call an integral domain R a **unique factorisation domain (UFD,** in short) if every non-zero element of R which is not a unit in R can be uniquely expressed as a product of a finite number of irreducible elements of R.

Thus, if R is a UFD and $a \in R$, with $a \neq 0$ and a being non-invertible, then

(i) a can be written as a product of a finite number of irreducible elements, and

(ii) if $a = p_1p_2.. ..p_n = q_1q_2 ..... q_m$, be two factorisations into irreducibles, then $n = m$ and each p_i is an associate of some q_j, where $1 \mid i \mid n$, $1 \leq j \leq m$.

Thus, F[x] is a UFD for any field F.

Also, since any Euclidean domain is a PID, it is also a UFD. You directly proved that Z is a UFD. Why don't you go through that proof and then try and solve the exercises.

Now we give you an example of a domain which is not a UFD (and hence, neither a PID nor a Euclidean domain).

ED implies PID implies UFD

Theorem 1: Every Euclidean domain is a principal ideal domain.

Proof: For any ideal l, take a nonzero element of minimal norm b. Then l must be generated by b, because for any $a \in l$ we have $a = bq + r$ for some q, r with $N(r) < N(b)$, and we must have $r = 0$ otherwise r would be a nonzero element of smaller norm than b, which is a contradiction.

Fact: If R is a UFD then R[x] is also a UFD.

Theorem 2: Every principal ideal domain is a unique factorization domain.

Proof: We show it is impossible to find an infinite sequence $a_1, a_2,...$ such that a_1 is divisible by a_{i+1} but is not an associate. Once done we can iteratively factor an element as we are guaranteed this process terminates.

Suppose such a sequence exists. Then the a_i generate the sequence of distinct principal ideals $(a_1) \subset (a_2) \subset ...$ The union of these ideals is some principal ideal (a). So $a \in (a_n)$ for some n, which implies $(a_i) = (a_n)$ for all $i \geq n$, a contradiction.

Uniqueness: Each irreducible p generates a maximal ideal (p) because if $(p) \subset (a) \subset R$ then $p = ab$ for some $b \in R$ implying that a or b is a unit, thus $(a) = (p)$ or $(a) = R$. Thus $R/(p)$ is a field. Next suppose a member of R has two factorizations

$$p_1 \cdots p_r = q_1 \cdots q_s$$

Consider the ideals (p_i) . (q_i). Relabel so that p_1 generates a minimal ideal amongst these (in other words, (p_1) does not strictly contain another one of the ideals). Now we show $(p_1) = (q_i)$ for some i. Suppose not. Then (p_1) does not contain any q_i, thus q_i is nonzero modulo (p_1) for all i, which is a contradiction because the left-hand side of the above equation is zero modulo (p_1).

Relabel so that $(p_1) = (q_1)$. Then $p_1 = uq_1$ for some unit u. Cancelling gives $up_2 ... p_r = q_2 ... q_z$. The element up_2 is also irreducible, so by induction we have that factorization is unique.

The converse of the above theorem is not always true. Consider the ring $\mathbb{Z}[x]$. The ideal (2, x) is not principal: suppose (2, x) = (a) for some a. Since this ideal contains the even integers, a must be some integer (multiplication never reduces the degree of an element), and in fact it must be (an associate of) 2. But (2) does not contain polynomials with odd coefficients, so (2, x) = (2).

Example: Show that $Z[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in Z\}$ is not a UFD.

Solution: Let us define a function

$f : Z[\sqrt{-5}] \rightarrow N \cup \{0\}$ by $f(a+b\sqrt{-5}) = a^2 + 5b^2$.

This function is the norm function, and is usually denoted by N.

You can check that this function has the property that

$f(\alpha\beta) = f(\alpha)\, f(\beta)\ \ \forall\ , \alpha,\beta \in Z\,[\sqrt{-5}\,]$.

Now, 9 has two factorisations in $Z[\sqrt{-5}]$, namely,

$9 = 3.3 = (2 + \sqrt{-5}\,)\,(2 - \sqrt{-5}\,)$.

You have already shown that the only units of $Z\,[\sqrt{-5}\,]$ are 1 and –1. Thus, no two of 3, $2+\sqrt{-5}$ and $2 - \sqrt{-5}$ are associates of each other.

Also, each of them is irreducible. For suppose any one of them, say $2 + \sqrt{-5}$, is reducible. Then

$2+\sqrt{-5} = \alpha\beta$ for some non-invertible $a,\beta \in Z[\sqrt{-5}\,]$.

Applying the function f we see that

$f\,(2 + \sqrt{-5}\,) = f(\alpha)\, f(\beta)$,

i.e., $9 = f(\alpha)\, f(\beta)$.

Since $f(\alpha), f(\beta) \in N$ and a, β are not units, the only possibilities are $f(\alpha) = 3 = f(\beta)$.

So, if $a = a + b\sqrt{-5}$, then $a^2 + 5b^2 = 3$.

But, if $b \neq 0$, then $a^2 + 5b^2 \geq 5$; and if $b = 0$, then $a^2 = 3$ is not possible in Z. So we reach a contradiction. Therefore, our assumption that $2 + \sqrt{-5}$ is reducible is wrong. That is, $2 + \sqrt{-5}$ is irreducible.

Similarly, we can show that 3 and $2-\sqrt{-5}$ are irreducible. Thus, the factorisation of 9 as a product of irreducible elements is not unique. Therefore, $Z[\sqrt{-5}\,]$ is not a UFD.

From this example you can also see that an irreducible element need not be a prime element.

For example, $2 + \sqrt{-5}$ is irreducible and $2+\sqrt{-5}\ |3.3$, but $2+\sqrt{-5}\ |\ 3$. Thus, $2 + \sqrt{-5}$ is not a prime element.

Now let us discuss some properties of a UFD. The first property says that any two elements of a UFD have a g.c.d. and their g.c.d. is the product of all their common factors. Here we will use the fact that any element a in a UFD R can be written as

$a = p_1^{r_1} p_2^{r_2} \ldots p_n^{r_n}$

where the pis are distinct irreducible elements of R. For example, in Z[x] we have

$x^3 - x^2 - x + 1 = (x - 1)\,(x + l)\,(x - 1\,) = (x - 1)^2\,(x + 1)$.

So, let us prove the following result.

Theorem 3: Any two elements of a UFD have a g.c.d.

Proof: Let R be a UFD and $a.b \in R$.

Let $a = p_1^{r_1} p_2^{r_2} \ldots p_n^{r_n}$ and $b = p_1^{s_1} p_2^{s_2} \ldots p_n^{s_n}$

where $p_1, p_2, ..., p_n$ are distinct irreducible elements of R and r_i and s_i are non-negative integers $\forall$ i = 12, ..., n.

(If some p_i does not occur in the factorisation of a, then the corresponding $r_i = 0$. Similarly, if some p_i is not a factor of b, then the corresponding $s_i = 0$. For example, take 20 and 15 in Z. Then $20 = 2^2 \times 3^0 \times 5$ and $15 = 2^0 \times 3^1 \times 5^1$.)

Now, let t, = min (r_i, s_i) $\forall$ i = 1, 2 ,....,n .

Then $d = p_1^{t_1} p_2^{t_2} ... p_n^{t_n}$ divides a as well as b, since $t_i \leq r_i$ and $t_i \leq s_i$ $\forall$ i = 1, 2, ..., n.

Now, let c | a and c | b. Then every irreducible factor of c must be an irreducible factor of a and of b, because of the unique factorisation property.

Thus, $c = p_1^{m_1} p_2^{m_2} ... p_n^{m_n}$, where $m_i \leq r_i$ and $m_i \leq s_i$ $\forall$ i = 1,2, ...,n . Thus, $m_i \leq t_i$ $\forall$ i = 1,2 ,..., n.

Therefore, c | d.

Hence, d = (a, b).

Over there we found a non-UFD in which an irreducible element need not be a prime element. The following result says that this distinction between irreducible and prime elements can only occur in a domain that is not a UFD.

Theorem 4: Let R be a UFD. An element of R is prime iff it is irreducible.

Proof: We know that every prime in R is irreducible. So let us prove the converse.

Let $a \in R$ be irreducible and let a | bc, where $b, c \in R$.

Consider (a,b). Since a is irreducible, (a,b) = 1 or (a,b) = a.

If (a,b) = a, a | b.

If (a,b) = I, then $d \nmid b$. Let bc = ad, where $d \in R$.

Let $b = p_1^{r_1} p_2^{r_2} ... p_m^{r_m}$, and $c = q_1^{s_1} q_2^{s_2} ... q_n^{s_n}$, be irreducible factorisations of b and c. Since bc = ad and a is irreducible, a must be one of the pis or one of the q_js. Since $a \nmid b$, $a \neq p_i$ for any i. Therefore, $a = q_j$ for some j. That is, a | c.

Thus, if (a,b) = 1 then alc.

So, we have shown that a/ bc $\Rightarrow$ a | b or a | c.

Hence, a is prime.

Theorem 5: Let R be a UFD. Then R[x] is a UFD.

We will not prove this result here, even though it is very useful to mathematicians. But let us apply it. You can use it to solve the following exercises.

Lemma: Let D be a unique factorization domain, and let p be an irreducible element of D. If a,b are in D and p | ab, then p | a or p | b.

Definition: Let D be a unique factorization domain. A non-constant polynomial

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \quad \text{in } D[x]$$

is called **primitive** if there is no irreducible element p in D such that p | a_i for all i.

Lemma: The product of two primitive polynomials is primitive.

Lemma: Let Q be the quotient field of D, and let f(x) be a polynomial in Q[x]. Then f(x) can be written in the form f(x) = (a/b)f*(x), where f*(x) is a primitive element of D[x], a,b are in D, and a and b have no common irreducible divisors. This expression is unique, up to units of D.

Lemma: Let D be a unique factorization domain, let Q be the quotient field of D, and let f(x) be a primitive polynomial in D[x]. Then f(x) is irreducible in D[x] if and only if f(x) is irreducible in Q[x].

Theorem 6: If D is a unique factorization domain, then so is the ring D[x] of polynomials with coefficients in D.

Corollary: For any field F, the ring of polynomials

$$F[x_1, x_2, \dots, x_n]$$

in n indeterminates is a unique factorization domain.

For example, the ring Z [$\sqrt{-5}$] is not a unique factorization domain.

Self Assessment

1. If R is a UFD and a ∈ R, with a ≠ 0 and being a ...., then a can be written as a product of finite number of irreducible elements.

   (a) invertible (b) non-invertible

   (c) external (d) infinite

2. Any euclidean domains is a PID, it is also a ....

   (a) integral domain (b) UFD

   (c) SFD (d) Ideal

3. Let R be a UFD. Then R(x) is a ....

   (a) UFD (b) SFD

   (c) PID (d) Special range domain

4. In a UFD an element is prime iff it is ....

   (a) reducible (b) finite

   (c) irreducible (d) infinite

5. Any two elements in a .... have g.c.d.

   (a) SFD (b) PID

   (c) UFD (d) Domain

3.2 Summary

- In a PID every prime ideal is a maximal ideal.
- The definition and examples of a unique factorisation domain (UFD).
- Every PID is a UFD, but the converse is not true. Thus, Z, F′ and F[x] are UFDs, for any field F.

Notes

- In a UFD (and hence, in a PID) an element is prime iff it is irreducible.
- Any two elements in a UFD have a g.c.d.
- If R is a UFD. then so is K[x].

3.3 Keyword

Unique Factorisation Domain: We call an integral domain R a **unique factorisation domain (UFD,** in short) if every non-zero element of R which is not a unit in R can be uniquely expressed as a product of a finite number of irreducible elements of R.

3.4 Review Questions

1. Directly prove that F[x] is a UFD, for any field F.

   (Hint: Suppose you want to factorise f(x). Then use induction on deg f(x)).
2. Give two different prime factorisations of 10 in Z.
3. Give two different factorisations of 6 as a product of irreducible elements in $Z[\sqrt{-5}]$.
4. Give an example of a UFD which is not a PID.
5. If p is an irreducible element of a UFD R, then is it irreducible in every quotient ring of R?
6. Is the quotient ring of a UFD a UFD? Why?
7. Is a subring of a UFD a UFD? Why?

Answers: Self Assessment

1. (b) 2. (b) 3. (a) 4. (c) 5. (c)

3.5 Further Readings

Books

Dan Saracino: Abstract Algebra; A First Course.

Mitchell and Mitchell: An Introduction to Abstract Algebra.

John B. Fraleigh: An Introduction to Abstract Algebra (Relevant Portion).

Online links

www.jmilne.org/math/CourseNotes/

www.math.niu.edu

www.maths.tcd.ie/

archives.math.utk.edu

Unit 4 : Polynomial Rings

Notes

CONTENTS

Objectives

After studying this unit, you will be able to:

- Identify polynomials over a given ring
- Prove and use the fact that R [x], the set of polynomials over a ring R, is a ring
- Relate certain properties of R[x] to those of R

Introduction

In the earlier units, you must have come across expressions of the form x+1, x^2+2x+1, and so on. These are examples of polynomial. You have also dealt with polynomials in the course of Linear Algebra. In this unit, we will discuss sets whose elements are polynomials of the type a_0 + a, x + ... + $a_n x^n$, where a_0, a_1,......, a,, are elements of a ring R. You will see that this set, denoted by R [x], is a ring also.

You may wonder why we are talking of polynomial rings in a block on domains and fields. The reason for this is that we want to focus on a particular case, namely, R [x], where R is a domain. This will turn out to be a domain also, with a lot of useful properties. In particular, the ring of polynomials over a field satisfies a division algorithm, which is similar to the one satisfied by Z. We will prove this property and use it to show how many roots any polynomial over a field can have.

4.1 Ring of Polynomials

As we have said above, you may already be familiar with expressions of the type 1 + x, 2 + 3x + $4x^2$, x^5-1, and so on. These are examples of polynomials over the ring Z. Do these examples suggest to you what a polynomial over any ring R is ? Let's hope that your definition agrees with the following one.

Definition: A **polynomial** over a ring R in the indeterminate x is an expression of the form

$a_0x^0 + a_1x^1 + a_2x^2 + ... + a_nx^n$,

Notes

where n is a non-negative integer and a_0, a,, ..., $a_n \in$ R.

While discussing polynomials we will observe the **following conventions.** We will

(i) write x^0 as 1, so that we will write a_0 for a_0x^0,

(ii) write x^1 as x,

(iii) write x^m instead of 1 .x^m (i.e., when a_m = l),

(iv) omit terms of the type O.x^m.

Thus, the polynomial 2 + $3x^2 - 1.x^3$ is $2x^0 + 0.x^1 + 3x^2 + (-1)x^3$.

Henceforth, whenever we use the word polynomial, we will mean a polynomial in the indeterminate x. We will also be using the shorter notation $\sum_{i=0}^{n} a_i x^i$ for the polynomial $a_0 + a_1x + \ldots + a_nx^n$.

Let us consider a few mox basic definitions related to a polynomial.

Definition: Let a_n + a, x + ... + a, x^n be a polynomial over a ring R. Each of a_0 ,a_l, . . ., a, is a coefficient of this polynomial. If a, ≠ 0, we call a, the leading coefficient of this polynomial.

If $a_1 = 0 = a_2 = \ldots = a_n$, we get the constant polynomial, a_0. Thus, every element of R is a constant polynomial.

In particular, the constant polynomial 0 is the zero polynomial.

It has no leading coefficient.

Now, there is a natural way of associating a non-negative integer with any non-zero polynomial.

Definition: Let a,, + a, x + . . . + a,, x^n be a polynomial over a ring R, where a, ≠ 0. Then we call the integer n the degree of this polynomial, and we write

$$\deg\left(\sum_{i=0}^{n} a_i x^i\right) = n, \text{of a,,} \neq 0.$$

We define the degree of the zero polynomial to be – ∞. Thus, deg 0 = –∞.

Let us consider some examples.

(i) $3x^2 + 4x + 5$ is a polynomial of degree 2, whose coefficients belong to the ring of integers Z. Its leading coefficient is 3.

(ii) $x^2 + 2x^4 + 6x + 8$ is a polynomial of degree 4, with coefficients in Z and leading coefficient 2. (Note that this polynomial can be rewritten as $8 + 6x + x^2 + 2x^4$.)

(iii) Let R be a ring and r ∈ R, r ≠ 0. Then r is a polynomial of degree 0, with leading coefficient r.

Before giving more examples we would like to set up some notation.

Notation: We will denote the set of all polynomials over a ring R by R[x]. (Please note the use of the square brackets [ ]. Do not use any other kind of brackets because R [x] and R (x) denote different sets.)

$$\text{Thus, R[x]} = \left\{\sum_{i=0}^{n} a_1 x^i \;\middle|\; a_i \in R \;\forall\; i = 0, 1, \ldots n, \text{ where } n \geq 0, n \in Z\right\}.$$

We will also often denote a polynomial $a_0 + a_1 x + \ldots + a_n x^n$ by f(x), p (x), q(x), etc.

Notes

Thus, an example of an element from Z_4 [x] is f(x) = $\bar{2}$ x^2 + $\bar{3}$ x + i.

Here deg f(x) = 2, and the leading coefficient of f(x) is $\bar{2}$.

Now, for ring R, we would like to see if you can define operations on the set R [x] so that it becomes a ring. For this purpose we define the operations of addition and multiplication of polynomials.

Definition: Let f(x) = a,, + a1x + .. + a, x^n and g (x) = b_0 + b, x + .. + $b_m x^m$ be two polynomials in R[X]. Let us assume that m 2 n. Then their sum f(x) + g(x) is given by

f(x) + g(x) = (a,, + b_0) + (a, + b_1)x + .. + (a_n+ b,) x_n + b_{n+1} x^{n+l} .. + $b_m x^m$.

For example, consider the two polynomials p(x), q(x).in Z[x] given by

p(x) = 1 + 2x + $3x^2$, q(x) = 4 + 5x + $7x^3$

Then

p(x) + q(x) = (1+4) + (2+5)x + (3+0) x2 + $7x^3$ = 5 + 7x + $3x^2$ + $7x^3$.

Note that p (x) + q (x) ∈ Z [X] and that

From the definition given above, it seems that deg (f(x)+g(x)) = max (deg f (x), deg g (x)). But this is not always the case. For example, consider p(x) = 1 + x^2 and q (x) = 2 + 3x – x^2 in Z [X].

Then p(x) + q(x) = (1+2) + (0+3)x + (1-1)x^2 = 3 a 3x.

Here deg (p(x) + q (x)) = 1 < max (deg p(x), deg q(x)).

So, what we can say is that

deg (f(x) + g(x)) ≤ max (deg f(x), deg g(x))

∀ f(x), g(x) ∈ R[x].

Now let us define the product of polynomials.

Definition: If f(x) = a,, + a_1x + .. + a, x^n and g(x) = b_0 + b, x + .. + $b_m x^m$ are two polynomials in R [x], we define their product f(x). g(x) by

f(x) . g(x) = c_0 a c_1x +.. + $c_{m+n} x^{m+n}$

where c_1 = $a_1 b_0$, + a_{i-1} b_1 + ... $a_0 b_i$ ∀ i = 0,l ,... ; m + n.

Note that a_i = 0 for i > n and b_i = 0 for i > m,

As an illustration, let us multiply the following polynomials in Z[x] :

p(x) = 1 – x + $2x^3$, q(x) = 2 + 5x + $7x^2$.

Here a, = 1, a, = –1, a_2 = 0, a_3 = 2, b_0 = 2, b, = 5, b_2 = 7.

Thus, p(x) q(x) = $\sum_{i=0}^{5} c_i x^i$, where

c_0 = $a_0 b_0$ = 2,

c_1 = $a_1 b_0$ + $a_0 b_1$ = 3,

c_2 = $a_2 b_0$ + a_1 b_1 + $a_0 b_2$ = 2,

c_3 = $a_3 b_0$ + $a_2 b_1$ + $a_1 b_2$ + $a_0 b_3$ = –3 (since b_3 = 0).

$c_4 = a_4b_0 + a_3b_1 + a_2b_2 + a_1b_3 + a_0b_4 = 10$ (since $a_4 = 0 = b_4$).

$c_5 = a_5b_0 + a_4b_1 + a_3b_2 + a_2b_3 + a_1b_4 + a_0b, = 14$ (since $a_5 = 0 = b_5$).

So $p(x).\ q(x) = 2 + 3x + 2x^2 - 3x^3 + 10x^4 + 14x^5$.

Note that $p(x).\ q(x) \in Z[X]$, and $\deg (p(x)\, q(x)) = 5 = \deg p(x) + \deg q(x)$.

As another example, consider

$$p(x) = \bar{1} + \bar{2}x, q(x) = \bar{2} + \bar{3}x^2 \in Z^6[x].$$

Then, $p(x).\ q(x) = \bar{2} + \bar{4}x + \bar{3}x^2 + \bar{6}x^3 = \bar{2} + \bar{4}x + \bar{3}x^2$.

Here, $\deg (p(x).\ q(x)) = 2 < \deg p(x) + \deg q(x)$ (since $\deg p(x) = 1$, $\deg q(x) = 2$).

In the next section we will show you that

$\deg (f(x)\, g(x)) \le \deg f(x) + \deg g(x)$

By now you must have got used to addition and multiplication of polynomials. We would like to prove that for any ring R, R[x] is a ring with respect to these operations. For this we must note that by definition, + and . are binary operations over R [x].

Now let us prove the following theorem. It is true for any ring, commutative or not,

Theorem 1: If R is a ring, then so is R[x], where x is an indeterminate.

Proof: We need to establish the axioms R1 – R6 of Unit 14 for (R[x], + , .).

(i) ***Addition is Commutative:*** We need to show that

$p(x) + q(x) = q(x) + p(x)$ for any $p(x)$, $q(x) \in R[x]$.

Let $p(x) = a_0 + a_1x + ... + a,x^n$, and

$q(x) = b_0 + b_1x + ... + b_mx^m$ be in R[x].

Then, $p(x) + q(x) = c_0 + c_1x + ... + c_1x^t$,

where $c_i = a_i + b_i$ and $t = \max(m,n)$.

Similarly,

$q(x) + p(x) = d_0 + d_1x + ... + d_sx^s$,

where $d_i = b_i + a_i$, $s = \max(n, m) = t$.

Since addition is commutative in R, $c, = d_i\ \forall\ i \ge 0$.

So we have

$p(x) + q(x) = q(x) + p(x)$.

(ii) ***Addition is Associative:*** Again, by using the associativity of addition in R, we can show that if $p(x), q(x), s(x) \in R[x]$, then

$\{p(x) + q(x)\} + s(x) = p(x) + \{q(x) + s(x)\}$.

(iii) ***Additive Identity:*** The zero polynomial is the additive identity in R [x]. This is because, for any $p(x) = a_0 + a, x + ... + a_nx^n \in R[x]$,

$$\begin{aligned} 0 + p(x) &= (0 + a,) + (0 + a_1)x + ... + (0 + a_n)x^n \\ &= a_0 + a_1x + ... + a_nx^n \\ &= p(x) \end{aligned}$$

(iv) ***Additive Inverse:*** For p (x) = a, + a_1x +... + $a_n x^n \in R[x]$, consider the polynomial –p(x) = –a, –a_1x – ... –$a_n x^n$, – a_i being the additive inverse of ai in R. Then

$$\begin{aligned} p(x) + (-p(x)) &= (a_{,,} - a_{,,}) + (a_1 - a_1)\, x + \ldots + (a_1 - a_n)x^n \\ &= 0 + 0.x + 0.x^2 + \ldots + 0.x^n \\ &= 0. \end{aligned}$$

Therefore, – p(x) is the additive inverse of p(x).

(v) ***Multiplication is Associative:***

Let p(x) =a, +a_1x + ... +$a_n x^n$,

q(x) = $b_0 + b_1x + \ldots + b_m x^m$,

and t (x) = $d_0 + d_1x + \ldots + d_r x^r$, be in R [x]

Then

p(x) . q(x) = $c_0 + c_1\, x + \ldots + c_s x^s{}_{,}$ where s = m + n and

ck = $a_k b_0 + a_{k-1} b_1 + \ldots + a_0 b_k \;\forall\;$ k = 0,l, ...,s .

Therefore,

{p(x) . q(x)} t (x) = $e_0 + e_1\, x + \ldots + e_1 x^t$,

where t = s + r = m+n+r and

$e_k = c_k d_0 + c_{k-1} d_1 + \ldots + c_0 d_k$

$\quad = (a_k b_0 + \ldots + a_0 b_k) d_0 + (a_{k-1}, b_0 + \ldots + a_0 b_{k-1})\, d_1 + \ldots + a_0 b_0 d_k.$

Similarly, we can show that the coefficient of x^k (for any k ≥ 0) in p(x) (q (x) t(x))

is $a_k b_0 d_0 + a_{k-1}, (b_1 d_0 + b_0 d_1) + \ldots + a_0(b_k d_0 + b_{k-1}, d_1 + \ldots + b_0 d_k)$

= e_k, by using the properties of + and . in R.

Hence, {p(x).q(x)} . t(x) = p(x) . {q (x). t (x)}

(vi) ***Multiplication Distributes over Addition:***

Let p(x) = $a_0 + a_1x + \ldots + a_n x_n$,

q(x) = $b_0 + b_l x + \ldots + b_m x^m$

and t(x) = d_0 + d, x + . . . + $d_r\, x^r$ be in R[x],

The coefficient of xk in p (x). (q(x) + t (x)) is

$c_k = a_k\, (b_0 + d_0) + a(b_1 + d_1) + (b_1 + d_1) + \ldots +$ a, $(b_k + d_k)$.

And the coefficient of xk in p (x) q (x) + p (x) t(x) is

$(a_k b_0 + a_{k-1} b_1 + \ldots + a_0 b_k) + (a_k d_0 + a_{k-1} d_1 + \ldots + a_0 d_k),$

$= a_k(b_0 + d_0) + a_{k-1}\, (b + d_1) + \ldots + a_0\, (b_k + d_k) = c_k$

This is true ∀ k ≥ 0.

Hence, p (x) . (q(x) + t (x)] = p (x) . q(x) + p (x). t.(x).

Similarly, we can prove that

{q(x)+t(x).p(x)=q(x).p(x)+t(x).p(x)

Thus, R [x] is a ring.

Notes

Note that the definitions and theorem in this section are true for any ring. We have not restricted ourselves to commutative rings. But, the case that we are really interested in is when R is a domain. In the next section we will progress towards this case.

4 .2 Some Properties of R[x]

In the previous section you must have realised the intimate relationship between the operations on a ring R and the operations on R [x]. The next theorem reinforces this fact.

Theorem 2: Let R be a ring.

(a) If R is commutative, so is R [x].

(b) If R has identity, so does R [x].

Proof: (a) Let p (x) = a_0 + a, x + .. . + a,x^n and

q(x) = $b_0 + b_1x + ... + b_m x_m$ be in R[x].

Then (x) . q(x) = $c_0 + c_1$ x + .. . + $c_s x^s$, where s = m + n and

$c_k = a_k b_0 + a_{k-1} b_1 +. . .+ a_0 b_k$

= $b_k a_0 + b_{k-1} a_1 4$ ... + $b_1 a_{k-1} + b_0 a_k$, since both addition and multiplication are commutative in R.

= coefficient of x^k in q (x) p(x).

Thus, for every i ≥ 0 the coefficients of x^1 in p(x) q(x) and q(x) p(x) are equal

Hence, P(x) q(x) = q(x) p(x).

(b) We know that R has identity 1. We will prove that the constant polynomial 1 is the identity of R [X]. Take any

p(x) = $a_0 + a_1x + ... + a_n x^n \in$ R[x].

Then 1.p(x) = $c_0 + c_1x + ... + c_n x^n$ (since deg 1 = 0),

where $c_k = a_k$, 1 + ak_{-1} . 0 + a_{k-2} . 0 + ... + a_0.0 = a_k

Thus, 1, p(x) = p (x).

Similarly, p(x). 1 = p(x).

This shows that 1 is the identity of R[x]. ,

In the following exercise we ask you to check if the converse of Theorem 2 is true.

Now let us explicitly state a result which will help in showing us that R is a domain iff R [x} is a domain, This result follows just from the definition of multiplication of polynomials.

Theorem 3: Let R be a ring and f (x) and g (x) be two non-zero elements of R [x]. Then deg (f(x) g (x)) ≤ deg f(x) + deg g (x), with equality if R is an integral domain.

Proof: Let f (x) = $a_0 + a_1x + ... + a_n x^n$, $a_n \neq 0$,

and g (x) = $b_0 + b_1x + ... + b_m x^m$, $b_m \neq 0$.

Then deg f (x) = n, deg g (x) = m. We know that

f (x). g (x) = $c_0 + c_1x + ... + c_{m+n} \times {}^{m+n}$,

where $c_k = a_k b_0$ + a, b_1 + ... + $a_0 b_k$,.

Since a_{n+1}, a_{n+2}, ... and b_{m+1}, b_{m+2}. .. . are all zero,

$c_{m+n} = a_n b_m$

Now, if R is without zero divisors, then $a_n b_m \neq 0$, since a, ≠ 0

and b ≠ 0. Thus, in this case,

deg (f(x) g (x)) = deg f(x) + deg g (x).

On the other hand, if R has zero divisors, it can happen that a,b, = 0. In this case,

deg (f (x) g (x)) < m+n = deg f(x) + deg g(x).

Thus, our theorem is proved.

The following result follows immediately from Theorem 3.

Theorem 4: R [x] is an integral domain <=>. R is an integral domain.

Proof: From Theorem 2, we know that R is a commutative ring with identity iff R[x] is a commutative ring with identity. Thus, to prove this theorem we need to prove that. R is without zero divisors iff R [x] is without zero divisors.

So let us first assume that R is without zero divisors.

Let $p(x) = a_0 + a_1 x + ... + a_n x_n$, and $q(x) = b_0 + b_1\ x + ... + b_m x_m$

be in R [x], where a, ≠ 0 and b, ≠ 0.

Then, in Theorem 3 we have seen that deg .(p (x) q (x)) = m + n ≥ 0.

Thus, p (x) q (x) ≠ 0

Thus, R [x] is without zero divisors.

Conversely, let us assume that R [x] is without zero divisors. Let a and b be non-zero elements of R. Then they are non-zero elements of R [x] also. Therefore, ab ≠ 0. Thus, R is without zero divisors. So, we have proved the theorem.

Now, you have seen that many properties of the ring R carry over to R′[x]. Thus, if F is a field, we should expect F[x] to be a field also, But this is not so. F[x] can never be a field.

This is because any polynomial of positive degree in F|x| does not have a multiplicative inverse. Let us see why.

Let f (x) ∈ F [x] and deg f (x) = n > 0. Suppose g (x) ∈ F [x] such that f (x) g (x) = 1. Then

0 = deg 1 = deg (f(x) g (x)) = deg f(x) + deg g (x), since F [x] is a domain.

= n + deg g (x) ≥ n > 0.

We reach a contradiction.

Thus, F [x] cannot be a field.

But there are several very interesting properties of F [x], which are similar to those of Z, the set of integers. In the next section we shall discuss the properties of division in F [x].

Self Assessment

1. A polynomial over a ring R in determinate X is an expression of the form ....

   (a) $a_0x^0 + a_1x^1 + a_2x^2 + ... a_nx^n$ (b) $a^0x_1 + a^2x_2 + a^3x_3 + ... a^nx_n$

   (c) $a^{-1}x + a^{-1}x_2 + a^{-1}x_3 ...... a^{-1}x_n$ (d) $a_0x^{-1} + a_1x^{-1} + a_2x^{-3} ...... a_nx^{-n}$

2. The degree of the zero polynomial to be .... thus degree 0 = ...

   (a) $-\infty, -\infty$ (b) ∞, ∞

   (c) $\infty, -1$ (d) $-1, \infty$

3. $3x^2 + 4x + 5$ is a polynomial of degree ...., whose coefficients belong to the ring of integers Z its leading coefficients is ....

   (a) 4, 5 (b) 2, 3

   (c) 2, 4 (d) 2, 5

4. $x^2 + 2x^4 + 6x + 8$ is a polynomial of degree .... with coefficient 2.

   (a) 4 (b) 5

   (c) 6 (d) 8

5. Let R be a ring and $r \in R$, R .... 0. Then r is polynomial degree of 0 with leading coefficient r.

   (a) = (b) ≠

   (c) ≥ (d) ≤

4.3 Summary

- The definition and examples of polynomials over a ring.
- The ring structure df R[x], where R is a ring.
- R is a commutative ring with identity iff R[x] is a commutative ring with identity.
- R is an integral domain iff R[x] is an integral domain.

4.4 Keywords

Polynomial: A **polynomial** over a ring R in the indeterminate x is an expression of the form

$a_0x^0 + a_1x^1 + a_2x^2 + \ldots + a_nx^n$,

where n is a non-negative integer and a_0, a,, ..., $a_n \in R$.

Coefficient of Polynomial: Let a_n + a, x + ... + a, x^n be a polynomial over a ring R. Each of a_0 ,a_l, . . ., a, is a coefficient of this polynomial. If a, ≠ 0, we call a, the leading coefficient of this polynomial.

4.5 Review Questions

1. Identify the polynomials from the following expressions. Which of these are elements of Z[x]?

   (a) $x^6 + x^5 + x^4 + x^2 + x + 1$ (b) $\frac{2}{x^2} + \frac{1}{x} + x + x^2$

   (c) $\sqrt{3}x^2 + \sqrt{2}x + \sqrt{5}$ (d) $1 + \frac{1}{2}x + \frac{1}{3}x^2 + \frac{1}{4}x^3$

   (e) $x^{1/2} + 2x^{3/2} + 3x^{5/2}$ (f) -5

2. Calculate

   (a) (2 + 3x2 + 4x3) + (5x + x3) in Z[x].   (b) $(\bar{6} + \bar{2}x^2) + (\bar{1} - \bar{2}x + \bar{5}x^3)$ in Z_7 [x].

   (c) $(1 + x)(1 + 2x + x^2)$ in Z[x].   (d) $(\bar{1} + x)(\bar{1} + \bar{2}x + x^2)$ in Z_3[x]

   (e) $(2 + x + x^2)(5x + x^3)$ in Z[x]

3. If R is a ring such that R[x] is commutative and has identity, then

   (a) is R commutative?

   (b) does R have identity?

Answers: Self Assessment

1. (a) 2. (a) 3. (b) 4. (a) 5. (b)

4.6 Further Readings

Books

Dan Saracino: Abstract Algebra; A First Course.

Mitchell and Mitchell: An Introduction to Abstract Algebra.

John B. Fraleigh: An Introduction to Abstract Algebra (Relevant Portion).

Online links

www.jmilne.org/math/CourseNotes/

www.math.niu.edu

www.maths.tcd.ie/

archives.math.utk.edu

Unit 5 : Division of Algorithm

CONTENTS

Objectives

After studying this unit, you will be able to:

- Prove and use the division algorithm for F[X], where F is a field
- Discuss examples related to algorithms

Introduction

In the last unit, you have studied about polynomials rings. In this unit, we will discuss the division of algorithm.

5.1 The Division Algorithm

We have discussed various properties of divisibility in Z. In particular, we proved the division algorithm for integers. We will now do the same for polynomials over a field F.

Theorem 1 (Division Algorithm): Let F be a field. Let f(x) and g(x) be two polynomials in F[x], with $g(x) \neq 0$. Then

(a) there exist two polynomials q(x) and r (x) in F [X] such that

$f(x) = q(x)\, g(x) + r(x)$, where deg $r(x) <$ deg $g(x)$.

(b) the polynomials q (x) and r (x) are unique.

Proof: (a) If deg f (x) < deg g (x), we can choose $q(x) = 0$.

Then $f(x) = 0.\, g(x) + f(x)$, where deg $f(x) <$ deg $g(x)$.

Now, let us assume that deg $f(x) \geq$ deg $g(x)$.

Let $f(x) = a_0 + a_1x + \ldots + a_nx^n$, $a, \neq 0$, and

$g(x) = b_0 + b_1x + \ldots + b_mx^m$, $b_m \neq 0$, with $n \geq m$.

We shall apply the principle of induction on deg f(x), i.e., n.

If n = 0, then rn = 0, since g(x) ≠ 0. Now

f(x) = a,,, g(x) = b,, and hence

f(x) = (a,, b_0^{-1}) b_0 + 0 = q (x) g (x) + r (x), where q(x) = $a_0b_0^{-1}$ and r(x) = 0.

Thus,

f(x) = q(x) g(x) + r (x), where deg r(x) < deg g(x).

So the algorithm is true when n = 0. Let us assume that the algorithm is valid for all polynomials of degree ≤ n – 1 and how to establish that it is true for f(x). Consider the polynomial

$f_1(x) = f(x) – a_nb_m^{-1}x^{n-m}\ g(x)$

= (a,, + a, x +. . .+a_nx^n) – ($a_nb_m^{-1}\ b_0x^{n-m}+a_nb_m^{-1}\ b_1x^{n-m+1}$ +...+ $a_nb_m^{-1}b_mx^n$)

Thus, the coefficient of xn in f, (x) is zero; and hence,

deg f, (x) ≤ n-1.

By the induction hypothesis, there exist q, (x) and r (x) in

F[x] such that f, (x) = q, (x) g(x) + r(x), where deg r(x) < deg g(x).

Substituting the value of f,(x), we get

f(x)-$a_nb_m^{-1}$g(x) = q_1(x) g(x) + r(x),

i.e., f(x) = {$a_nb_m^{-1}\ x^{n-m}$ +q_1(x)} g(x) + (x)

= q(x) g(x)+r(x), where q(x) = $a_nb_m^{-1}\ x^{n-m}$ +q_1(x)

and deg r(x) < deg g(x).

Therefore, the algorithm is true for f(x), and hence for all polynomials in F[x].

(b) Now let us show that q(x) and r(x) are uniquely determined.

If possible, let

$f(x) = q_1(x)\ g(x) + r_1(x)$, where deg $r_1(x)$ < deg g(x).

and

$f(x) =q_2(x)\ g(x)+r_2(x)$, where deg $r_2(x)$ < deg g(x).

Then

$q_1(x)\ g(x)+r_1(x) = q_2(x)\ g(x)+r_2(x)$, so that

$\{q_1(x) – q_2(x)\}\ g(x) = r_2(x) – r_1(x)$ ...(1)

Now if $q_1(x) \neq q_2(x)$, then deg {$q_1(x) – q_2(x)$} ≥ 0, so that

deg [{$q_1(x) – q_2(x)\ g(x)$] ≥ deg g(x).

On the other hand, deg {$r_2(x)$ - $r_1(x)$} < deg g(x), since

deg $r_2(x)$ < deg g(x) and deg $r_1(x)$ < deg g(x).

But this contradicts Equation (1). Hence. Equation (1) will remain valid only if

$q_1(x) – q_2(x) = 0$. And then $r_2(x) – r_1(x) = 0$,

i.e., $q_1(x) = q_2(x)$ and $r_1(x) = r_2(x)$.

Thus, we have proved the uniqueness of q(x) and r(x) in the expression f(x) = q(x) g(x)+r(x). Here q(x) is called the quotient and r(x) is called the remainder obtained on dividing f(x) by g(x).

Now, what happens if **we** take g(x) of Theorem 1 to be a linear polynomial? We get the remainder theorem. Before proving it let us set up some notation.

Notation: Let R be a ring and $f(x) \in R[x]$. Let

$$f(x) = a_0 + a_1x + ... +a_nx^n.$$

Then, for any $r \in R$, we define

that is, f(r) is the value of f(x) obtained by substituting r for x.

Thus, if $f(x) = 1 + x + x^2 \in Z[x]$, then

f(2) = 1 + 2 + 4 = 7 and f(0) = 1 + 0 + 0 = 1.

Let us now prove the remainder theorem, which is a corollary to the division algorithm.

Theorem 2 (Remainder Theorem): Let F be a field. If $f(x) \in P[x]$ and $b \in F$, then there exists a unique polynomial $q(x) \in F[x]$ such that f(x) = (i-b) q(x)+f(b).

Proof: Let g(x) = x-b. Then, applying the division algorithm to f(x) and g(x), we can find unique q(x) and r(x) in F[x], such that

$$\begin{aligned} f(x) &= q(x)g(x) + r(x) \\ &= q(x)\,(x - b) + r(x), \text{ where } \deg r(x) < \deg g(x) = 1. \end{aligned}$$

Since deg r(x) < 1, r (x) is an element of F, say a.

So, f(x) = (x - b)q(x) + a,

Substituting b for x, we get

$$\begin{aligned} f(b) &= (b - b)\, q(b) + a \\ &= 0.q(b) + a= a \end{aligned}$$

Thus, a = f(b).

Therefore, f(x) = (x-b) q(x)+f(b).

Note that deg f(x) = deg(x-b)+deg q(x) = l+deg q(x).

Therefore, deg q(x) = deg f(x)-1.

Let us apply the division algorithm in a few situations now.

Example: Express $x^4 + x^3 + 5x^2 - x$ as

$(x^2 + x + 1)\, q(x) + r(x)$ in Q[x].

Solution: We will apply long division of polynomials to solve this problem.

$$\begin{array}{r} x^2 + x + 1)\sqrt{x^4 + x^3 + 5x^2 - x} \\ \underline{x^4 + x^3 + x^2} \\ 4x^2 - x \\ \underline{4x^2 + 4x + 4} \\ -5x - 4 \end{array}$$

Now, since the degree of the remainder -5x- 4 is less than deg .(x^2+x+1), we stop the process. We get

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

Here the quotient is $x^2 + 4$ and the remainder is – (5x+4).

Now, let us see what happens when the remainder in the expression f = qg + r is zero.

Self Assessment

1. Let F be a field. Let f(x) and g(x) be two polynomials is f[x], with g(x) ≠ 0, then the polynomial q(x) and r(x) an ....

   (a) unique (b) deficient

   (c) finite (d) infinite

2. If deg f(x) < deg g(x) we can chosen q(x) = 0. Then f(x) = 0.g(x) + f(x) where degf(x) .... deg g(x).

   (a) < (b) >

   (c) ≥ (d) ≤

3. $x^4 + x^3 + 5x^2 – x$ is equal to ....

   (a) $(x^2 + x + 1) (q(x) + r(x)$ is Q[x])

   (b) $(x + x^2 + 1) (q^{-1}(x) + r^{-1}(x)$ in Q[x])

   (c) $(x + x^2 + 1)^{-1} (q(x) + r(x)$ in Q[x])

   (d) $q(x)^{-1} + q(x)^2 + (x + x^2 + 1)$ in Q[x]

4. .... theorem said that let F be a field, if F[x] ∈ P[x] and b ∈ F, then there exists a unique polynomial q(x) ∈ F[x] such that f(x) = (i - b) q(x) + F(b)

   (a) remainder theorem (b) division algorithm

   (c) contradiction theorem (d) division matrix

5.2 Summary

- The division algorithm in F[x], where F is a field, which states that if f(x), g(x) ∈ F(x), g(x) ≠ 0, then there exist unique q(x), r(x) ∈ F[x] with f(x) = q(x) g(x)+r(x) and deg r(x) < deg g(x).

  a F is a root of f(x) ∈ F[x] iff (x–a) | f(x).

- A non-zero polynomial of degree n over a field F can have at the most n roots.

5.3 Keywords

Division Algorithm: Let F be a field. Let f(x) and g(x) be two polynomials in F[x], with g(x) ≠ 0.

Remainder Theorem: Let F be a field. If f(x) ∈ P[x] and b ∈ F, then there exists a unique polynomial q(x) ∈ F[x] such that f(x) = (i-b) q(x)+f(b).

5.4 Review Questions

1. Express f as gq + r, where deg r < degg, in each of the following cases.

   (a) $f = x^4 + 1$, $g = x^3$ in Q[x]

   (b) $f = x^3 + \bar{2}x^2 - x + \bar{1}$, $g = x + \bar{1}$ in $Z_3[x]$.

   (c) $f = x^3 - 1$, $g = x - 1$ in R[x].

2. You know that if $p, q \in Z$, $q \neq 0$, then $\frac{p}{q}$ can be written as the sum of an integer and a fraction * with $| m | < | q |$. What is the analogous property for elements of F[x]?

Answers: Self Assessment

1. (a) 2. (a) 3. (a) 4. (a)

5.5 Further Readings

Books

Dan Saracino: Abstract Algebra; A First Course.

Mitchell and Mitchell: An Introduction to Abstract Algebra.

John B. Fraleigh: An Introduction to Abstract Algebra (Relevant Portion).

Online links

www.jmilne.org/math/CourseNotes/

www.math.niu.edu

www.maths.tcd.ie/

archives.math.utk.edu

Unit 6 : Irreducibility and Field Extensions

Notes

CONTENTS

Objectives

After studying this unit, you will be able to:

- Prove and use Eisenstein's criterion for irreducibility in Z[x] and Q[x]
- Obtain field extensions of a field F from F[x]
- Obtain the prime field of any field
- Use the fact that any finite field F has pn elements, where char F = p and dim z_p F = n

Introduction

We have discussed various kinds of integral domains, including unique factorisation domains. Over there you saw that Z[x] and Q[x] are UFDs. Thus, the prime and irreducible elements coincide in these rings. In this unit, we will give you a method for obtaining the prime (or irreducible) elements of Z[x] and Q[x]. This is the Eisenstein criterion, which can also be used for obtaining the irreducible elements of any polynomial ring over a UFD.

After this, we will introduce you to the field extensions and subfields. We will use irreducible polynomials for obtaining field extensions of a field F from F[x]. We will also show you that every field is a field extension of Q or Z, for some prime p. Because of this, we call Q and the Z_ps prime fields. We will discuss these fields briefly.

Finally, we will look at finite fields. These fields were introduced by the young French mathematician Evariste Galois while he was exploring number theory. We will discuss some properties of finite fields which will show us how to classify them.

Before reading this unit ,we suggest that you go through the definitions of irreducibility.

6.1 Irreducibility in Q[x]

We introduced you to irreducible polynomials in F[x], where F is a field. We also stated the Fundamental Theorem of Algebra, which said that a polynomial over C is irreducible iff it is linear. You also learnt that if a polynomial over R is irreducible, it must have degree 1 or degree 2. Thus, any polynomial over R of degree more than 2 is reducible. And, using the quadratic formula, we know which quadratic polynomials over R are irreducible.

Now let us look at polynomials over Q. Again, as for any field F, a linear polynomial over Q is irreducible. Also, by using the quadratic formula we can explicitly obtain the roots of any quadratic polynomial over Q, and hence figure out whether it is irreducible or not. But, can you tell whether $2x^7 + 3x^5 – 6x^4 + 3x^3 + 12$ is irreducible over Q. This criterion was discovered by the nineteenth century mathematician Ferdinand Eisenstein. In this section we will build up the theory for proving this useful criterion.

Let us start with a definition.

Definition: Let $f(x) = a, + a_1x + . .. + a_nx^n \in Z[x]$. We define the content of f[x] to be the g.c.d. of the integers a_0, a_1,,..., a,.

We say that f(x) is primitive if the content of f(x) is 1.

For example, the content of $3x^2 + 6x + 12$ is the g.c.d. of 3, 6 and 12, i.e., 3. Thus, this polynomial is not primitive. But $x^5 + 3x^2 + 4x – 5$ is primitive, since the g.c.d of 1, 0, 0, 3, 4, –5 is 1.

We will now prove that the product of primitive polynomials is a primitive polynomial. This result is well known as Gauss' lemma.

Theorem 1: Let f(x) and g(x) be primitive polynomials. Then so is f(x) g(x).

Proof: Let $f(x) = a_0 + a_1x + ... + a_nx^n \in Z[x]$ and

$g(x) = b_0 + b_1x + ... + b_mx^m \in Z[x]$, where the

g.c.d. of a_0, a_1, ..., a, is 1 and the g.c.d. of b_0, b_1..., b_m is 1. Now

$f(x)\, g(x) = c_0 + c_1x + ... + c_{m+n}x^{m+n}$

where c, $= a_0b_k + a_1b_{k-1} + ... + a_kb_0$.

To prove the result we shall assume that it is false, and then reach a contradiction. So, suppose that f(x) g(x) is not primitive. Then the g.c.d. of c_0, c_1...., c_{m+n} is greater than 1, and hence some prime p must divide it. Thus, $p \mid c_i\ \forall\ i = 0, 1, ..., m+n$. Since f(x) is primitive, p does not divide some a_i. Let r be the least integer such that $p \nmid a_r$. Similarly, let s be the least integer such that $p \nmid b_s$.

Now consider

$$c_{r+s} = a_0b_{r+s} + a_1b_{r+s-1} + ... + a_rb_s + ... + a_{r+s}\, b_0$$

$$= a_rb_s + (a_0b_{r+s} + a_1b_{r+s-1} + ... + a_{r-1}\, b_{s+1} + a_{r+1}b_{s-1} + ... + a_{r+s}\, b_0)$$

By our choice of r and s, $p \mid a_0$, $p \mid a_1$, ..., $p \mid a_{r-1}$, and $p \mid b_0$, $p \mid b_1$, ..., $p \mid b_{s-1}$. Also $p \mid c_{r+s}$,

Therefore, $p \mid c_{r+s} – (a_0b_{r+s} +... + a_{r-1}\, b_{s+1} + a_{r+1}\, b_{s-1} + ... + a_{r+s}\, b_0)$

i.e., $p \mid a_r$ b,.

⇒ p (a, or $p \mid b_s$, since p is a prime.

But $p \nmid a_r$ and $p \nmid b_s$. So we reach a contradiction. Therefore, our supposition is false. That is, our theorem is true.

Let us shift our attention to polynomials over Q now.

Consider any polynomial over Q, say $f(x) = \frac{3}{2}x^3 + \frac{1}{5}x^2 + 3x + \frac{1}{3}$. If we take the l.c.m of the denominators, is., of 2, 5, 1 and 3, i.e., 30 and multiply f(x) by it, what do we get? We get

$30f(x) = 45x^3 + 6x^2 + 90x + 10 \in Z[x]$

Using the same process, we can multiply any $f(x) \in Q[x]$ by a suitable integer d so that df(x), $\in Z[X]$. We will use this fact while relating irreducibility in Q[x] with irreducibility in Z[x].

Theorem 2: If $f(x) \in Z[x]$ is irreducible in Z[x], then it is irreducible in Q[x].

Proof: Let us suppose that f(x) is not irreducible over Q[x]. Then we should reach a contradiction. So let f(x) = g(x) h(x) in Q[x], where neither g(x) nor h(x) is unit, i.e., deg g(x) > 0, deg h(x) > 0. Since $g(x) \in Q[x]$. $\exists\, m \in Z$ such that $mg(x) \in Z[x]$. Similarly, $\exists\, n \in Z$ such that $nh(x) \in Z[x]$. Then,

$mnf(x) = mg(x)\, nh(x)$ ... (1)

Thus, (1) gives us

$mnrf_1(x) = stg_1(x)h_1(x)$ ...(2)

Since $g_1(x)$ and $h_1(x)$ are primitive, Theorem 1 says that $g_1(x)\, h_1(x)$ is primitive. Thus, the content of the right hand side polynomial in (2) is st. But the content of the left hand side polynomial in (2) is mnr. Thus, (2) says that mnr = st.

Hence, using the cancellation law in (2), we get $f,(x) = g,(x)\, h_1(x)$.

Therefore, $f(x) = rf_1(x) = (rg_1(x))\, h_1(x)$ in Z[x], where neither $rp_1(x)$ nor $h_1(x)$ is a unit. This contradicts the fact that f(x) is irreducible in Z[x].

Thus, our supposition is false. Hence, f(x) must be irreducible in Q[x].

What this result says is that to check irreducibility of ii polynomial in Q[x], it is enough to check it in Z[x]. And, for checking it in Z[x] we have the terrific Eisenstein's criterion, that we mentioned at the beginning.

Theorem 3 (Eisenstein's Criterion): Let $f(x) = a_0 + a_1x + ... + a_,,x^n \in Z[x]$. Suppose that for some prime number p;

(i) $P \nmid a_n$,

(ii) $p \mid a_0, p \mid a_1, ..., p \mid a_{n-1}$, and

(iii) $p^2 \nmid a_0$.

Then f(x) is irreducible in Z[x] (and hence Q[x]).

Proof: Suppose f(x) is reducible in Z[x].

Let f(x) = g(x) h(x),

where $g(x) = b_0 + b_1x + ... + b_,,\, x^m$, m > 0 and

$h(x) = c_0 + c_1\, x + ... + c_rx^r$, r > 0.

Then n = deg f = deg g + deg h = m + r, and

$a_k = b_0\, c_k + b_1\, c_{k-1} \ldots + b_k\, c_0 \;\forall\; k = 0, 1 \ldots, n.$

Now $a_0 = b_0c_0$. We know that $p \mid a_0$. Thus, $p \mid b_0c_0$, $\therefore$ $p \mid b_0$ or $p \mid c_0$. Since $p^2 \nmid a_0$, p cannot divide both b_0 and c_0. Let us suppose that $p \mid b_0$ and p k CJ

Now let us look at a,, = b, c,. Since p $\nmid$ a, we see that $p \nmid b_m$ and $p \nmid c_r$. Thus, we see that for some i, $p \nmid b_i$. Let k be the least integer such that $p \nmid b_k$. Note that $0 < k \leq m < n$.

Therefore, $p \mid a_k$.

Since $p \mid a_k$ and $p \mid b_0$, $p \mid b_1$, ..., $p \mid b_{k-1}$, we see that $p(a_k – (b_0c_k + ... + b_{k-1}c_1)$, i. e.,

$p\,(b_kc_0$. But $p \nmid b_k$ and $p \nmid c_0$. So we reach a contradiction.

r Thus, f(x) must be irreducible in Z[x].

Let us illustrate the use of this criterion.

Example: Is $2x^7 + 3x^5 – 6x^4 + 3x^3 + 12$ irreducible in Q[x]?

Solution: By looking at the coefficients we see that the prime number 3 satisfies the conditions given in Eisenstein's criterion. Therefore, the given polynomial is irreducible in Q[x].

Example: Let p be a prime number. Is $Q[x]/<x^3 – p >$ a field?

Solution: You know that for any field F, if f(x) is irreducible in F[x], then <f(x)> is a maximal ideal of F[x].

Now, by Eisenstein's criterion, x^3-p is irreducible since p satisfies the conditions given in Theorem 3. Therefore, $<x^3 – p>$ is a maximal ideal of Q[x].

You also know that if R is a ring, and M is a maximal ideal of R, then R/M is a field.

Thus, $Q[x]\ /<x^3 – p>$ is a field.

Example: Let p be a prime number. Show that

$f(x) = x^{p-1} + x^{p-2} + ... + x + 1$ is irreducible in Z[x], f(x) is called the pth cyclotornic polynomial.

Solution: To start with, we would like you to note that f(x) = g(x) h(x) in Z[x] iff f(x + 1) = g(x + 1) h(x + 1) in Z[x]. Thus, f(x) is irreducible in Z[x] iff f(x + l) is irreducible in Z[x].

Now, $f(x) = \dfrac{x^p - 1}{x - 1}$

$$\therefore \qquad f(x + 1) = \frac{(x+1)^p - 1}{x}$$

$= \dfrac{1}{x}\,(x^p + {}^pC_1\, x^{p-1} + \ldots + {}^pC_{p-1}\, x + 1 – 1)$, (by the binomial theorem)

$= x^{p-1} + px^{p-2} + {}^pC_2x^{p-3} + \ldots + {}^pC_{p-2}\, x + p.$

Now apply Eisenstein's criterion taking p as the prime. We find that f(x+l) is irreducible.

Therefore, f(x) is irreducible.

So far we have used the fact that if f(x) $\in$ Z[x] is irreducible over Z, then it is also irreducible over Q. Do you think we can have a similar relationship between irreducibility in Q[x] and R[xl? To answer this, consider f(x) = x^2 - 2. This is irreducible in Q[x], but f(x) = $(x-\sqrt{2})(x+\sqrt{2})$ in R[x]. Thus, we cannot extend irreducibility over Q to irreducibility over W.

But, we can generalise the fact that irreducibility in Z[x] implies irreducibility in Q[x]. This is not only true for Z and Q; it is true for any UFD R and its field of quotients F. Let us state this relationship explicitly.

Theorem 4: Let R be a UFD with field of quotients F.

(i) If f(x) $\in$ R[x] is an irreducible primitive polynomial, then it is also irreducible in F[x].

(ii) (Eisenstein's Criterion) Let f(x) = $a_0 + a_1x + ... + a, x^n \in$ R[x] and p $\in$ R be a prime element such that p $\nmid$ a,, $p^2 \nmid a_0$ and p | a_i for $0 \leq i < n$. Then f(x) is irreducible in F[x].

The proof of this result is on the same lines as that of Theorems 2 and 3. We will not be doing it here. But if you are interested, you should try and prove the result yourself.

Now, we have already pointed out that if F is a field and f(x) is irreducible over F, then F[x]/<f(x)> is field. How is this field related to F? That is part of what we will discuss in the next section.

6.2 Field Extensions

We shall discuss subfields and field extensions. To start with let us define these terms. By now the definition may be quite obvious to you.

Definition: A non-empty subset S of a field F is called a subfield of F if it is a field with respect to the operations on F. If S$F, then S is galled a proper subfield of F.

A field K is called a field extension of F if F is a subfield of K. Thus, Q is a subfield of R and R is a field extension of Q. Similarly, C is a field extension of Q as well as of R.

Note that a non-empty subset S of a field F is a subfield of F if

(i) S is a subgroup of (F,+), and

(ii) the set of all non-zero elements of S forms a subgroup of the group of non-zero elements of F under multiplication.

Theorem 5: A non-empty subset S of a field F is a subfield of F if and only if

(i) $a \in S, b \in S \Rightarrow a - b \in S$, and

(ii) $a \in S, b \in S, b \neq 0 \Rightarrow ab^{-1} \in S$.

Now, let us look at a particular field extension of a field F. Since F[x] is an integral domain, we can obtain its field of quotients. We denote this field by F(x). Then F is a subfield of F(x). Thus, F(x) is a field extension of F. Its elements are expressions of the form f,(x) where f(x), g(x) $\in$ F[x] and g(x) # 0.

g(x)

There is another way of obtaining a field extension of a field F from F[x]. We can look at quotient rings of F[x] by its maximal ideals. You know that an ideal is maximal in F[x] iff it is generated by an irreducible polynomial over F. So, F[x]/<f(x)> is a field iff f(x) is irreducible over F.

Notes

Now, given any $f(x) \in F[x]$, such that deg $f(x) > 0$, we will show that there is a field monomorphism from F into F[x]/d(x)>. This will show that F[x)/<f(x)> contains an isomorphic copy of F; and hence, we can say, that it contains F. So, let us define $0 : F \to F[x]/d(x)>: \phi(a) = a + <f(x)>$.

Then $\phi\,(a+b) = \phi\,(a) + \phi\,(b)$, and

$\phi(ab) = \phi(a)\,\phi(b)$.

Thus, ϕ is a ring homomorphism.

What is Ker ϕ ?

$$\begin{aligned} \text{Ker} \quad \phi &= \{a \in F]\ a + <f(x)> = <f(x)>\} \\ &= \{a \in F \mid a \in <f(x)>\} \\ &= \{a \in F \mid f(x) \mid a\} \\ &= \{0\}, \text{ since deg } f > 0 \text{ and deg } a \leq 0. \end{aligned}$$

Thus, ϕ is 1-1, and hence an inclusion.

Hence, F is embedded in F[x]/<f(x)>.

Thus, if f(x) is irreducible in F[x], then F[x]/<f(x)> is a field extension of F.

Well, we have looked at field extensions of any field F. Now let us look at certain fields, one of which F will be an extension of.

6.2.1 Prime Fields

Let us consider any field F. Can we say anything about what its subfields look like? Yes, we can say something about one of its subfields. Let us prove this very startling and useful fact.

Theorem 6: Every field contains a subfield isomorphic to Q or to Z_p, for some prime number p.

Proof: Let F be a field. Define a function $f : Z \to F : f(n) = n.1 = 1 + 1 + ... + 1$ (n times).

f is a ring homomorphism and Ker f = pZ, where p is the characteristic of F.

You know that char F = 0 or char F = p, a prime. So let us look at these two cases separately.

Case 1 (char F = 0): In this case f is one-one. $\therefore$ Z = f(Z). Thus, f(Z) is an integral domain contained in the field F. Since F is a field, it will also contain the field of quotients of f(Z). This will be isomorphic' to the field of quotients of Z, i.e., Q. Thus, F has a subfield which is isomorphic to Q.

Case 2 (char F = p, for some prime p):

Since p is a prime number, Z/pZ is a field.

Also, by applying the Fundamental Theorem of Homomorphism to f, we get $Z/pZ \simeq f(Z)$. Thus, f(Z) is isomorphic to Z_p and is contained in F. Hence, F has a subfield isomorphic to Z_p.

Let us Theorem 6 slightly. What it says is that:

Let F be a field.

(i) If char F = 0, then F has a subfield isomorphic to Q.

(ii) If char F = p, then P has a subfield isomorphic to Z.

Because of this property of Q arid Zp (where p is a prime number) we call these fields prime fields.

Thus, the prime fields are Q, Z_2, Z_3, Z_5, etc.

We call the subfield isomorphic to a prime field (obtained in Theorem 6), the prime subfield of the given field.

Let us again reword Theorem 6 in terms of field extensions. What it says is that every field is a Weld extension of a prime field.

Now, suppose a field F is an extension of a field K. Are the prime subfields of K and F isomorphic or not? To answer this let us look at char K and char F. We want to know if char K = char F or not. Since F is a field extension of K, the unity of F and K is the same, namely, 1. Therefore, the least positive integer n such that n.1 = 0 is the same for F as well as K. Thus, char K = char F. Therefore, the prime subfields of K and F are isomorphic.

A very important fact that a field is a prime field iff it has no proper subfields.

Now let us look at certain field extensions of the fields Z_p.

6.2.2 Finite Fields

You have dealt a lot with the finite fields Z_p. Now we will look at field extensions of these fields. You know that any finite field F has characteristic p, for some prime p. And then F is an extension of Z. Suppose P contains q elements. Then q must be a power of p. That is what we will prove now.

Theorem 7: Let F be a finite field having q elements and characteristic p. Then $q = p^n$, some positive integer n.

The proof of this result uses the concepts of a vector space and its basis.

Proof: Since char F = p, F has a prime subfield which is isomorphic to Z_p. We lose nothing if we assume that the prime subfield is Z_p. We first show that F is a vector space over Z_p with finite dimension.

Recall that a set V is a vector space over a field K if:

(i) we can define a binary operation + on V such that (V, +) is an abelian group,

(ii) we can define a 'scalar multiplication. : K × V → V such that $\forall$ a, b $\in$ K and v, w $\in$ V,

$a(a + w) = a.v + a.w$

$(a + b).v = a.v + b.w$

$(ab).\ v = a.\ (b.v)$

$1.v = v.$

Now, we know that (F, +) is an abelian group. We also know that the multiplication in F will satisfy all the conditions that the scalar multiplication should satisfy. Thus, F is a vector space over 2,. Since F is a finite field, it has a finite dimension over Z_p. Let dim Z_p F = n. Then we can find a,. .., a_n, a F such that

$F = Z_pa_1 + Z_pa_2 + .. + Z_pa_n.$

We will show that F has pn elements.

Now, any element of F is of the form

b_1a_1, + b_2a_2 + ... +, b_na_n, where b,, . .., $b_n \in$ Zp.

Now, since o(Zp) = p, b_1 can be any one of its p elements.

Similarly, each of b_2, b_3, ..., b_n has p choices. And, corresponding to each of these choices we get a distinct element of F. Thus, the number of elements in F is p × p × ... × p (n times) = p^n.

The utility of this result is something similar to that of Lagrange's theorem. Using this result we know that, for instance, no field of order 26 exists. But does a field of order 25 exist? Does Theorem 7 answer this question? It only says that a field of order 25 can exist. But it does not say that it does exist. The following exciting result, the proof of which is beyond the scope of this course, gives us the required answer. This result was obtained by the American mathematician E.H. Moore in 1893.

Theorem 8: For any prime number p and $n \in N$, there exists a field with pn elements. Moreover, any two finite fields having the same number of elements are isomorphic.

Self Assessment

1. If $f(x) \in Z(x)$ is irreducible over Q[x]. Then it is .... in Q[x].

   (a) reducible (b) irreducible

   (c) direct (d) finite

2. A non-empty subsets of a field F is called a .... of F it is a field with respect to the operation on F.

   (a) subfield (b) field domain

   (c) range field (d) extension

3. Every field contains a subfield is o morphic to Q or to Z_p for r some .... P.

   (a) prime (b) finite

   (c) infinite (d) external

4. Let F be a finite having of elements and characteristics P, then q = ..., some positive integer n.

   (a) p^{-1} (b) p^n

   (c) xp^n (d) $p.x^p$

5. For any prime number P and $n \in N$, then exists a field with Pn elements. Move over, and two .... fields having the same number of elements are isomorphic.

   (a) infinite (b) finite

   (c) direct (d) extension

6.3 Summary

- Gauss lemma, i.e., the product of primitive polynomials is primitive.
- For any $n \in N$, we can obtain an irreducible polynomial over Q of degree n.
- Definitions and examples of subfields and field extensions.
- Different ways of obtaining field extensions of a field F from F[x].

- Eisenstein's irreducibility criterion for polynomials over Z and Q. This states that if $f(x) = a_0 + a, x + . . . + a_n x^n \in Z[x]$ and there is a prime $p \in Z$ such that

  ❖ $p \mid a_i \ \forall \ i = 0 , 1 . ..., n – 1.$

  ❖ $p \nmid a$, and

  ❖ $p \nmid a_0$,

  then f(x) is irreducible over Z′ (and hence over Q).

- Every field contains a subfield isomorphic to a prime field.

  The prime fields are Q or Zp, for some prime p.

- The number of elements in a finite field F is pn′, where char F = p and dim $z_p F = n$.

- Given a prime number p′and $n \in N$, there exists a field containing p^n elements. Any two finite fields with the same number of elements are isomorphic.

- If F is a finite field with pn elements, then $x^{p^n} - x$ is a product of pn linear polynomials over F.

6.4 Keywords

Eisenstein's Criterion: Let $f(x) = a_0 + a_1 x + ... + a,,x^n \in Z[x]$. Suppose that for some prime number p; (i) $P \nmid a_n$, (ii) $p \mid a_0$, $p \mid a_1$,...$p | a_{n-1}$

Subfield of F: A non-empty subset S of a field F is called a subfield of F if it is a field with respect to the operations on F. If S$F, then S is galled a proper subfield of F.

6.5 Review Questions

1. What are the contents of the following polynomials over Z?

   (a) $1 + x + x^2 + x^3 + x^4$ (b) $7x^4 – 7$

   (c) $5(2x^2 – 1) (x + 2)$

2. Prove that any polynomial $f(x) \in Z[x]$ can be written as dg(x), where d is the content of f(x) and g(x) is a primitive polynomial.

3. For any $n \in N$ and prime number p, show that $x^n – p$ is irreducible over Q[x]. Note that this shows us that we can obtain irreducible polynomials of any degree over Q[x].

4. If $a_0 + a_1 x + ... + a, x^n \in Z[x]$ is irreducible in Q[x], can you always find a prime p that satisfied the conditions (i), (ii) and (iii) of Theorem 3?

5. Which of the following elements of Z[x] are irreducible over Q?

   (a) $x^2 – 12$ (b) $8x^3 + 6x^2 – 9x + 24$

   (c) $5x + 1$

6. Let p be a prime: integer. Let a be a non-zero non-unit square-free integer, i.e., $b^2 \nmid a$ for any $b \in Z$. Show that $Z[x]/<x^p + a>$ is an integral domain.

7. Show that $x^P + \bar{a} \in Z_p[x]$ is not irreducible for any $\bar{a} \in Z$.

Notes

Answers: Self Assessment

1. (b) 2. (a) 3. (a) 4. (b) 5. (b)

6.6 Further Readings

Books

Dan Saracino: Abstract Algebra; A First Course.

Mitchell and Mitchell: An Introduction to Abstract Algebra.

John B. Fraleigh: An Introduction to Abstract Algebra (Relevant Portion).

Online links

www.jmilne.org/math/CourseNotes/

www.math.niu.edu

www.maths.tcd.ie/

archives.math.utk.edu

Unit 7 : Roots of a Polynomial

CONTENTS

Objectives

After studying this unit, you will be able to:

- Define roots of polynomials
- Discuss examples of roots of polynomial

Introduction

You have seen when we can say that an element in a ring divides another element. Let us recall the definition in the context of F[x], where F is a field.

7.1 Roots of Polynomials

Definition: Let f(x) and g(x) be in F[x], where F is a field and $g(x) \neq 0$. We say that g(x) divides f(x)(or g(x) is a factor of f(x), or f(x) is divisible by gi(x)) if there-exists $q(x) \in F[x]$ such that

$f(x) = q(x)\, g(x)$.

We write $g(x) \mid f(x)$ for 'g(x) divides f(x)', and $g(x) \nmid f(x)$ for 'g(x) does not divide f(x)'.

Now, if $f(x) \in F[x]$ and $g(x) \in F[x]$, where $g(x) \neq 0$, when $g(x) \mid f(x)$? We find that $g(x) \mid f(x)$ if $r(x) = 0$.

Definition: Let F be a field and $f(x) \in F[x]$. We say that an element $a \in F$ is a root (or zero) of f(x) if $f(n) = 0$.

For example, 1 is a root of $x^2 - 1 \in R[x]$, since $1^2 - 1 = 0$.

Similarly, –1 is a root of $f(x) = x^3 + x^2 + \frac{1}{2}x + \frac{1}{2} \in Q[x]$, since

$f(-1) = -1 + 1 - \frac{1}{2} + \frac{1}{2} = 0.$

Let F be a field and f (x) $\in$ F[x]. Then a $\in$ P is a root of f(x) if and only if (x–a) | f(x)).

We can generalise this criterion to define a root of multiplicity m of a polynomial in F[x].

Definition: Let F be a field and f(x) $\in$ F[x]. We say that a $\in$ F is a root of multiplicity m (where m is a positive integer) of

$$f(x) \text{ if } (x - a)^m \mid f(x), \text{ but } (x-a)^{m+1} \nmid f(x).$$

For example, 3 is a root of multiplicity 2 of the polynomial $(x-3)^2 (x+2) \in Q[x]$; and (–2) is a root of multiplicity 1 of this polynomial.

Now, is it easy to obtain all the roots of a given polynomial? Any linear polynomial ax+b $\in$ F[x] will have only one root, namely, $-a^{-1}b$. This is because ax+b = 0 iff x = $-a^{-1}b$.

In the case of a quadratic polynomial $ax^2 + bx + c \in F[x]$, you know that its two roots are obtained by applying the quadratic formula

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

For polynomials of higher degree we may be able to obtain some roots by trial and error. For example, consider $f(x) = x^5 - 2x + 1 \in R[x]$. Then, we try out x = 1 and find f(1) = 0. So, we find that 1 is a zero of f(x). But this method doesn't give us all the roots of f(x).

As we have just seen, it is not easy to find all the roots of a given polynomial. But, we can give a definite result about the number of roots of a polynomial.

Theorem 1: Let f(x) be a non-zero polynomial of degree n over a field F:Then f(x) has at most n roots in F.

Proof: If n = 0, then f(x) is a non-zero constant polynomial.

Thus, it has no roots, and hence, it has at most 0 (= n) roots in F.

So, let, us assume that n $\geq$ 1. We will use the principle of induction on n. If deg f(x) = 1,

then

$f(x) = a_0 + a_1x$, where a_0, a, $\in$ F and a, $\neq$ 0.

So f(x) has only one root, namely, $(-a_1^{-1} a_0)$.

Now assume that the theorem is true for all polynomials in F[x] of degree $\leq$ n. We will show that the number of roots of f(x) $\leq$ n.

If f(x) has no root in F, then the number of roots of f(x) in F is 0 S n. So, suppose f(x) has a root a $\in$ F.

Then f(x) = (x – a) g(x), where deg g(x) = n–1.

Hence, by the induction hypothesis g(x) has at most n–1 roots in F, say $a_1,....,a_{n-1}$. Now,

a_i is a root of g(x) $\Rightarrow g(a_i) = 0 \Rightarrow f(a_i) = (a,-a)\, g(a_i) = 0$

$\Rightarrow$ a a_i is a root of f(x) $\forall$ i = 1, ..., n – 1.

Thus, each root of g(x) is a root of f(x).

Now, b $\in$ F is a root of f(x) iff f(b) = 0, i.e., iff (b – a) g(b) = 0, i.e., iff b – a = 0 or g(b) = 0, since F is an integral domain. Thus, b is a root of f(x) iff b = a or b is a root of g(x). So, the only roots of f(x) are a and $a_1, ..., a_{n-1}$. Thus, f(x) has at the most n roots, and so, the theorem is true for n.

Hence, the theorem is true for all n ≥ 1.

Using this result we know that, for example, $x^3–1 \in Q[x]$ can’t have more than 3 roots in Q.

In Theorem 1 we have not spoken about the roots being distinct. But an obvious corollary of Theorem 1 is that

if $f(x) \in F[x]$ is of degree n, then f(x) has st most n distinct roots in F.

We will use this result to prove the following useful theorem.

Theorem 2: Let f(x) and g(x) be two non-zero polynomials of degree n over the field F. If there exist n+l distinct elements a,,.. .,a_{n+1}, in F such that $f(a_i) = g(a_i)$ $\forall$ i = I , ..., n+l, then f(x) = g(x).

Proof: Consider the polynomial h(x) = f(x) = g(x)

Then deg h(x) ≤ n, but it has n + l distinct roots a,, ..., a_{n+1}.

This is impossible, unless h(x) = 0, i.e., f(x) = g(x).

Example: Prove that $x^3 + \bar{5}x \in Z_6[x]$ has more roots than its degree. (Note that Z_6 is not a field.)

Solution: Since the ring is finite, it is easy for us to run through all its elements and check which of them, are roots of

$$f(x) = x^3 + \bar{5}x.$$

So, by substitution we find that

$$f(\bar{0}) = 0 = f(\bar{1}) = f(\bar{2}) = f(\bar{3}) = f(\bar{4}) = f(\bar{5}).$$

In fact, every element of Z_6 is a zero of f(x). Thus, f(x) has 6 zeros, while deg f(x) = 3.

So far, we have been saying that a polynomial of degree n over F has at most n roots in Fa. It can happen that the polynomial has no root in F. For example, consider the polynomial $x^2 + 1 \in R[x]$. You know that it can have 2 roots in R, at the most. But as you know, this has no roots in R (it has two roots, i and –i, in C).

We can find many other examples of such polynomials in R[x]. We call such polynomials irreducible over R. We shall discuss them in detail in the next units.

Now let us end this unit by seeing what we have covered in it.

Definition: Let F be a set on which two binary operations are defined, called addition and multiplication, and denoted by + and ·respectively. Then F is called a **field** with respect to these operations if the following properties hold:

(i) ***Closure:*** For all a,b in F the sum a + b and the product a · b are uniquely defined and belong to F.

(ii) ***Associative Laws:*** For all a,b,c in F,

$$a + (b + c) = (a + b) + c \text{ and } a \cdot (b \cdot c) = (a \cdot b) \cdot c.$$

(iii) ***Commutative Laws:*** For all a,b in F,

$$a + b = b + a \text{ and } a \cdot b = b \cdot a.$$

(iv) ***Distributive Laws:*** For all a, b, c in F,

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \text{ and } (a + b) \cdot c = (a \cdot c) + (b \cdot c).$$

(v) ***Identity Elements:*** The set F contains an additive identity element, denoted by 0, such that for all a in F,

$$a + 0 = a \text{ and } 0 + a = a.$$

The set F also contains a multiplicative identity element, denoted by 1 (and assumed to be different from 0) such that for all a in F,

$$a \cdot 1 = a \text{ and } 1 \cdot a = a.$$

(vi) ***Inverse Elements:*** For each a in F, the equations

$$a + x = 0 \text{ and } x + a = 0$$

have a solution x in F, called an additive inverse of a, and denoted by -a. For each nonzero element a in F, the equations

$$a \cdot x = 1 \text{ and } x \cdot a = 1$$

have a solution x in F, called a multiplicative inverse of a, and denoted by a^{-1}.

Definition: Let F be a field. For $a_m, a_{m-1}, \ldots, a_1, a_0$ in F, an expression of the form

$$a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$$

is called a polynomial over F in the indeterminate x with coefficients $a_m, a_{m-1}, \ldots, a_0$. The set of all polynomials with coefficients in F is denoted by F[x]. If n is the largest nonnegative integer such that $a_n \neq 0$, then we say that the polynomial

$$f(x) = a_n x^n + \cdots + a_0$$

has degree n, written deg(f(x)) = n, and a_n is called the leading coefficient of f(x). If the leading coefficient is 1, then f(x) is said to be monic.

Two polynomials are equal by definition if they have the same degree and all corresponding coefficients are equal. It is important to distinguish between the polynomial f(x) as an element of F[x] and the corresponding polynomial function from F into F defined by substituting elements of F in place of x. If $f(x) = a_m x^m + \cdots + a_0$ and c is an element of F, then $f(c) = a_m c^m + \cdots + a_0$. In fact, if F is a finite field, it is possible to have two different polynomials that define the same polynomial function. For example, let F be the field Z_5 and consider the polynomials $x^5 - 2x + 1$ and $4x + 1$. For any c in Z_5, by Fermat's theorem we have $c^5 \equiv c \pmod 5$, and so

$$c^5 - 2c + 1 \equiv - c + 1 \equiv 4c + 1 \pmod 5,$$

which shows that $x^5 - 2x + 1$ and $4x + 1$ are identical, as functions.

For the polynomials

$$f(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$$

and

$$g(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0,$$

the sum of f(x) and g(x) is defined by just adding corresponding coefficients. The product f(x)g(x) is defined to be

$$a_m b_n x^{n+m} + \cdots + (a_2 b_0 + a_1 b_1 + a_0 b_2)x^2 + (a_1 b_0 + a_0 b_1)x + a_0 b_0.$$

The coefficient c_k of x^k in f(x)g(x) can be described by the formula

$$c_k = \sum\nolimits_{i=0a_i}^{k} b_{k-i}.$$

This definition of the product is consistent with what we would expect to obtain using a naive approach: Expand the product using the distributive law repeatedly (this amounts to multiplying each term be every other) and then collect similar terms.

Proposition: If f(x) and g(x) are non-zero polynomials in F[x], then f(x)g(x) is non-zero and deg(f(x)g(x)) = deg(f(x)) + deg(g(x)).

Corollary: If f(x),g(x),h(x) are polynomials in F[x], and f(x) is not the zero polynomial, then f(x)g(x) = f(x)h(x) implies g(x) = h(x).

Definition: Let f(x),g(x) be polynomials in F[x]. If f(x) = q(x)g(x) for some q(x) in F[x], then we say that g(x) is a **factor** or **divisor** of f(x), and we write g(x) | f(x). The set of all polynomials divisible by g(x) will be denoted by < g(x) >.

Lemma: For any element c in F, and any positive integer k,

$$(x - c) \mid (x^k - c^k).$$

Theorem 3: Let f(x) be a non-zero polynomial in F[x], and let c be an element of F. Then there exists a polynomial q(x) in F[x] such that

$$f(x) = q(x)(x - c) + f(c).$$

Moreover, if $f(x) = q_1(x)(x - c) + k$, where $q_1(x)$ is in F[x] and k is in F, then $q_1(x) = q(x)$ and k = f(c).

Definition: Let $f(x) = a_m x^m + \cdot \cdot + a_0$ belong to F[x]. An element c in F is called a **root** of the polynomial f(x) if f(c) = 0, that is, if c is a solution of the polynomial equation f(x) = 0 .

Corollary: Let f(x) be a non-zero polynomial in F[x], and let c be an element of F. Then c is a root of f(x) if and only if x-c is a factor of f(x). That is,

f(c) = 0 if and only if (x-c) | f(x).

Corollary: A polynomial of degree n with coefficients in the field F has at most n distinct roots in F.

Self Assessment

1. Let F be a field and f(x) ∈ F[x] then we say that an element a ∈ F is a root of f(x) of f(n) = ...

(a)	1	(b)	2
(c)	0	(d)	2^{-1}

2. 1 is a root of $x^2 - 1 \in R[x]$, since $1^2 - 1$ = ...

(a)	2	(b)	1
(c)	0	(d)	–1

3. .... is a root of $f(x) = x^3 + x^2 + \frac{1}{2}x + \frac{1}{2} \in Q[x]$

(a)	1	(b)	2
(c)	–1	(d)	–2

4. If n = 0 then f(x) is a non-zero .... polynomial

(a)	constant	(b)	degree
(c)	range	(d)	power

5. x3 + $\bar{5}$x ∈ z_6[x] has .... roots than its degree.

(a) 2 (b) 3

(c) 1 (d) more

7.2 Summary

- If f(x) and g(x) are non-zero polynomials in F[x], then f(x)g(x) is non-zero and deg(f(x)g(x)) = deg(f(x)) + deg(g(x)).
- If f(x),g(x),h(x) are polynomials in F[x], and f(x) is not the zero polynomial, then f(x)g(x) = f(x)h(x) implies g(x) = h(x).
- Let f(x),g(x) be polynomials in F[x]. If f(x) = q(x)g(x) for some q(x) in F[x], then we say that g(x) is a **factor** or **divisor** of f(x), and we write g(x) | f(x). The set of all polynomials divisible by g(x) will be denoted by < g(x) >.
- For any element c in F, and any positive integer k,

  $$(x - c) \mid (x^k - c^k).$$

- Let f(x) be a non-zero polynomial in F[x], and let c be an element of F. Then there exists a polynomial q(x) in F[x] such that

  $$f(x) = q(x)(x - c) + f(c).$$

  Moreover, if $f(x) = q_1(x)(x - c) + k$, where $q_1(x)$ is in F[x] and k is in F, then $q_1(x) = q(x)$ and k = f(c).
- Let $f(x) = a_m x^m + \cdot\cdot + a_0$ belong to F[x]. An element c in F is called a **root** of the polynomial f(x) if f(c) = 0, that is, if c is a solution of the polynomial equation f(x) = 0 .
- Let f(x) be a non-zero polynomial in F[x], and let c be an element of F. Then c is a root of f(x) if and only if x-c is a factor of f(x). That is,

  $$f(c) = 0 \quad \text{if and only if} \quad (x-c) \mid f(x).$$

- A polynomial of degree n with coefficients in the field F has at most n distinct roots in F.

7.3 Keywords

Field: Let F be a set on which two binary operations are defined, called addition and multiplication, and denoted by + and · respectively. Then F is called a **field** with respect to these operations.

Identity Elements: The set F contains an additive identity element, denoted by 0, such that for all a in F,

$$a + 0 = a \text{ and } 0 + a = a.$$

Inverse Elements: For each a in F, the equations

$$a + x = 0 \text{ and } x + a = 0$$

have a solution x in F, called an additive inverse of a, and denoted by -a. For each non-zero element a in F, the equations

$$a \cdot x = 1 \text{ and } x \cdot a = 1$$

7.4 Review Questions

Notes

1. Let F be a field and $f(x) \in F[x]$ with $\deg f(x) \geq 1$. Let $a \in F$. Show that f(x) is divisible by x – a iff f(a) = 0.

2. Find the roots of the following polynomials, along with their multiplicity.

   (a) $f(x) = \frac{1}{2}x^2 - \frac{5}{2}x + 3 \in Q[x]$ (b) $f(x) = x^2 + x + \bar{1} \in Z_3[x]$

   (c) $f(x) = x^4 + \bar{2}x^3 - \bar{2}x - \bar{1} \in Z_5[x]$

3. Let F be a field and $a \in F$. Define a function

   $\phi : F[x] \rightarrow F : f(f(x)) = f(x)$

   This function is the evaluation at a.

   Show that

   (a) f is an onto ring homomorphism.

   (b) f (b) = b $\forall$ b $\in$ F.

   (c) Ker f = <x – a>

   So, what does the Fundamental Theorem of Homomorphism say in this case?

4. Let p be a prime number. Consider $x^{p-1} - \bar{1} \in Z_p[x]$. Use the fact that Zp is a group of order p to show that every non-zero element of Zp is a root of $x^{p-1} - \bar{1}$. Thus, show that $x^{p-1} - \bar{1}$ = $(x - \bar{1})(x - \bar{2})...(x - \overline{p-1})$.

5. The polynomial $x^4 + \bar{4}$ can be factored into linear factors in $Z_5[x]$. Find this factorisation.

Answers: Self Assessment

1. (c) 2. (c) 3. (c) 4. (a) 5. (d)

7.5 Further Readings

Books

Dan Saracino: Abstract Algebra; A First Course.

Mitchell and Mitchell: An Introduction to Abstract Algebra.

John B. Fraleigh: An Introduction to Abstract Algebra (Relevant Portion).

Online links

www.jmilne.org/math/CourseNotes/

www.math.niu.edu

www.maths.tcd.ie/

archives.math.utk.edu

Richa Nandra, Lovely Professional University

Unit 8 : Splitting Fields, Existence and Uniqueness

CONTENTS

Objectives

After studying this unit, you will be able to:

- Discuss splitting field
- Describe extension field and theorem related to extension

Introduction

Beginning with a field K, and a polynomial f(x) ∈ K, we need to construct the smallest possible extension field F of K that contains all of the roots of f(x). This will be called a splitting field for f(x) over K. The word "the" is justified by proving that any two splitting fields are isomorphic.

Let F be an extension field of K and let u ∈ F. If there exists a non-zero polynomial f(x) ∈ K[x] such that f(u) = 0, then u is said to be algebraic over K. If not, then u is said to be transcendental over K.

8.1 Extension Field

If F is an extension field of K, and u ∈ F is algebraic over K, then there exists a unique monic irreducible polynomial p(x) ∈ K[x] such that p(u) = 0. It is the monic polynomial of minimal degree that has u as a root, and if f(x) is any polynomial in K[x] with f(u) = 0, then p(x) | f(x).

Alternate proof: The proof in the text uses some elementary ring theory. Then decided to include a proof that depends only on basic facts about polynomials.

Assume that u ∈ F is algebraic over K, and let I be the set of all polynomials f(x) ∈ K[x] such that f(u) = 0. The division algorithm for polynomials can be used to show that if p(x) is a non-zero monic polynomial in I of minimal degree, then p(x) is a generator for I, and thus p(x) | f(x) whenever f(u) = 0.

Furthermore, p(x) must be an irreducible polynomial, since if p(x) = g(x)h(x) for g(x); h(x) ∈ K[x], then g(u)h(u) = p(u) = 0, and so either g(u) = 0 or h(u) = 0 since F is a field. From the choice of p(x) as a polynomial of minimal degree that has u as a root, we see that either g(x) or h(x) has the same degree as p(x), and so p(x) must be irreducible.

In the above proof, the monic polynomial p(x) of minimal degree in K[x] such that p(u) = 0 is called the minimal polynomial of u over K, and its degree is called the degree of u over K.

Let F be an extension field of K, and let $u_1, u_2, ..., u_n \in F$. The smallest subfield of F that contains K and $u_1, u_2,..., u_n$ will be denoted by $K(u_1, u_2,..., u_n)$. It is called the extension field of K generated by u1, $u_2,...., u_n$. If F = K(u) for a single element u ∈ F, then F is said to be a simple extension of K.

Let F be an extension field of K, and let u ∈ F. Since K(u) is a field, it must contain all elements of the form

$$\frac{a_0 + a_1u + a_2u^2 + ... + a_mu^m}{b_0 + b_1u + b_2u^2 + ... + b_nu^n},$$

where $a_i, b_j \in K$ for i = 1,..., m and j = 1,... n. In fact, this set describes K(u), and if u is transcendental over K, this description cannot be simplified. On the other hand, if u is algebraic over K, then the denominator in the above expression is unnecessary, and the degree of the numerator can be assumed to be less than the degree of the minimal polynomial of u over K.

If F is an extension field of K, then the multiplication of F defines a scalar multiplication, considering the elements of K as scalars and the elements of F as vectors. This gives F the structure of a vector space over K, and allows us to make use of the concept of the dimension of a vector space. The next result describes the structure of the extension field obtained by adjoining an algebraic element.

Definition: Let F be an extension field of K and let u ∈ F be an element algebraic over K.

(a) K(u) ≃ K[x]= hp(x)i, where p(x) is the minimal polynomial of u over K.

(b) If the minimal polynomial of u over K has degree n, then K(u) is an n-dimensional vector space over K.

Alternate proof: The standard proof uses the ring homomorphism θ : K[x] → F defined by evaluation at u. Then the image of θ is K(u), and the kernel is the ideal of K[x] generated by the minimal polynomial p(x) of u over K. Since p(x) is irreducible, ker() is a prime ideal, and so K[x] = ker() is a field because every nonzero prime ideal of a principal ideal domain is maximal. Thus K(u) is a field since K(u) 245= K[x]= ker().

The usual proof involves some ring theory, but the actual ideas of the proof are much simpler. To give an elementary proof, define ϕ : K[x]= {p(x)} → K(u) by ϕ ([f(x)]) = f(u), for all congruence classes [f(x)] of polynomials (modulo p(x)). This mapping makes sense because K(u) contains u, together with all of the elements of K, and so it must contain any expression of the form $a_0 + a_1u + ... + a_mu^m$, where $a_i \in K$, for each subscript i. The function ϕ is well-defined, since it is also independent of the choice of a representative of [f(x)]. In fact, if g(x) ∈ K[x] and f(x) is equivalent to g(x), then f(x) – g(x) = q(x)p(x) for some q(x) ∈ K[x], and so f(u) – g(u) = q(u)p(u) = 0, showing that ϕ ([f(x)]) = ϕ ([g(x)]).

Since the function ϕ simply substitutes u into the polynomial f(x), and it is not difficult to show that it preserves addition and multiplication. It follows from the definition of p(x) that ϕ is one-to-one. Suppose that f(x) represents a nonzero congruence class in K[x]= {p(x)}. Then $p(x) \nmid f(x)$, and so f(x) is relatively prime to p(x) since it is irreducible. Therefore, there exist polynomials a(x) and b(x) in K[x] such that a(x)f(x) + b(x)p(x) = 1. It follows that [a(x)][f(x)] = [1] for the corresponding equivalence classes, and this shows that K[x] /{p(x)} is a field. Thus the image E of ϕ in F must be subfield of F. On the one hand, E contains u and K, and on the other hand, we have already shown that E must contain any expression of the form $a_0 + a_1u + ... + a_mu^m$, where $a_i \in K$. It follows that E = K(u), and we have the desired isomorphism.

(b) It follows from the description of K(u) in part (a) that if p(x) has degree n, then the set $B = \{1, u, u^2,..., u^{n-1}\}$ is a basis for K(u) over K.

Let F be an extension field of K. The dimension of F as a vector space over K is called the degree of F over K, denoted by [F : K]. If the dimension of F over K is finite, then F is said to be a finite extension of K. Let F be an extension field of K and let $u \in F$. The following conditions are equivalent: (1) u is algebraic over K; (2) K(u) is a finite extension of K; (3) u belongs to a finite extension of K.

Never underestimate the power of counting: the next result is crucial. If we have a tower of extensions $K \subseteq E \subseteq F$, where E is finite over K and F is finite over E, then F is finite over K, and [F : K] = [F : E][E : K]. This has a useful corollary, which states that the degree of any element of F is a divisor of [F : K].

Let K be a field and let $f(x) = a_0 + a_1x + ... + a_nx^n$ be a polynomial in K[x] of degree n > 0. An extension field F of K is called a splitting field for f(x) over K if there exist elements $r_1, r_2,..., r_n \in F$ such that

(i) $f(x) = a_n(x - r_1)(x - r_2) ... (x - rn)$ and

(ii) $F = K(r_1, r_2,..., r_n)$.

In this situation we usually say that f(x) splits over the field F. The elements $r_1, r_2,..., r_n$ are roots of f(x), and so F is obtained by adjoining to K a complete set of roots of f(x). An induction argument (on the degree of f(x)) can be given to show that splitting fields always exist. Theorem states that if $f(x) \in K[x]$ is a polynomial of degree n > 0, then there exists a splitting field F for f(x) over K, with $[F : K] \leq n!$.

The uniqueness of splitting fields follows from two lemmas. Let $\phi : K \to L$ be an isomorphism of fields. Let F be an extension field of K such that F = K(u) for an algebraic element $u \in F$. Let p(x) be the minimal polynomial of u over K. If v is any root of the image q(x) of p(x) under ϕ, and E = L(v), then there is a unique way to extend ϕ to an isomorphism $: F \to E$ such that $\theta(u) = v$ and $\theta(a) = \phi(a)$ for all $a \in K$. The required isomorphism $\theta : K(u) \to L(v)$ must have the form

$$\theta(a_0 + a_1u + ... + a_{n-1}u^{n-1}) = \phi(a_0) + \phi(a_1)v + ... + \phi(a_{n-1})v^{n-1}$$

The second lemma is stated as follows. Let F be a splitting field for the polynomial $f(x) \in K[x]$. If $\phi : K \to L$ is a field isomorphism that maps f(x) to $g(x) \in L[x]$ and E is a splitting field for g(x) over L, then there exists an isomorphism $\theta : F \to E$ such that $\theta(a) = \phi(a)$ for all $a \in K$. The proof uses induction on the degree of f(x), together with the previous lemma.

Theorem states that the splitting field over the field K of a polynomial $f(x) \in K[x]$ is unique up to isomorphism. Among other things, this result has important consequences for finite fields.

Self Assessment

1. If F is an extension field k and $u \in F$ is algebraic over K, then their exists a ....

   (a) different (b) finite

   (c) infinite (d) unique

2. The monic polynomial P(x) of minimal degree in K[x] such that P(u) = 0 is called is .... of r over K and its degree is called the degree of u over K.

   (a) maximal polynomial (b) minimal polynomial

   (c) finite polynomial (d) infinite polynomial

3. The dimension of F as a vector space K is called the .... of F over K, denoted by [f : k]

   (a) range (b) domain

   (c) degree (d) field

4. The splitting field over the field K of a polynomial f(x) ∈ K[x] is unique up to ....

   (a) homomorphism (b) isomorphism

   (c) automorphism (d) finite extension

8.2 Summary

If F is an extension field of K, and u ∈ F is algebraic over K, then there exists a unique monic irreducible polynomial p(x) ∈ K[x] such that p(u) = 0. It is the monic polynomial of minimal degree that has u as a root, and if f(x) is any polynomial in K[x] with f(u) = 0, then p(x) | f(x).

Alternate Proof: The proof in the text uses some elementary ring theory. I've decided to include a proof that depends only on basic facts about polynomials.

Let F be an extension field of K, and let $u_1, u_2, ..., u_n \in F$. The smallest subfield of F that contains K and $u_1, u_2,..., u_n$ will be denoted by $K(u_1, u_2,..., u_n)$. It is called the extension field of K generated by $u_1, u_2,...., u_n$. If F = K(u) for a single element u ∈ F, then F is said to be a simple extension of K.

Let F be an extension field of K, and let u ∈ F. Since K(u) is a field, it must contain all elements of the form

$$\frac{a_0 + a_1u + a_2u^2 + ... + a_mu^m}{b_0 + b_1u + b_2u^2 + ... + b_nu^n},$$

where $a_i, b_j \in K$ for i = 1,..., m and j = 1,... n. In fact, this set describes K(u), and if u is transcendental over K, this description cannot be simplified. On the other hand, if u is algebraic over K, then the denominator in the above expression is unnecessary, and the degree of the numerator can be assumed to be less than the degree of the minimal polynomial of u over K.

If F is an extension field of K, then the multiplication of F defines a scalar multiplication, considering the elements of K as scalars and the elements of F as vectors. This gives F the structure of a vector space over K, and allows us to make use of the concept of the dimension of a vector space. The next result describes the structure of the extension field obtained by adjoining an algebraic element.

The uniqueness of splitting fields follows from two lemmas. Let $\phi : K \to L$ be an isomorphism of fields. Let F be an extension field of K such that F = K(u) for an algebraic element u ∈ F. Let p(x) be the minimal polynomial of u over K. If v is any root of the image q(x) of p(x) under ϕ, and E = L(v), then there is a unique way to extend ϕ to an isomorphism $: F \to E$ such that $\theta(u) = v$ and $\theta(a) = \phi(a)$ for all a ∈ K. The required isomorphism $\theta : K(u) \to L(v)$ must have the form

$$\theta(a_0 + a_1u + ... + a_{n-1}u^{n-1}) = \phi(a_0) + \phi(a_1)v + ... + \phi(a_{n-1})v^{n-1}$$

The second lemma is stated as follows. Let F be a splitting field for the polynomial f(x) ∈ K[x]. If $\phi : K \to L$ is a field isomorphism that maps f(x) to g(x) ∈ L[x] and E is a splitting field for g(x) over L, then there exists an isomorphism $\theta : F \to E$ such that $\theta(a) = \phi(a)$ for all a ∈ K. The proof uses induction on the degree of f(x), together with the previous lemma.

The splitting field over the field K of a polynomial f(x) ∈ K[x] is unique up to isomorphism.

8.3 Keywords

Splitting Field: Beginning with a field K, and a polynomial f(x) ∈ K, we need to construct the smallest possible extension field F of K that contains all of the roots of f(x). This will be called a splitting field for f(x) over K.

Extension Field: Let F be an extension field of K and let u ∈ F. If there exists a nonzero polynomial f(x) ∈ K[x] such that f(u) = 0, then u is said to be algebraic over K. If not, then u is said to be transcendental over K.

In the above proof, the monic polynomial p(x) of minimal degree in K[x] such that p(u) = 0 is called the minimal polynomial of u over K, and its degree is called the degree of u over K.

8.4 Review Questions

1. Find the splitting field over Q for the polynomial $x^4 + 4$.
2. Let p be a prime number. Find the splitting fields for $x^p - 1$ over Q and over R.
3. Find the splitting field for $x^3 + x + 1$ over Z_2.
4. Find the degree of the splitting field over Z_2 for the polynomial $(x^3 + x + 1)(x^2 + x + 1)$.
5. Let F be an extension field of K. Show that the set of all elements of F that are algebraic over K is a subfield of F.
6. Let F be a field generated over the field K by u and v of relatively prime degrees m and n, respectively, over K. Prove that [F : K] = mn.
7. Let $F \supseteq E \supseteq K$ be extension fields. Show that if F is algebraic over E and E is algebraic over K, then F is algebraic over K.
8. Let $F \supset K$ be an extension field, with u ∈ F. Show that if [K(u) : K] is an odd number, then $K(u^2) = K(u)$.
9. Find the degree [F : Q], where F is the splitting field of the polynomial $x^3 - 11$ over the field Q of rational numbers.
10. Determine the splitting field over Q for $x^4 + 2$.
11. Determine the splitting field over Q for $x^4 + x^2 + 1$.
12. Factor $x^6 - 1$ over Z_7; factor $x^5 - 1$ over Z_{11}.

Answers: Self Assessment

1. (d) 2. (b) 3. (c) 4. (b)

8.5 Further Readings

Books

Dan Saracino: Abstract Algebra; A First Course.

Mitchell and Mitchell: An Introduction to Abstract Algebra.

John B. Fraleigh: An Introduction to Abstract Algebra (Relevant Portion).

Online links

www.jmilne.org/math/CourseNotes/

www.math.niu.edu

www.maths.tcd.ie/

archives.math.utk.edu

Unit 9 : Separable Extensions

CONTENTS

Objectives

After studying this unit, you will be able to:

- Define separability
- Discuss examples related to separable extension

Introduction

In the last unit, you have studied about the splitting field and extension field. This unit will provide you information related to separable extension.

9.1 Separability

Separability of a finite field extension L/K can be described in several different ways. The original definition is that every element of L is separable over K (that is, has a separable minimal polynomial in K[X]). We will give here three descriptions of separability for a finite extension and use each of them to prove two theorems about separable extensions.

Theorem 1: Let L/K be a finite extension. Then L/K is separable if and only if the trace function $\mathrm{Tr}_{L/K} : L \to K$ is not identically 0.

The trace function is discussed in Appendix A.

Theorem 2: Let L/K be a finite extension. Then L/K is separable if and only if the ring $\overline{K} \otimes_K L$ has no non-zero nilpotent elements. When L/K is separable, the ring $\overline{K} \otimes_K L$ is isomorphic to $\overline{K}^{[L:K]}$.

Example: Consider the extension Q($\sqrt{2}$)=Q. Since Q($\sqrt{2}$) $\simeq$ Q[X]/(X^2 – 2), tensoring with $\overline{Q}$ gives $\overline{Q} \otimes_Q Q\left(\sqrt{2}\right) ; \overline{Q}[X]/(X^2-2) = Q[X]/((X+\sqrt{2})(X-\sqrt{2}) \simeq \overline{Q} \times \overline{Q}$,

which is a product of 2 copies of $\overline{Q}$ (associated to the 2 roots of $X_2 \Leftrightarrow 2$) and has no nilpotent elements besides 0.

Example: Consider the extension $F_2(\sqrt{u})/F_2(u)$. Since $F_2(\sqrt{u}) \simeq F_2[X]/(X^2 - u)$,

$$\overline{F_2(u)} \otimes_{F_2(u)} F_2(\sqrt{u}) \simeq F_2(\sqrt{u}) \simeq \overline{F_2(u)}[X]/(X^2 - u) = \overline{F^2(u)}[X]/(X - \sqrt{u})^2,$$

which has the nonzero nilpotent element $X - \sqrt{u}$.

Theorem 3: Let L/K be a finite extension. Then L is separable over K if and only if any derivation of K has a unique extension to a derivation of L.

For above two proofs, the reader should be comfortable with the fact that injectivity and surjectivity of a linear map of vector spaces can be detected after a base extension: a linear map is injective or surjective if and only if its base extension to a larger field is injective or surjective.

Each of the three theorems above will be proved and then lead in its own way to proofs of the following two theorems.

Theorem 4: If L = K(a_1,....., a_r) and each a_i is separable over K then every element of L is separable over K (so L/K is separable).

Theorem 5: Let L/K be a finite extension and F be an intermediate field. If L/F and F/K are separable then L/K is separable.

We will use our new viewpoints to define separability for arbitrary (possibly non-algebraic) field extensions.

We want to show L/K is separable if and only if $Tr_{L/K} : L \to K$ is not identically 0. The trace map is either identically 0 or it is onto, since it is K-linear with target K, so another way of putting Theorem 1 is that we want to show L/K is separable if and only if the trace from L to K is onto.

Proof: We might as well take K to have positive characteristic p, since in characteristic 0 all finite field extensions are separable and the trace is not identically 0 : $TrL_{/K}(1) = [L : K] \neq 0$ in characteristic 0.

If L/K is separable, by the primitive element theorem we can write L = K(α) where α is separable over K. To show the trace is surjective for finite separable extensions, it suffices to prove surjectivity of the trace map on K(α)/K when K is any base field and α is separable over K.

If L/K is inseparable, then there must be some a ∈ L which is inseparable over K. Since $Tr_{L/K} = Tr_{K(\alpha)/K}$ o $Tr_{L/K(\alpha)}$, it success to prove the trace map on K(α)=K vanishes when α is inseparable over K.

For both cases of the field extension K(α)/K (α separable or inseparable over K), let α have minimal polynomial π(X) in K[X]. Write π(X) = $\bar{\pi}$ (Xpm) where m is as large as possible, so $\bar{\pi}$ (X) is separable. Thus π(X) is separable if and only if m = 0.

Let n = deg π = $p^m d$, with d = deg $\bar{\pi}$. In $\bar{K}[X]$,

$$\bar{\pi}(X) = (X - \beta_1) \dots (X - \beta_d)$$

for some β_i's, which are all distinct since $\bar{\pi}$ (X) is separable. Write $\beta_i = g_i^{p^m}$, so the γ_i's are distinct. Then

$$\pi(X) = \bar{\pi}(X^{p^m}) = (X^{p^m} - \beta_1) \dots (X^{p^m} - \beta_d) = (X - \gamma_1)^{p^m} \dots (X - \gamma_d)^{p^m}.$$

Consider now the extension of scalars up to $\overline{K}$ of the trace map $\mathrm{Tr}_{K(a)/K} : K(a) \to K$:

$$\overline{\mathrm{Tr}} = \mathrm{id}_{\overline{K}} \otimes \mathrm{Tr}_{k(a)/K} : \overline{K} \otimes_K K(a) \to \overline{K} \otimes_K K \simeq K.$$

$\overline{\mathrm{Tr}}$ is the trace map on $\overline{K} \otimes_K K(\alpha)$ as a $\overline{K}$-vector space.

Since tensoring with a field extension preserves injectivity and surjectivity of a linear map,

$$\mathrm{Tr}_{K(a)/K} \text{ is onto} \Leftrightarrow \overline{\mathrm{Tr}} \text{ is onto; } \mathrm{Tr}_{K(a)} = K \Leftrightarrow \overline{\mathrm{Tr}} = 0$$

Since $K(\alpha) \simeq K[X]/(\pi(X))$ as K-algebras, $K(\alpha) \simeq K[X]/(\pi(X))$ as $\overline{K}$-algebras, and thus is isomorphic to the direct product of the rings $\overline{K}[X]/(X^{p^m} - \beta_i)$. The trace is the sum of the traces to $\overline{K}$ on each $\overline{K}[X]/(X^{p^m} - \beta_i)$. Let's look at the trace from $\overline{K}[X]/(X^{p^m} - \beta_i)$. to $\overline{K}$.

In $\overline{K}[X]$, $X^{p^m} - \beta_i = (X - \gamma_i)^{p^m}$. Then $\overline{K}[X]/(X^{p^m} - \beta_i) = \overline{K}[Y]/(Y^{p^m})$, where $Y = X - \gamma_i$. If $m = 0$, then $\overline{K}[Y]/(Y^{p^m}) = \overline{K}$, so the trace to $\overline{K}$ is the identity. If $m > 0$, any element of $\overline{K}[Y]/(Y^{p^m})$ is the sum of a constant plus a multiple of Y , which is a constant plus a nilpotent element (since Y mod Y^{p^r} is nilpotent). Any constant in $\overline{K}[Y]/(Y^{p^m})$ has trace 0 since pm = 0 in $\overline{K}$ (because m > 0). A nilpotent element has trace 0. Thus the trace to K of any element of $\overline{K}[Y]/(Y^{p^m})$ is 0.

To summarize, when α is separable over K (i.e., m = 0), the trace map from $K(\alpha)$ to K is onto since it is onto after extending scalars to $\overline{K}$. When a is inseparable over K (i.e., m > 0), the trace map is identically 0 since it vanishes after extending scalars.

Theorem 1 implies Theorem 4.

Proof. Set $L_0 = K$, $L_1 = K(\alpha_1) = L_0(\alpha_1)$, and more generally $L_i = K(\alpha_1,....\alpha_i) = L_{i-1}(\alpha_i)$ for $i \geq 1$. So we have the tower of field extensions

$$K = L_0 \subset L_1 \subset L_2 \subset ... \subset L_{r-1} \subset L_r = L.$$

By transitivity of the trace,

$$\mathrm{Tr}_{L/K} = \mathrm{Tr}_{L_1/L_0} \text{ o } \mathrm{Tr}_{L_2/L_1} \text{ o} \cdots \text{o } \mathrm{Tr}_{L_r/L_{r-1}}$$

Since α_i is separable over K and the minimal polynomial of α_i over L_{i-1} divides its minimal polynomial over K, α_i is separable over L_{i-1}. Therefore $\mathrm{Tr}_{Li-1}(\alpha_i)/L_{i-1} : L_i \to L_{i-1}$ is onto from the proof of Theorem 1, so the composite map TrL/K : L $\to$ K is onto. Therefore L/K is separable by Theorem 1.

Corollary: Theorem 1 implies Theorem 5.

Proof: By Theorem 1 and the hypothesis of Theorem 5, both $\mathrm{Tr}_{L/F}$ and $\mathrm{Tr}_{F/K}$ are onto. Therefore, their composite $\mathrm{Tr}_{L/K}$ is onto, so L/K is separable by Theorem 1.

Proof: We will begin with the case of a simple extension $L = K(\alpha)$. Let $\pi(X)$ be the minimal polynomial of α over K, so $L \simeq K[X]/(\pi(X))$ as K-algebras and

$$\overline{K} \otimes_K L \cong \overline{K}[X]/(\pi(X))$$

as $\overline{K}$-algebras. This ring was considered in the proof of Theorem 1, where we saw its structure is different when $\pi(X)$ is separable or inseparable. If $\pi(X)$ is separable in K[X], then $K[X]/(\overline{K}(X))$

is a product of copies of the field $\overline{K}$, so it has no non-zero nilpotent elements. If $\pi(X)$ is inseparable, then $\overline{K}[X]/(\pi(X))$ is a product of copies of rings $\overline{K}[Y]/(Y^{p^m})$ with m > 0, which all have nonzero nilpotents.

Now we consider the structure of $\overline{K} \otimes_K L$ when L/K is any finite extension.

First assume L/K is separable. By the primitive element theorem, we can write L = K(α) and α is separable over K. By the first paragraph of the proof, $\overline{K} \otimes_K L \simeq \overline{K}^{[L:K]}$ since $\pi(X)$ has distinct linear factors in $\overline{K}$.

If L/K is inseparable, then some a $\in$ L is inseparable over K. Tensoring the inclusion map K(α) → L up to $\overline{K}$, we have an inclusion

$$\overline{K} \otimes_K K(\alpha) \to \overline{K} \otimes_K L.$$

The ring $\overline{K} \otimes_K K(\alpha)$ has a non-zero nilpotent element by the first paragraph of the proof, so $\overline{K} \otimes_K L$ does as well.

Corollary: The proof of Theorem 2 implies Theorem 4.

Proof: Make a tower of intermediate extensions in L/K as in (2.2). Note $\overline{K}$ is an algebraic closure of every field L_i in the tower. Since

$$\overline{K} \otimes_K L \simeq (\overline{K} \otimes_K L_1) \otimes_{L1} L$$

and $L_1 = K(\alpha_1)$ with α_1 separable over K, the proof of Theorem 2 implies

$$\overline{K} \otimes_K L_1 \simeq \overline{K}^{[L_1:K]}$$

as $\overline{K}$-algebras. Therefore

$$\overline{K} \otimes_K L \simeq \overline{K}^{[L_1:K]} \otimes_{L_1} L \simeq (\overline{K} \otimes_{L_1} L)^{[L_1:K]}$$

Since $L = L_1(\alpha_2, \ldots \alpha_r)$ with each α_i separable over L_1, we can run through the same computation for $\overline{K} \otimes_{L_2} L$ as we did for $\overline{K} \otimes_K L$, and we get $\overline{K} \otimes_{L_1} L \simeq (\overline{K} \otimes_{L_2} L)^{[L_2:L_1]}$, so

$$\overline{K} \otimes_K L \simeq (\overline{K} \otimes_{L_2} L)^{[L_2:L_1][L_1:K]} = (\overline{K} \otimes L_2\, L)^{[L_2:K]}.$$

Repeating this enough, in the end we get

$$\overline{K} \otimes_K L \simeq (\overline{K} \otimes_{L_r} L)^{[L_r:K]} \simeq \overline{K}^{[L:K]}.$$

Corollary: The proof of Theorem 2 implies Theorem 5.

Proof: The field $\overline{K}$ is an algebraic closure of F and L. Using Theorem 2,

$$\begin{aligned} \overline{K} \otimes_K L &\simeq (\overline{K} \otimes_K F) \otimes_F L \\ &\simeq \overline{K}\,[F:K] \otimes_F L && \text{since F/K is separable} \\ &\simeq (\overline{K} \otimes_F L)^{[F:K]} \end{aligned}$$

$\simeq \overline{K}^{[L:F][F:K]}$ since L=F is separable

$\simeq \overline{K}$ [L:K]

Thus L/K is separable by Theorem 1.2.

Theorem 6: Let L/K be an extension of fields, and $\alpha \in L$ be algebraic over K. Then is separable over K if and only if any derivation on K has a unique extension to a derivation on K(α).

Proof: When $\alpha \in L$ is separable over K, Corollary B.10 shows any derivation on K extends uniquely to a derivation on K(α).

Now suppose $\alpha \in L$ is inseparable over K. Then $\pi'(X) = 0$, where $\pi(X)$ is the minimal polynomial of α over K. In particular $\pi'(\alpha) = 0$. We are going to use this vanishing of $\pi'(\alpha)$ to construct a nonzero derivation on K(α) which extends the zero derivation on K.

Then the zero derivation on K has two lifts to K(α): the zero derivation on K(α) and this other derivation we will construct.

Define $Z : K(\alpha) \to K(\alpha)$ by $Z(f(\alpha)) = f'(\alpha)$, where $f(X) \in K[X]$. Is this well-defined?

Well, if $f_1(\alpha) = f_2(\alpha)$, then $f_1(X) \equiv f_2(X) \bmod \pi(X)$, say

$f_1(X) = f_2(X) + \pi(X)k(X)$.

Differentiating both sides with respect to X,

$f'_1(X) = f'_2(X) + \pi(X)k'(X) + \pi'(X)k(X)$:

Evaluating both sides at yields $f'_1(\alpha) = f'_2(\alpha)$ since $\pi'(\alpha) = 0$. So $Z : K(\alpha) \to K(\alpha)$ is well-defined.

It is left to the reader to check Z is a derivation on K(α). This derivation kills K, but $Z(\alpha) = 1$, so Z extends the zero derivation on K while not being the zero derivation itself.

The reader can check more generally that when α is inseparable over K and $\beta \in K(\alpha)$ is arbitrary the map $f(\alpha) \to f'(\alpha)\beta$ is a derivation on K(α) that extends the zero derivation on K and sends α to β. So there are many extensions of the zero derivation on K to K(α): one for each element of K(α).

We need a lemma to put inseparable extensions into a convenient form for our derivation constructions later.

Lemma: Let L/K be a finite inseparable field extension. Then there is an $\alpha \in L$ and intermediate field F such that $L = F(\alpha)$ and α is inseparable over F.

Proof: Inseparable field extensions only occur in positive characteristic. Let p be the characteristic of K. Necessarily $[L : K] > 1$. Since L/K is inseparable, there is some $\beta \in L$ that is inseparable over K.

Write $L = K(\alpha_1,.... \alpha_r)$. We will show by contradiction that some α_i has to be inseparable over K. Assume every α_i is separable over K. Then we can treat L/K as a succession of simple field extensions as in (2.2), where $L_i = L_{i-1}(\alpha_i)$ with α_i separable over L_{i-1}. By Theorem, any derivation on L_{i-1} extends to a derivation on L_i, so any derivation on K extends to a derivation on L. Moreover, this extended derivation on L is unique. To show that, consider two derivations D and D′ on L that are equal on K. Since $L_1 = K(\alpha_1)$ and α_1 is separable over K, the proof of Corollary B.10 tells us that D and D′ both send L_1 to L_1 and are equal on L_1. Now using L_1 in place of K, D and D′ being equal on L_1 implies they are equal on L_2 since $L_2 = L_1(\alpha_2)$ and α_2 is separable over L_1. We can keep going like this until we get D = D′ on $L_r = L$. As a special case of this uniqueness, the only derivation on L which vanishes on K is the zero derivation on L.

Now replace K as base field with K(β), over which the α_i's are of course still separable. Then any derivation on K(β) extends uniquely to a derivation on L. But in the proof of Theorem we saw there is a non-zero derivation Z on K(β) that vanishes on K, and an extension of that to a derivation on L is non-zero on L and is zero on K. We have a contradiction of the uniqueness of extensions, so in any set of field generators $\{\alpha_1, ..., \alpha_r\}$, some α_i must be inseparable in K.

Choose a generating set $\{\alpha_1,....,\alpha_r\}$ with as few inseparable elements as possible. At least one α_i is inseparable over K and we may assume that α_r is one of them. Set $\alpha = \alpha_r$ and $F = K(\alpha_1,....\alpha_{r-1})$ (so F = K if r = 1). Then L = F(α). We will show by contradiction that α must be inseparable over F, which is the point of the lemma.

Suppose α is separable over F. Then α is separable over the larger field $F(\alpha^p)$ since its minimal polynomial over $F(\alpha^p)$ divides its minimal polynomial over F. Since α is a root of $X^p - \alpha^p \in F(\alpha^p)[X]$, its (separable) minimal polynomial in $F(\alpha^p)[X]$ is a factor of this, so that polynomial must be X – α. Therefore, $\alpha \in F(\alpha^p)$. Taking p^k-th powers for any $k \geq 0$, $a^{p^k} \in F(a^{p^{k+1}})$, so

$$F(a^{p^k}) \subset F(a^{p^{k+1}}).$$

The reverse inclusion is obvious, so $F(a^{p^k}) = F(a^{p^{k+1}})$ for all $k \geq 0$. Therefore,

$$L = F(\alpha) = F(\alpha^{p^k}) = K(\alpha_1, ..., \alpha_{r-1}, \alpha_r^{pk})$$

for any $k \geq 0$. We can pick k so that α^{p^k} is separable over K (why?). Then the generating set $\{\alpha_1, ..., \alpha_{r-1}, a_r^{p^k}\}$ has with one less inseparable element among the field generators. This contradicts the choice of generators to have as few members in the list as possible that are inseparable over K, so α has to be inseparable over F.

Proof: Assume L/K is separable, so by the primitive element theorem L = K(α) where α is separable over K. Any derivation on K can be extended (using Theorem) uniquely to a derivation on L.

If L/K is inseparable, then Lemma lets us write L = F(α) with α inseparable over F, and $F \supset K$. The, by a construction used in the proof of Theorem, $f(\alpha) \to f'(\alpha)$ with $f(X) \in F[X]$ is a nonzero derivation on L which is zero on F, and thus also zero on the smaller field K. This shows the zero derivation on K has a non-zero extension (and thus two extensions) to a derivation on L.

Corollary: The proof of Theorem 3 implies Theorem 4.

Proof: Again we consider the tower of field extensions (2.2). Since $L_i = L_{i-1}(\alpha_i)$ and α_i is separable over L_{i-1}, the proof shows any derivation on L_{i-1} extends uniquely to a derivation on L_i. Therefore, any derivation on $K = L_0$ can be extended step-by-step through the tower (2.2) to a derivation on Lr = L. By the argument in the proof of Lemma, this derivation on L is unique.

Lemma: Let L/K be a finite extension and F be an intermediate extension such that F/K is separable. Then any derivation $F \to L$ which sends K to K has values in F.

Proof: Pick $\alpha \in F$, so α is separable over K. Now use Corollary B.10 to see the derivation $F \to L$ sends α to an element of $K(\alpha) \subset F$.

Corollary: Theorem 3 implies Theorem 5.

Proof: To prove L/K is separable, we want to show any derivation on K has a unique extension to a derivation on L. Since F/K is separable, a derivation on K extends to a derivation on F. Since L/F is separable, a derivation on F extends to a derivation on L.

For uniqueness, let D_1 and D_2 be derivations on L which extend the same derivation on K. Since $D_1(K) \subset K$ and $D_2(K) \subset K$, we have $D_1(F) \subset F$ and $D_2(F) \subset F$ by Lemma. Then $D_1 = D_2$ on F since F/K is separable, and $D_1 = D_2$ on L since L/F is separable.

When L/K is an algebraic extension of possibly infinite degree, here is the way separability is defined.

Definition: An algebraic extension L/K is called separable if every finite subextension of L=K is separable. Equivalently, L=K is separable when every element of L is separable over K.

This definition makes no sense if L/K is not an algebraic extension since a non-algebraic extension is not the union of its finite subextensions.

Theorem 1 has a problem in the infinite-degree case: there is no natural trace map. However, the conditions in Theorems 2 and 3 both make sense for a general L/K. (In the case of Theorem 2, we have to drop the specification of $\overline{K} \otimes_K L$ as a product of copies of $\overline{K}$, and just leave the statement about the tensor product having no non-zero nilpotent elements.) It is left to the reader to check for an infinite algebraic extension L/K that the conditions of Theorems 2 and 3 match Definition.

The conditions in Theorems 2 and 3 both make sense if L/K is not algebraic, so they could each potentially be used to define separability of a completely arbitrary field extension. But there is a problem: for transcendental (that is, non-algebraic) extensions the conditions in Theorems 2 and 3 are no longer equivalent. Indeed, take L = K(u), with u transcendental over K. Then $\overline{K} \otimes_K L = \overline{K}(u)$ is a field, so the condition in Theorem 2 is satisfied. However, the zero derivation on K has more than one extension to K(u): the zero derivation on K(u) and differentiation with respect to u on K(u).

Definition: A commutative ring with no nonzero nilpotent elements is called reduced.

A domain is reduced, but a more worthwhile example is a product of domains, like F3 × Q[X], which is not a domain but is reduced.

Definition: An arbitrary field extension L/K is called separable when the ring $\overline{K} \otimes_K L$ is reduced.

Using this definition, in characteristic 0 all field extensions are separable. In characteristic p, any purely transcendental extension is separable. The condition in Theorem 3, that derivations on the base field admit unique extensions to a larger field, characterizes not separable field extensions in general, but separable algebraic field extensions.

A condition equivalent to that in Definition is that $F \otimes_K L$ is reduced as F runs over the finite extensions of K.

The condition that $\overline{K} \otimes_K L$ is reduced makes sense not just for field extensions L/K, but for any commutative K-algebra. Define an arbitrary commutative K-algebra A to be separable when the ring $\overline{K} \otimes_K A$ is reduced. This condition is equivalent to $A \otimes_K F$ being reduced for every finite extension field F/K.

Example: Let A = K[X]/(f(X)) for any non-constant $f(X) \in K[X]$. The polynomial f(X) need not be irreducible, so A might not be a field. It is a separable K-algebra precisely when f(X) is a separable polynomial in K[X].

When [A : K] is finite, an analogue of Theorem 1 can be proved: A is a separable K-algebra if and only if the trace pairing hx; yi = $\mathrm{Tr}_{A/K}(xy)$ from A × A to K is non-degenerate.

Traces

Let A be a finite-dimensional commutative K-algebra (with identity), such as a finite extension field of K or the product ring Kn or even a mixture of the two: a product of finite extensions of K. To any a 2 A we associate the K-linear map m_α : A → A which is left multiplication by a:

$$x \to \alpha x:$$

For a; b ∈ A and α ∈ K, $m_{a+b} = m_a + m_b$ and $m_{aa} = am_a$, so m_a is a K-linear map.

Definition: For a finite-dimensional K-algebra A, the trace of a ∈ A is the trace of m_a.

That is, the trace of a is $\mathrm{tr}(m_a) \in K$, usually written as $\mathrm{Tr}_{A/K}(a)$, so $\mathrm{Tr}_{A/K} : A \to K$. The trace from A to K is K-linear, hence identically zero or surjective since K is a one-dimensional K-vector space.

Example: Since m_1 is the identity function, $\mathrm{Tr}_{A/K}(1) = [A : K]$.

Example: Suppose a ∈ A is nilpotent: ar = 0 for some r ≥ 1. Then $m_a^r = 0$, so m_a is a nilpotent linear transformation. Thus its eigenvalues are all 0, so $\mathrm{Tr}_{A/K}(a) = 0$.

We now consider a finite-dimensional L-algebra A with K a subfield of L such that [L : K] < ∞. We have finite-dimensional algebras A/L, A/K, and L/K. The next theorem is called the transitivity of the trace.

Theorem 7: In the above notation, $\mathrm{Tr}_{A/K} = \mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{A/L}$. In particular, if a ∈ L, then $\mathrm{Tr}_{A/K}(a) = [A : L]\mathrm{Tr}_{L/K}(a)$.

Proof: Let (e1; : : : ; em) be an ordered L-basis of A and (f1; : : : ; fn) be an ordered K-basis

of L. Thus as an ordered K-basis of A we can use

$$(e_1f_1,\ldots.., e_1f_n,\ldots.., e_mf_1,\ldots.., e_mf_n):$$

For a ∈ A, let

$$ae_j = \sum_{i=1}^{m} c_{ij}e_i,\ c_{ij}f_s = \sum_{r=1}^{n} b_{ijrs}f_r,$$

for $c_{ij} \in L$ and $b_{ijrs} \in K$. Thus $a(e_jf_s) = \sum_i \sum_r b_{ijrs}e_if_r$. So

$$[m_a]_{A/L} = (c_{ij}),\ [m_{cij}]_{L/K} = (b_{ijrs}),\ [m_a]_{A/K} = ([m_{cij}]_{L/K}):$$

Thus

$$\begin{aligned}
\mathrm{Tr}_{L/K}(\mathrm{Tr}_{A/L}(a)) &= \mathrm{Tr}_{L/K}(\sum_i c_{ii}) \\
&= \sum_i \mathrm{Tr}_{L/K}(c_{ii}) \\
&= \sum_i \sum_r b_{iirr} \\
&= \mathrm{Tr}_{A/K}(a).
\end{aligned}$$

Theorem 8: Let A and B be finite-dimensional K-algebras. For (a; b) in the product ring A × B, $\mathrm{Tr}_{(A\times B)/K}(a, b) = \mathrm{Tr}_{A/K}(a) + \mathrm{Tr}_{B/K}(b)$.

Proof: Let $e_1,\ldots.., e_m$ be a K-basis of A and $f_1,\ldots.., f_n$ be a K-basis of B. In A × B, $e_i \cdot f_j = 0$. Therefore, the matrix for multiplication by (a, b), with respect to the K-basis { e_if_j }, is a block-diagonal matrix $\begin{pmatrix} [m_a] & 0 \\ 0 & [m_b] \end{pmatrix}$, whose trace is $\mathrm{Tr}_{A/K}(a) + \mathrm{Tr}_{B/K}(b)$.

Theorem 9: Let A be a finite-dimensional K-algebra, L/K be a field extension, and B = $L\otimes_K A$ be the base extension of A to an L-algebra. For a ∈ A, $Tr_{B/L}(1\otimes a) = Tr_{A/K}(a)$.

Proof: Let $e_1,\ldots\ldots, e_n$ be a K-basis of A. Write $ae_j = \sum_{i=1}^{n} c_{ij}e_i$, so the matrix for m_a in this basis is (c_{ij}).

The tensors $1 \otimes e_1,\ldots\ldots, 1 \otimes$ en are an L-basis of B, and we have

$$(1 \otimes a)\,(1 \otimes e_j) = 1 \otimes ae_j = \sum_{i=1}^{n} c_{ij}(1\otimes e_i),$$

so the matrix for $m_{1\otimes a}$ on B is the same as the matrix for m_a on A. Thus $Tr_{A/K}(a) = Tr_{B/L}(1 \otimes a)$.

Remark: Because $m_{1\otimes a}$ and m_a have the same matrix representation, not only are their traces the same but their characteristic polynomials are the same.

Theorem 10: Let A be a finite-dimensional K-algebra. For any field extension L/K, the base extension by K of the trace map A → K is the trace map $L \otimes_K A \to L$. That is, the function $id\otimes Tr_{A/K}$: L⊗K A → L which sends an elementary tensor x ⊗ a to $xTr_{A/K}(a)$ is the trace map $Tr_{(L\otimes KA)/L}$.

Proof: We want to show $Tr_{(L\otimes KA)/L}(t) = (id\otimes Tr_{A/K})(t)$ for all t ∈ $L\otimes_K A$. The elementary tensors additively span $L\otimes_K A$ so it succes to check equality when t = x ⊗ a for x ∈ K and a ∈ A. This means we need to check $Tr_{(L\otimes KA)/K}(x \otimes a) = xTr_{A/K}(a)$.

Pick a K-basis $e_1,\ldots, e_n$ for A and write $ae_j = \sum_{i=1}^{n} c_{ij}e_i$ with c_{ij} ∈ K. The elementary tensors $1 \otimes e_1,\ldots, 1 \otimes e_n$ are an L-basis of L⊗K A and

$$(x\otimes a)(1\otimes e_j) = x\otimes ae_j = \sum_{i=1}^{n} c_{ij}(x\otimes e_i) = \sum_{i=1}^{n} c_{ij}x(1\otimes e_i)$$

by the definition of the L-vector space structure on $L\otimes_K A$. So the matrix for multiplication by x ⊗ a in the basis $\{1 \otimes e_i\}$ is $(c_{ij}x)$, which implies

$$Tr_{(L\otimes KA)/L}(x\otimes a) = \sum_{i=1}^{n} c_{ii}x = x\sum_{i=1}^{n} cii = xTr_{A/K}(a).$$

Derivations

A derivation is an abstraction of differentiation on polynomials. We want to work with derivations on fields, but polynomial rings will intervene, so we need to understand derivations on rings before we focus on fields.

Let R be a commutative ring and M be an R-module (e.g., M = R). A derivation on R with values in M is a map D : R → M such that D(a + b) = D(a) + D(b) and D(ab) = aD(b) + bD(a). Easily, by induction $D(a^n) = na^{n-1}D(a)$ for any n ≥ 1. When M = R, we will speak of a derivation on R.

Example: For any commutative ring A, differentiation with respect to X on A[X] is a derivation on A[X] (R = M = A[X]).

Example: Let R = A[X] and M = A as an R-module by f(X)a := f(0)a. Then D: R → M by D(f) = f′(0) is a derivation.

Example: Let D : R → R be a derivation. For $f(X) = \sum_i a_iX^i$ in R[X], set $f^D(X) = \sum_i D(a_i)X^i$.

This is the application of D coefficentwise to f(X). The operation f → f^D is a derivation on R[X] (to check the product rule, it suffices to look at monomials).

If $R = F_2[u]$ and D is the usual u-derivative on $F_2[u]$, then the polynomial $f(X) = (u^3 + u)X^4 + uX^3 + u^2X + 1$ in R[X] has $f^D(X) = (u^2 + 1)X^4 + X^3$.

Any element of R satisfying D(a) = 0 is called a D-constant, or just a constant if the derivation is understood. The constants for a derivation form a subring. For instance, from the product rule, taking a = b = 1, we obtain D(1) = 0.

Example: The set of all constants for X-differentiation on K[X] is K when K has characteristic 0 and K[Xp] when K has characteristic p.

Example: If D: R → R is a derivation and $f \to f^D$ is the corresponding derivation on R[X], its ring of constants is C[X], where C is the constants for D.

We will generally focus on derivations from R to R, although it will be convenient to allow R-modules as the target space for derivations in Corollary, which is used in the main text in the proofs of Theorem 3 and Lemma.

Example: Let's check that any derivation on K[X] which has the elements of K among its constants has the form D(f) = hf′ for some h ∈ K[X]. (When h = 1, this is the usual X-derivative.)

When K is among the constants of D, D is K-linear: D(cf) = cD(f) + fD(c) = cD(f). Therefore, D is determined by what it does to a K-basis of K[X], such as the power functions X^n. By induction, $D(X^n) = nX^{n-1}D(X)$ for all n ≥ 1. Therefore, by linearity, D(f) = f′(X)D(X) for every f ∈ K[X]. Set h = D(X).

Theorem 11: Let R be a domain with fraction field K. Any derivation D: R → K uniquely extends to $\tilde{D}$: K → K, given by the quotient rule: $\tilde{D}$ (a/b) = (bD(a) – aD(b))/b^2.

Proof: Suppose there is an extension of D to a derivation on K. Then, if x = a/b is in K (with a, b ∈ A), a = bx, so

$$D(a) = bD(x) + xD(b):$$

Therefore in K,

$$D(x) = \frac{D(a) - xD(b)}{b} = \frac{bD(a) - aD(b)}{b^2}$$

To see, conversely, that this formula does give a derivation $\tilde{D}$ on K, first we check it is well-defined: if a/b = c/d (with b and d nonzero), then ad = bc, so

$$aD(d) + dD(a) = bD(c) + cD(b).$$

Therefore,

$$\begin{aligned}\frac{bD(a) - aD(b)}{b^2} - \frac{dD(a) - cD(d)}{d^2} &= \frac{d^2(bD(a) - aD(b)) - b^2(dD(c) - cD(d))}{b^2d^2}\\ &= \frac{bd(dD(a) - bD(c)) - d^2aD(b) + b^2cD(d)}{b^2d^2}\\ &= \frac{bd(cD(b) - aD(d)) - d^2aD(b) + b^2cD(d)}{b^2d^2}\\ &= \frac{(bc - ad)dD(b) - (ad - bc)bD(d)}{b^2d^2}\\ &= 0 \text{ since } ad = bc.\end{aligned}$$

That $\tilde{D}$ satisfies the sum and product rules is left to the reader to check.

Theorem 12: Let L/K be a finite extension of fields, and D: K → K be a derivation. Suppose a ∈ L is separable over K, with minimal polynomial $\pi(X) \in K[X]$. That is, $\pi(X)$ is irreducible in K[X], $\pi(\alpha) = 0$, and $\pi'(\alpha) \neq 0$. Then D has a unique extension from K to a derivation on the field K(α), and it is given by the rule

$$D(f(\alpha)) = f^D(\alpha) - f'(\alpha)\frac{\pi D(a)}{\pi'(a)}$$

for any f(X) ∈ K[X].

Proof: The rule (B.1) looks bizarre at first. To make it less so, we start by assuming D has an extension to K(α), and prove by a direct computation that it must be given by the indicated formula. For any β ∈ K(α), write β = f(α), where f(X) = $\sum_{i=0}^{r} c_i X_i$ and $c_i \in K$. Then

$$D(\beta) = D(f(\alpha)) = \sum_{i=0}^{r}(D(c_i)\alpha^i + c_i(i\alpha^{i-1}D(\alpha))) = f^D(\alpha) + f'(\alpha)D(\alpha).$$

Taking f(X) = π(X) to be the minimal polynomial of α over K, f(α) = 0, so if D has an extension to K(α) then (B.2) becomes

$$0 = \pi^D(\alpha) + \pi'(\alpha)D(\alpha),$$

which proves (since $\pi'(\alpha) \neq 0$) that D(α) must be given by the formula $-\pi^D(\alpha)/\pi'(\alpha)$. Plugging this formula for D(α), shows D(β) must be given by the formula. Since β was a general element of K(α), this proves D has at most one extension to a derivation on K(α).

Now, to show the formula works, we start over and define

$$D(f(\alpha)) := f^D(a) - f'(\alpha)\frac{\pi^D(\alpha)}{\pi'(\alpha)}.$$

We need to show this formula is well-defined.

Suppose $f_1(\alpha) = f_2(\alpha)$ for $f_1; f_2 \in K[X]$. Then $f_1(X) \equiv f_2(X) \bmod \pi(X)$, say

$$f_1(X) = f_2(X) + \pi(X)k(X)$$

for some k(X) ∈ K[X]. Differentiating both sides with respect to X in the usual way,

$$f'_1(X) = f'_2(X) + \pi(X)k'(X) + \pi'(X)k(X).$$

Evaluating at X = α,

$$f'_1(\alpha) = f'_2(\alpha) + \pi'(\alpha)k(\alpha).$$

Since $\pi'(\alpha) \neq 0$, we divide by $\pi'(\alpha)$ and multiply through by $-\pi^D(\alpha)$ to get

$$-f'_1(\alpha)\frac{\pi^D(a)}{\pi'(a)} = -f'_2(a)\frac{\pi^D(\alpha)}{\pi'(\alpha)} - \pi^D(\alpha)k(\alpha).$$

We want to add $f_1^D(\alpha)$ to both sides. First, apply D to the coefficients in (B.3), which is a derivation on K[X], to get

$$f_1^D(X) = f_2^D(X) + \pi(X)_k^D(X) + \pi^D(X)k(X).$$

Therefore,

$$f_1^D(a) = f_2^D(a) + \pi^D(\alpha)k(a).$$

Add this to both sides to get

$$f_1^D(\alpha) - f_2^{'}(\alpha)\frac{\pi^D(a)}{\pi'(a)} = f_2^D(\alpha) + \pi^D(\alpha)k(\alpha) - f_2^{'}(\alpha)\frac{\pi^D(a)}{\pi'(a)} - \pi^D(\alpha)k(\alpha)$$

$$= f_2^D(\alpha) - f_2^{'}(a)\frac{\pi^D(\alpha)}{\pi'(\alpha)}.$$

This proves the formula for a derivation on K(α) is well-defined. It is left to the reader to check this really is a derivation.

Example: In contrast with Theorem 12, consider K = F_p(u) and L = K(α) where α is a root of X^p – u ∈ K[X]. This is an inseparable irreducible polynomial over K. The u-derivative on K does not have any extension to a derivation on L. Indeed, suppose the u-derivative on K has an extension to L, and call it D. Applying D to the equation a^p = u gives

$$p\alpha^{p-1}D(\alpha) = D(u).$$

The left side is 0 since we're in characteristic p. The right side is 1 since D is the u-derivative on F_p(u). This is a contradiction, so D does not exist.

Corollary: Let L/K be a finite extension of fields. For any derivation D: K → L and α ∈ L which is separable over K, D has a unique extension to a derivation K(α) → L. If D(K) ⊂ K then D(K(α)) ⊂ K(α).

Proof: Follow the argument in the proof of Theorem 12, allowing derivations to have values in L rather than in K(α). The formula for D(f(α)) still turns out to be the same as in (B.1). In particular, if D(K) ⊂ K then the extension of D to a derivation on K(α) actually takes values in K(α).

Self Assessment

1. A .... ring with no non-zero nilpotent element is called reduced.

   (a) associative ring (b) commutative ring

   (c) multiplicative ring (d) addition ring

2. An arbitrary field extension .... is called separable when the ring $\overline{K} \otimes_u L$ is reduced.

   (a) $L^{-1}k$ (b) L/K

   (c) K/L^{-1} (d) $(L + K)^{-1}$

3. If L/K be a .... extensions. Then L is separable over K. If and only if any derivation of K has a unique extension to a derivative of L.

   (a) finite (b) infinite

   (c) domain (d) split

4. The extension $F_2(\sqrt{u})/F_2/4)$. Since $F_2(\sqrt{u}) \cong F_2[x]/x^2 - u$, which then the non-zero nilpotent element ....

   (a) $X - \sqrt{u}$ (b) $\sqrt{u} - X$

   (c) $X^{-1} - \sqrt{u}$ (d) $u - \sqrt{u} - x^{-1}$

5. If $D : R \rightarrow R$ is a derivatives and $f \rightarrow F0$ is the corresponding derivation on R[x] from its ring of constants in C[x], where .... is the constant for ...., $f(x) = \sum a_1 x^1$ in R[x] and $fd(x) = \sum_{u} D(a_i)X_i$

   (a) D, C (b) C, D

   (c) X, C (d) C, D

9.2 Summary

- Let L/K be a finite extension. Then L is separable over K if and only if any derivation of K has a unique extension to a derivation of L.
- If $L = K(a_1, ..., a_r)$ and each a_i is separable over K then every element of L is separable over K (so L/K is separable).
- Let L/K be a finite extension and F be an intermediate field. If L/F and F/K are separable then L/K is separable.
- The proof of Theorem 2 implies Theorem 4.
- Let L/K be an extension of fields, and $\alpha \in L$ be algebraic over K. Then is separable over K if and only if any derivation on K has a unique extension to a derivation on $K(\alpha)$.
- A commutative ring with no nonzero nilpotent elements is called reduced.
- A domain is reduced, but a more worthwhile example is a product of domains, like F3 × Q[X], which is not a domain but is reduced.
- An arbitrary field extension L/K is called separable when the ring $\overline{K} \otimes_K L$ is reduced.
- A derivation is an abstraction of differentiation on polynomials. We want to work with derivations on fields, but polynomial rings will intervene, so we need to understand derivations on rings before we focus on fields.

9.3 Keywords

Separability: Separability of a finite field extension L/K can be described in several different ways.

Commutative Ring: A commutative ring with no nonzero nilpotent elements is called reduced.

Domain: A domain is reduced, but a more worthwhile example is a product of domains, like F3 × Q[X], which is not a domain but is reduced.

Derivation: A derivation is an abstraction of differentiation on polynomials.

9.4 Review Questions

1. Let R be a domain with fraction field K. Any derivation $D: R \rightarrow K$ uniquely extends to $\tilde{D} : K \rightarrow K$, given by the quotient rule: $\tilde{D}(a/b) = (bD(a) - aD(b))/b^2$. Prove it.
2. Let L/K be a finite extension of fields, and $D: K \rightarrow K$ be a derivation. Suppose $a \in L$ is separable over K, with minimal polynomial $\pi(X) \in K[X]$. That is, $\pi(X)$ is irreducible in K[X], $\pi(\alpha) = 0$, and $\pi'(\alpha) \neq 0$. Then D has a unique extension from K to a derivation on the field $K(\alpha)$, and it is given by the rule.

Notes

Answers: Self Assessment

1. (b) 2. (b) 3. (a) 4. (a) 5. (b)

9.5 Further Readings

Books

Dan Saracino: Abstract Algebra; A First Course.

Mitchell and Mitchell: An Introduction to Abstract Algebra.

John B. Fraleigh: An Introduction to Abstract Algebra (Relevant Portion).

Online links

www.jmilne.org/math/CourseNotes/

www.math.niu.edu

www.maths.tcd.ie/

archives.math.utk.edu

Unit 10: Galois Theory

Notes

CONTENTS

Objectives

After studying this unit, you will be able to:

- Discuss Galois theory
- Describe repeated roots

Introduction

In the last unit, you have studied about extension field. This unit will provide information related to Galois theory.

10.1 Galois Theory

This gives the definition of the Galois group and some results that follow immediately from the definition. We can give the full story for Galois groups of finite fields.

We use the notation Aut(F) for the group of all automorphisms of F, that is, all one-to-one functions from F onto F that preserve addition and multiplication. The smallest subfield containing the identity element 1 is called the prime subfield of F. If F has characteristic zero, then its prime subfield is isomorphic to Q, and if F has characteristic p, for some prime number p, then its prime subfield is isomorphic to Z_p. In either case, for any automorphisms ϕ of F we must have $\phi(x) = x$ for all elements in the prime subfield of F.

To study solvability by radicals of a polynomial equation $f(x) = 0$, we let K be the field generated by the coefficients of f(x), and let F be a splitting field for f(x) over K. Galois considered permutations of the roots that leave the coefficient field fixed. The modern approach is to consider the automorphism determined by these permutations. The first result is that if F is an extension field of K, then the set of all automorphism $\phi : F \to F$ such that $\phi(a) = a$ for all $a \in K$ is a group under composition of functions. This justifies the following definitions.

Definition: Let F be an extension field of K. The set

$$\{ \theta \in \text{Aut}(F) \mid \theta(a) = a \text{ for all } a \in K \}$$

is called the Galois group of F over K, denoted by Gal(F/K).

Definition: Let K be a field, let $f(x) \in K[x]$, and let F be a splitting field for f(x) over K. Then Gal(F/K) is called the Galois group of f(x) over K, or the Galois group of the equation f(x) = 0 over K.

Proposition states that if F is an extension field of K, and $f(x) \in K[x]$, then any element of Gal(F/K) defines a permutation of the roots of f(x) that lie in F. The next theorem is extremely important.

Theorem 1: Let K be a field, let $f(x) \in K[x]$ have positive degree, and let F be a splitting field for f(x) over K. If no irreducible factor of f(x) has repeated roots, then j Gal(F=K)j = [F : K].

This result can be used to compute the Galois group of any finite extension of any finite field, but first we need to review the structure of finite fields. If F is a finite field of characteristic p, then it is a vector space over its prime subfield Z_p, and so it has p^n elements, where $[F : Z_p] = n$. The structure of F is determined by the following theorem.

Theorem 2: If F is a finite field with p^n elements, then F is the splitting field of the polynomial $x^{p^n} - x$ over the prime subfield of F.

The description of the splitting field of $x^{p^n} - x$ over Z_p shows that for each prime p and each positive integer n, there exists a field with p^n elements. The uniqueness of splitting fields shows that two finite fields are isomorphic iff they have the same number of elements. The field with p^n elements is called the Galois field of order pn, denoted by $GF(p^n)$. Every finite field is a simple extension of its prime subfield, since the multiplicative group of nonzero elements is cyclic, and this implies that for each positive integer n there exists an irreducible polynomial of degree n in $Z_p[x]$.

If F is a field of characteristic p, and $n \in Z+$, then $\{a \in F \mid a^{p^n} = a\}$ is a subfield of F, and this observation actually produces all subfields. In fact, Proposition 6.5.5 has the following statement: Let F be a field with p^n elements. Each subfield of F has p^m elements for some divisor m of n.

Conversely, for each positive divisor m of n there exists a unique subfield of F with pm elements. If F is a field of characteristic p, consider the function $\phi : F \to F$ defined by $\phi(x) = xp$. Since F has characteristic p, we have $\phi(a + b) = (a + b)^p = a^p + b^p = \phi(a) + \phi(b)$, because in the binomial expansion of $(a + b)^p$ each coefficient except those of ap and bp is zero. (The coefficient $(p!)/(k!(p - k)!)$ contains p in the numerator but not the denominator since p is prime, and so it must be equal to zero in a field of characteristic p.) It is clear that ϕ preserves products, and so ϕ is a ring homomorphism. Furthermore, since it is not the zero mapping, it must be one-to-one. If F is finite, then ϕ must also be onto, and so in this case ϕ is called the Frobenius automorphism of F.

Note that $\phi^n(x) = x^{p^n}$ (Inductively, $\phi^n(x) = (\phi^{n-1}(x))^p = (x^{p^{n-1}})\ p = x^{p^n}$.) Using an appropriate power of the Frobenius automorphism, we can prove that the Galois group of any finite field must be cyclic.

Theorem 3: Let K be a finite field and let F be an extension of K with [F : K] = m. Then Gal(F/K) is a cyclic group of order m.

Outline of the proof: We start with the observation that F has pn elements, for some positive integer n. Then K has pr elements, for r = n/m, and F is the splitting field of $x^{p^n} - x$ over its prime subfield, and hence over K. Since f(x) has no repeated roots, to conclude that $|\text{Gal}(F/K)| = m$. Now define $\theta : F \to F$ to be the rth power of the Frobenius automorphism. That is, define

$\theta(x) = x^{p^r}$. To compute the order of in Gal(F/K), first note that θ^m is the identity since $\theta^m(x) = x^{p^{rm}} = x^{p^n} = x$ for all $x \in F$. But θ cannot have lower degree, since this would give a polynomial with too many roots. It follows that θ is a generator for Gal(F/K).

10.2 Repeated Roots

In computing the Galois group of a polynomial, it is important to know whether or not it has repeated roots. A field F is called perfect if no irreducible polynomial over F has repeated roots. This section includes the results that any field of characteristic zero is perfect, and that any finite field is perfect.

In the previous section, we showed that the order of the Galois group of a polynomial with no repeated roots is equal to the degree of its splitting field over the base field. The first thing in this section is to develop methods to determine whether or not a polynomial has repeated roots.

Let f(x) be a polynomial in K[x], and let F be a splitting field for f(x) over K. If f(x) has the factorization $f(x) = (x - r_1)^{m_1} \ldots (x - r_t)^{m_t}$ over F, then we say that the root r_i has multiplicity m_i. If $m_i = 1$, then r_i is called a simple root.

Let $f(x) \in K[x]$, with $f(x) = \sum_{k=0}^{t} a_k x^k$. The formal derivative f′(x) of f(x) is defined by the formula $f'(x) = \sum_{k=0}^{t} k a_k x^{k-1}$, where ka_k denotes the sum of a_k added to itself k times. It is not difficult to show from this definition that the standard differentiation formulas hold. Proposition shows that the polynomial $f(x) \in K[x]$ has no multiple roots iff it is relatively prime to its formal derivative f′(x). Proposition shows that f(x) has no multiple roots unless char(K) = $p \neq 0$ and f(x) has the form $f(x) = a_0 + a_1x^p + a_2x^{2p} + \ldots + a_nx^{np}$.

A polynomial f(x) over the field K is called separable if its irreducible factors have only simple roots. An algebraic extension field F of K is called separable over K if the minimal polynomial of each element of F is separable. The field F is called perfect if every polynomial over F is separable.

Theorem states that any field of characteristic zero is perfect, and a field of characteristic $p > 0$ is perfect if and only if each of its elements has a pth root in the field. It follows immediately from the theorem that any finite field is perfect.

To give an example of a field that is not perfect, let p be a prime number, and let $K = Z_p$. Then in the field K(x) of rational functions over K, the element x has no pth root. Therefore, this rational function field is not perfect.

The extension field F of K is called a simple extension if there exists an element $u \in F$ such that F = K(u). In this case, u is called a primitive element. Note that if F is a finite field, then Theorem shows that the multiplicative group $F^{\times}$ is cyclic. If the generator of this group is a, then it is easy to see that F = K(a) for any subfield K. Theorem shows that any finite separable extension is a simple extension.

10.3 The Fundamental Theorem

Here we study the connection between subgroups of Gal(F/K) and fields between K and F. This is a critical step in proving that a polynomial is solvable by radicals if and only if its Galois group is solvable.

Let F be a field, and let G be a subgroup of Aut(F). Then

$$\{a \in F \mid \theta(a) = a \text{ for all } \theta \in G\}$$

is called the G-fixed subfield of F, or the G-invariant subfield of F, and is denoted by F^G. (Proposition shows that F^G is actually a subfield of F.) If F is the splitting field over K of a separable polynomial and G = Gal(F/K), then Proposition shows that $F^G = K$. Artin's lemma provides the first really significant result of the section. It states that if G is a finite group of automorphism of the field F, and $K = F^G$, then $[F : K] \le |G|$.

Let F be an algebraic extension of the field K. Then F is said to be a normal extension of K if every irreducible polynomial in K[x] that contains a root in F is a product of linear factors in F[x]. With this definition, the following theorem and its corollary can be proved from previous results.

Theorem 4: The following are equivalent for an extension field F of K:

(1) F is the splitting field over K of a separable polynomial;

(2) K = FG for some finite group G of automorphism of F;

(3) F is a finite, normal, separable extension of K.

As a corollary, we obtain the fact that if F is an extension field of K such that $K = F^G$ for some finite group G of automorphisms of F, then G = Gal(F/K).

The next theorem is the centerpiece of Galois theory. In the context of the fundamental theorem, we say that two intermediate subfields E_1 and E_2 are conjugate if there exists $\phi \in \text{Gal}(F/K)$ such that $\phi(E_1) = E_2$. Proposition states that if F is the splitting field of a separable polynomial over K, and $K \subseteq E \subseteq F$, with H = Gal(F/E), then $\text{Gal}(F/\phi(E)) = \phi H \phi^{-1}$, for any $\phi \in \text{Gal}(F/K)$.

Theorem 5 (The Fundamental Theorem of Galois Theory): Let F be the splitting field of a separable polynomial over the field K, and let G = Gal(F/K).

(a) There is a one-to-one order-reversing correspondence between subgroups of G and subfields of F that contain K:

(i) The subfield F^H corresponds to the subgroup H, and $H = \text{Gal}(F/F^H)$.

(ii) If $K \subseteq E \subseteq F$, then the corresponding subgroup is Gal(F/E), and $E = F^{\text{Gal}}(F/E)$.

(b) [F : FH] = |H| and $[F^H : K] = [G : H]$, for any subgroup H of G.

(c) Under the above correspondence, the subgroup H is normal iff F^H is a normal extension of K. In this case, $\text{Gal}(E/K) \simeq \text{Gal}(F/K) / \text{Gal}(F/E)$.

For example, suppose that F is a finite field of characteristic p, and has p^m elements. Then [F : GF(p)] = m, and so G = Gal(F= GF(p)) is a cyclic group of degree m by Corollary. Since G is cyclic, the subgroups of G are in one-to-one correspondence with the positive divisors of m. Proposition shows that the subfields of F are also in one-to-one correspondence with the positive divisors of m. Remember that the smaller the subfield, the more automorphisms will leave it invariant. By the Fundamental Theorem of Galois Theory, a subfield E with [E : GF(p)] = k corresponds to the cyclic subgroup with index k, not to the cyclic subgroup of order k.

Self Assessment

1. If F has characteristics zero, then its prime subfield is isomorphic to Q and if F has characteristics P, for some prime number P, then its prime subfield is .... to Zp.

(a) homomorphic (b) isomorphic

(c) automorphism (d) polynomial

2. Let F be extension field of K. The set { Q ∈ Aut(F) | Q(a) = a for all a ∈ K } is Galois group is denoted by ....

   (a) Gal(F/K) (b) Gal(u/F)

   (c) Gal-1(K/F) (d) Gal(k × F)

3. Let K be a finite field and let F be an extension of K with [F : k] = m. Then Gal(F/k) is a .... group of order m.

   (a) cyclic (b) polynomial

   (c) permutation (d) finite

4. A polynomial f(x) over the field k is called .... if its irreducible factors have only simple roots.

   (a) spittery field (b) extension field

   (c) separable (d) finite field

5. The .... F of K is called simple extensions. If then exist an element u ∈ F. Such that F = K(u).

   (a) finite field (b) extension field

   (c) separable field (d) spliting field

10.4 Summary

- Let F be an extension field of K. The set

  $$\{ \theta \in \text{Aut}(F) \mid \theta(a) = a \text{ for all } a \in K \}$$

  is called the Galois group of F over K, denoted by Gal(F/K).

- Let K be a field, let f(x) ∈ K[x], and let F be a splitting field for f(x) over K. Then Gal(F/K) is called the Galois group of f(x) over K, or the Galois group of the equation f(x) = 0 over K.

- It states that if F is an extension field of K, and f(x) ∈ K[x], then any element of Gal(F/K) defines a permutation of the roots of f(x) that lie in F. The next theorem is extremely important.

- Let K be a field, let f(x) ∈ K[x] have positive degree, and let F be a splitting field for f(x) over K. If no irreducible factor of f(x) has repeated roots, then j Gal(F=K)j = [F : K].

  This result can be used to compute the Galois group of any finite extension of any finite field, but first we need to review the structure of finite fields. If F is a finite field of characteristic p, then it is a vector space over its prime subfield Z_p, and so it has p^n elements, where $[F : Z_p] = n$. The structure of F is determined by the following theorem.

- If F is a finite field with p^n elements, then F is the splitting field of the polynomial $x^{p^n} - x$ over the prime subfield of F.

- Let K be a finite field and let F be an extension of K with [F : K] = m. Then Gal(F/K) is a cyclic group of order m.

- (The fundamental theorem of Galois theory) Let F be the splitting field of a separable polynomial over the field K, and let G = Gal(F/K).

10.5 Keywords

Prime Subfield: If F is a finite field with p^n elements, then F is the splitting field of the polynomial $x^{p^n} - x$ over the prime subfield of F.

The Fundamental Theorem of Galois Theory: Let F be the splitting field of a separable polynomial over the field K, and let G = Gal(F/K).

10.6 Review Questions

1. Determine the group of all automorphisms of a field with 4 elements.
2. Let F be the splitting field in C of $x^4 + 1$.
   (a) Show that [F : Q] = 4.
   (b) Find automorphisms of F that have fixed fields Q($\sqrt{2}$), Q(i), and Q($\sqrt{2}$ i), respectively.
3. Find the Galois group over Q of the polynomial $x^4 + 4$.
4. Find the Galois groups of $x^3 - 2$ over the fields Z_5 and Z_{11}.
5. Find the Galois group of $x^4 - 1$ over the field Z_7.
6. Find the Galois group of $x^3 - 2$ over the field Z_7.
7. Let f(x) 2 Q[x] be irreducible over Q, and let F be the splitting field for f(x) over Q. If [F : Q] is odd, prove that all of the roots of f(x) are real.
8. Find an element α with Q($\sqrt{2}$, i) = Q(α).
9. Find the Galois group of $x^6 - 1$ over Z_7.
10. Prove that if F is a field and K = F^G for a finite group G of automorphisms of F, then there are only finitely many subfields between F and K.
11. Let F be the splitting field over K of a separable polynomial. Prove that if Gal(F/K) is cyclic, then for each divisor d of [F : K] there is exactly one field E with $K \subseteq E \subseteq F$ and [E : K] = d.
12. Let F be a finite, normal extension of Q for which |Gal(F=Q)| = 8 and each element of Gal(F/Q) has order 2. Find the number of subfields of F that have degree 4 over Q.
13. Let F be a finite, normal, separable extension of the field K. Suppose that the Galois group Gal(F/K) is isomorphic to D_7. Find the number of distinct subfields between F and K. How many of these are normal extensions of K?
14. Show that F = Q(i, $\sqrt{2}$) is normal over Q; find its Galois group over Q, and find all intermediate fields between Q and F.
15. Let F = Q($\sqrt{2}$, $\sqrt[3]{2}$). Find [F : Q] and prove that F is not normal over Q.
16. Find the order of the Galois group of $x^5 - 2$ over Q.

Answers: Self Assessment

1. (b) 2. (a) 3. (a) 4. (c) 5. (b)

10.7 Further Readings

Books

Dan Saracino: Abstract Algebra; A First Course.

Mitchell and Mitchell: An Introduction to Abstract Algebra.

John B. Fraleigh: An Introduction to Abstract Algebra (Relevant Portion).

Online links

www.jmilne.org/math/CourseNotes/

www.math.niu.edu

www.maths.tcd.ie/

archives.math.utk.edu

Richa Nandra, Lovely Professional University

Notes

Unit 11 : Computing Galois Groups

CONTENTS

Objectives

After studying this unit, you will be able to:

- Discuss transitively and transitive group
- Explain computing Galois group

Introduction

In the last unit, you have studied about Galois theory. In this unit, you will get information related to computing the Galois groups.

11.1 Transitively Group

Definition: Let G be a group acting on a set S. We say that G acts **transitively** on S if for each pair of elements x,y in S there exist an element g in G such that y = gx.

If G is a subgroup of the symmetric group S_n, then G is called a **transitive** group if it acts transitively on the set { 1, 2, ... , n }.

11.2 Separable Polynomial

Proposition: Let f(x) be a separable polynomial over the field K, with roots r_1 , ... , r_n in its splitting field F. Then f(x) is irreducible over K if and only if Gal(F/K) acts transitively on the roots of f(x).

Lemma: Let p be a prime number, and let G be a transitive subgroup of S_p. Then any nontrivial normal subgroup of G is also transitive.

Lemma: Let p be a prime number, and let G be a solvable, transitive subgroup of S_p. Then G contains a cycle of length p.

Proposition: Let p be a prime number, and let G be a solvable, transitive subgroup of S_p. Then G is a subgroup of the normalizer in S_p of a cyclic subgroup of order p.

Let f(x) be a polynomial of degree n over the field K, and assume that f(x) has roots $r_1, r_2, \dots, r_n$ in its splitting field F. The element Δ of F defined by

$$\Delta = \Pi(r_i - r_j)^2,$$

where the product is taken over all i, j with $1 \le i < j \le n$, is called the **discriminant** of f(x).

It can be shown that the discriminant of any polynomial f(x) can be expressed as a polynomial in the coefficients of f(x), with integer coefficients. This requires use of elementary symmetric functions, and lies beyond the scope of what we have chosen to cover in the book.

We have the following properties of the discriminant:

(i) $\Delta \neq 0$ if and only if f(x) has distinct roots;

(ii) Δ belongs to K;

(iii) If $\Delta \neq 0$, then a permutation in S_n is even if and only if it leaves unchanged the sign of

$$\Pi_{1 \le i < j \le n(r_i - r_j)} \ .$$

Proposition: Let f(x) be a separable polynomial over the field K, with discriminant , and let F be its splitting field over K. Then every permutation in Gal(F/K) is even if and only if is the square of some element in K.

We now restrict our attention to polynomials with rational coefficients. The next lemma shows that in computing Galois groups it is enough to consider polynomials with integer coefficients. Then a powerful technique is to reduce the integer coefficients modulo a prime and consider the Galois group of the reduced equation over the field GF(p).

Lemma: Let $f(x) = x^n + a_{n-1} x^{n-1} + \cdot \cdot \cdot + a_1 x + a_0$ be a polynomial in Q[x], and assume that $a_i = b_i / d$ for d, $b_0, b_1, \dots, b_{n-1}$ in Z.

Then $d^n f(x/d)$ is monic with integer coefficients, and has the same splitting field over Q as f(x).

If p is a prime number, we have the natural mapping $\pi : Z[x] > Z_p[x]$ which reduces each coefficient modulo p. We will use the notation $p(f(x)) = f_p(x)$.

Theorem [Dedekind]: Let f(x) be a monic polynomial of degree n, with integer coefficients and Galois group G over Q, and let p be a prime such that $f_p(x)$ has distinct roots. If $f_p(x)$ factors in $Z_p[x]$ as a product of irreducible factors of degrees $n_1, n_2, \dots, n_k$, then G contains a permutation with the cycle decomposition

$$(1,2, \dots ,n_1)\ (n_1+1, n_1+2, \dots , n_1+n_2) \cdot \cdot \cdot (n-n_k+1, \dots ,n),$$

relative to a suitable ordering of the roots.

Self Assessment

1. IF G is a .... of symmetric group sn then G is called transitive group. If it acts transitively on Set {1, 2, 3, n}

   (a) sub group (b) cyclic group

   (c) permutation group (d) finite group

2. Let P be a prime number and let G be a transitive subgroup of Sp. Then any .... normal subgroup of G is also transitive.

   (a) trivial (b) non-trivial

   (c) finite (d) infinite

3. Let P be a prime number and G be a solvable, transitive subgroup of S_p. Then G is a subgroup of the normalizer in S_p of a cyclic subgroup of order ....

   (a) P (b) G

   (c) S_p (d) S

4. If f(x) be a polynomial of degree n over the field k and assume that f(x) has roots $r_1, r_2,...r_n$ in its splitting field F. Then element Δ of F defined by

   (a) $\Delta = \Pi(r_1 - r_3)^2$ (b) $\Delta = \Pi^2(r_1 - r_j)^2$

   (c) $\Delta = (r_i - r_j)^{-2}$ (d) $\Delta = \Pi^3(r_1 - r_j)^3$

11.3 Summary

- Let f(x) be a separable polynomial over the field K, with roots $r_1, \ldots, r_n$ in its splitting field F. Then f(x) is irreducible over K if and only if Gal(F/K) acts transitively on the roots of f(x).
- Let p be a prime number, and let G be a transitive subgroup of S_p. Then any non-trivial normal subgroup of G is also transitive.
- Let p be a prime number, and let G be a solvable, transitive subgroup of S_p. Then G contains a cycle of length p.
- Let p be a prime number, and let G be a solvable, transitive subgroup of S_p. Then G is a subgroup of the normalizer in S_p of a cyclic subgroup of order p.
- Let $f(x) = x^n + a_{n-1} x^{n-1} + \cdot\cdot\cdot + a_1 x + a_0$ be a polynomial in Q[x], and assume that $a_i = b_i / d$ for d, $b_0, b_1, \ldots, b_{n-1}$ in Z.
- Then $d^n f(x/d)$ is monic with integer coefficients, and has the same splitting field over Q as f(x).
- If p is a prime number, we have the natural mapping $\pi : Z[x] > Z_p[x]$ which reduces each coefficient modulo p. We will use the notation $p(f(x)) = f_p(x)$.
- Let f(x) be a monic polynomial of degree n, with integer coefficients and Galois group G over Q, and let p be a prime such that $f_p(x)$ has distinct roots. If $f_p(x)$ factors in $Z_p[x]$ as a product of irreducible factors of degrees $n_1, n_2, \ldots, n_k$, then G contains a permutation with the cycle decomposition

  $$(1,2, \ldots ,n_1)\ (n_1+1, n_1+2, \ldots , n_1+n_2) \cdot\cdot\cdot (n-n_k+1, \ldots ,n),$$

  relative to a suitable ordering of the roots.

11.4 Keywords

Transitive Group: If G is a subgroup of the symmetric group S_n, then G is called a transitive group if it acts transitively on the set { 1, 2, ... , n }.

Separable Polynomial: Let f(x) be a separable polynomial over the field K, with roots $r_1, \ldots, r_n$ in its splitting field F. Then f(x) is irreducible over K if and only if Gal(F/K) acts transitively on the roots of f(x).

11.5 Review Questions

1. Give the order and describe a generator of the Galois group of GF (729) over GF(9).
2. Determine the Galois group of each of the following polynomials in Q[x]; hence, determine the solvability of each of the polynomials

   (a) $x^5 - 12x^2 + 2$

   (b) $x^5 - 4x^4 + 2x + 2$

   (c) $x^3 - 5$

   (d) $x^4 - x^2 - 6$

   (e) $x^5 + 1$

   (f) $(x^2 - 2)(x^2 + 2)$

   (g) $x^8 - 1$

   (h) $x^8 + 1$

   (i) $x^4 - 3x^2 - 10$
3. Find a primitive element in the splitting field of each of the following polynomials in Q[x].

   (a) $x^4 - 1$

   (b) $x^4 - 2x^2 - 15$

   (c) $x^4 - 8x^2 + 15$

   (d) $x^3 - 2$
4. Prove that the Galois group of an irreducible quadratic polynomial is isomorphic to Z_2.
5. Prove that the Galois group of an irreducible cubic polynomial is isomorphic to S_3 or Z_3.

Answers: Self Assessment

1. (a) 2. (b) 3. (a) 4. (a)

11.6 Further Readings

Books

Dan Saracino: Abstract Algebra; A First Course.

Mitchell and Mitchell: An Introduction to Abstract Algebra.

John B. Fraleigh: An Introduction to Abstract Algebra (Relevant Portion).

Online links

www.jmilne.org/math/CourseNotes/

www.math.niu.edu

www.maths.tcd.ie/

archives.math.utk.edu

Unit 12: Invariant Subfield

CONTENTS

Objectives

After studying this unit, you will be able to:

- Define G-invariant subfield
- Discuss examples related to subfield

Introduction

In the last unit, you have studied about computing Galois theory and groups. In this unit, you will get information related to fundamental theorem.

12.1 G-invariant Subfield

Proposition: Let F be a field, and let G be a subgroup of Aut(F). Then

$$\{ a \text{ in } F \mid \theta (a) = a \quad \text{for all } \theta \text{ in } G \}$$

is a subfield of F.

Definition: Let F be a field, and let G be a subgroup of Aut (F). Then

$$\{ a \text{ in } F \mid \theta (a) = a \quad \text{for all } \theta \text{ in } G \}$$

is called the **G-fixed subfield** of F, or the **G-invariant subfield** of F, and is denoted by F^G.

Proposition: If F is the splitting field over K of a separable polynomial and G = Gal(F/K), then $F^G = K$.

Lemma [Artin]: Let G be a finite group of automorphisms of the field F, and let $K = F^G$. Then

$$[F : K] \leq | G | .$$

Let F be an algebraic extension of the field K. Then F is said to be a **normal** extension of K if every irreducible polynomial in K[x] that contains a root in F is a product of linear factors in F[x].

The following conditions are equivalent for an extension field F of K:

(1) F is the splitting field over K of a separable polynomial;

(2) K = F^G for some finite group G of automorphisms of F;

(3) F is a finite, normal, separable extension of K.

If F is an extension field of K such that K = F^G for some finite group G of automorphisms of F, then G = Gal(F/K).

Example: The Galois group of GF(p^n) over GF(p) is cyclic of order n, generated by the automorphism ϕ defined by ϕ (x) = x^p, for all x in GF(p^n). This automorphism is usually known as the **Frobenius automorphism** of GF(p^n).

Let F be the splitting field of a separable polynomial over the field K, and let G = Gal(F/K).

(a) There is a one-to-one order-reversing correspondence between subgroups of G and subfields of F that contain K:

  (i) If H is a subgroup of G, then the corresponding subfield is F^H, and

$$H = \text{Gal}(F/F^H).$$

  (ii) If E is a subfield of F that contains K, then the corresponding subgroup of G is H = Gal(F/E), and

$$E = F^H.$$

(b) For any subgroup H of G, we have

$$[F : F^H] = |H| \text{ and } [F^H : K] = [G : H].$$

(c) Under the above correspondence, the subgroup H is normal if and only if the subfield E = F^H is a normal extension of K. In this case,

$$\text{Gal}(E/K) \simeq \text{Gal}(F/K)/\text{Gal}(F/E).$$

In the statement of the fundamental theorem we could have simply said that normal subgroups correspond to normal extensions. In the proof we noted that if E is a normal extension of K, then $\phi(E) \subseteq E$ for ϕ all in Gal(F/K). In the context of the fundamental theorem, we say that two intermediate subfields E_1 and E_2 are **conjugate** if there exists ϕ in Gal(F/K) such that $\phi(E_1) = E_2$. The next result shows that the subfields conjugate to an intermediate subfield E correspond to the subgroups conjugate to Gal(F/E). Thus E is a normal extension if and only if it is conjugate only to itself.

Let F be the splitting field of a separable polynomial over the field K, and let E be a subfield such that $K \subseteq E \subseteq F$, with H = Gal(F/E). If ϕ is in Gal(F/K), then

$$\text{Gal}(F/\phi(E)) = \phi H \phi^{-1}.$$

[Fundamental Theorem of Algebra]: Any polynomial in **C**[x] has a root in **C**.

Example: Prove that if F is a field extension of K and K = F^G for a finite group G of automorphisms of F, then there are only finitely many subfields between F and K.

Solution: The given condition is equivalent to the condition that F is the splitting field over K of a separable polynomial. Since we must have G = Gal (F/K), the fundamental theorem of Galois theory implies that the subfields between F and K are in one-to-one correspondence with the subgroups of F. Because G is a finite group, it has only finitely many subgroups.

Example: Let F be the splitting field over K of a separable polynomial. Prove that if Gal (F/K) is cyclic, then for each divisor d of [F:K] there is exactly one field E with K E F and [E:K] = d.

Solution: By assumption we are in the situation of the fundamental theorem of Galois theory, so that there is a one-to-one order-reversing correspondence between subfields of F that contain K and subgroups of G = Gal (F/K). Because G is cyclic of order [F:K], there is a one-to-one correspondence between subgroups of G and divisors of [F:K]. Thus for each divisor d of [F:K] there is a unique subgroup H of index d. By the fundamental theorem, $[F^H: K] = [G:H]$, and so E = F^H is the unique subfield with [E:K] = d.

Comment: Pay careful attention to the fact that the correspondence between subfields and subgroups reverses the order

Example: Let F be a finite, normal extension of Q for which | Gal (F/Q) | = 8 and each element of Gal (F/Q) has order 2. Find the number of subfields of F that have degree 4 over Q.

Solution: Since F has characteristic zero, the extension is automatically separable, and so the fundamental theorem of Galois theory can be applied. Any subfield E of F must contain Q, its prime subfield, and then [E:Q] = 4 iff [F:E] = 2, since [F:Q] = 8. Thus the subfields of F that have degree 4 over Q correspond to the subgroups of Gal (F/Q) that have order 2. Because each nontrivial element has order 2 there are precisely 7 such subgroups.

Example: Let F be a finite, normal, separable extension of the field K. Suppose that the Galois group Gal (F/K) is isomorphic to D_7. Find the number of distinct subfields between F and K. How many of these are normal extensions of K?

Solution: The fundamental theorem of Galois theory converts this question into the question of enumerating the subgroups of D_7, and determining which are normal. If we use the usual description of D_7 via generators a of order 7 and b of order 2, with $ba = a^{-1} b$, then a generates a subgroup of order 7, while each element of the form $a^i b$ generates a subgroup of order 2, for $0 \leq i < 7$. Thus there are 8 proper nontrivial subgroups of D_7, and the only one that is normal is < a >, since it has $|D_7| / 2$ elements. As you should recall from the description of the conjugacy classes of D_7 conjugating one of the 2-element subgroups by a produces a different subgroup, showing that none of them are normal.

Example: Show that $F = Q(\sqrt{2}, i)$ is normal over Q; find its Galois group over Q, and find all intermediate fields between Q and F.

Solution: It is clear that F is the splitting field over Q of the polynomial $(x^2 + 1)(x^2 - 2)$, and this polynomial is certainly separable. Thus, F is a normal extension of Q.

It follows that the Galois group is isomorphic to $Z_2 \times Z_2$. Since the Galois group has 3 proper nontrivial subgroups, there will be 3 intermediate subfields E with $Q \subset E \subset F$.

The existence of 3 nontrivial elements begins with the splitting field of x^4+1 over Q.

Comment: Recall that Z_7 is the splitting field of $x^7 - x = x(x^6 - 1)$.

Self Assessment

1. If F is field and G be a subgroup of Aut(F). Then {a in F | Q(a) = a ∀ Q in G} is called .... of F.

(a) G-invariant subfield (b) variant subfield

(c) finite field (d) domain subfield

2. G-invariant subfield is denoted by ....

(a) G^F (b) F^G

(c) F.G (d) GF^{-1}

3. G be a finite group of automorphisms of the field F and let K = FG then [F : K] .... |G|.

(a) ≥ (b) ≤

(c) = (d) ≠

4. For any subgroup H of G, we have .... and $[F^H : K] = [G : H]$

(a) $[F : F^H] = |H|$ (b) $[H^F : F] \neq |H|$

(c) $[F^{-1} : H] = |H|$ (d) $[F^{-1} : H^{-1}] \geq |H|$

5. Let F be an algebraic extensions of the field K. Then F is said to be a .... of K. If every irreducible polynomial in K[x] that contains a root in F is a product of linear factors in F[x]

(a) normal extension (b) finite extension

(c) infinite extension (d) subgroup extension

12.2 Summary

- The following conditions are equivalent for an extension field F of K:

  (1) F is the splitting field over K of a separable polynomial;

  (2) $K = F^G$ for some finite group G of automorphisms of F;

  (3) F is a finite, normal, separable extension of K.

- If F is an extension field of K such that $K = F^G$ for some finite group G of automorphisms of F, then G = Gal(F/K).

- Let F be the splitting field of a separable polynomial over the field K, and let G = Gal(F/K).

  (a) There is a one-to-one order-reversing correspondence between subgroups of G and subfields of F that contain K:

  (i) If H is a subgroup of G, then the corresponding subfield is F^H, and

  $$H = \mathrm{Gal}(F/F^H).$$

  (ii) If E is a subfield of F that contains K, then the corresponding subgroup of G is H = Gal(F/E), and

  $$E = F^H.$$

  (b) For any subgroup H of G, we have

  $$[F : F^H] = |H| \text{ and } [F^H : K] = [G : H].$$

  (c) Under the above correspondence, the subgroup H is normal if and only if the subfield $E = F^H$ is a normal extension of K. In this case,

  $$\mathrm{Gal}(E/K) \simeq \mathrm{Gal}(F/K) / \mathrm{Gal}(F/E).$$

- Let F be the splitting field of a separable polynomial over the field K, and let E be a subfield such that $K \subseteq E \subseteq F$, with $H = Gal(F/E)$. If ϕ is in Gal(F/K), then

$$Gal(F/\phi(E)) = \phi H \phi^{-1}.$$

- **[Fundamental Theorem of Algebra]** Any polynomial in C[x] has a root in C.

12.3 Keywords

Normal Extension: Let F be an algebraic extension of the field K. Then F is said to be a normal extension of K if every irreducible polynomial in K[x] that contains a root in F is a product of linear factors in F[x].

Frobenius Automorphism: The Galois group of $GF(p^n)$ over GF(p) is cyclic of order n, generated by the automorphism ϕ defined by $\phi(x) = x^p$, for all x in $GF(p^n)$. This automorphism is usually known as the Frobenius automorphism of $GF(p^n)$.

12.4 Review Questions

1. Compute each of the following Galois groups. Which of these field extensions are normal field extensions? If the extension is not normal, find a normal extension of Q in which the extension field is contained.

   (a) $G(Q(\sqrt{30})/Q)$ (b) $G(Q(\sqrt[4]{5})/Q)$

   (c) $G(Q(\sqrt{2},\sqrt{3},\sqrt{5})/Q)$ (d) $G(Q(\sqrt{2},\sqrt[3]{2},i)/Q)$

   (e) $G(Q(\sqrt{6},i)/Q)$

2. Let $F \subset K \subset E$ be field. If E is a normal extension of F, show that E must also be a normal extension of K.

3. Let G be the Galois group of a polynomial of degree n. Prove that $|G|$ divides n!.

4. Let $F \subset E$. If f(x) is solvable over F, show that f(x) is also solvable over E.

Answers: Self Assessment

1. (a) 2. (b) 3. (b) 4. (a) 5. (a)

12.5 Further Readings

Books

Dan Saracino: Abstract Algebra; A First Course.

Mitchell and Mitchell: An Introduction to Abstract Algebra.

John B. Fraleigh: An Introduction to Abstract Algebra (Relevant Portion).

Online links

www.jmilne.org/math/CourseNotes/

www.math.niu.edu

www.maths.tcd.ie/

archives.math.utk.edu

Unit 13: The Galois Group of a Polynomial

Notes

CONTENTS

Objectives

After studying this unit, you will be able to:

- Discuss the Galois group of polynomial
- Explain the theorem of Galois theory

Introduction

To study solvability by radicals of a polynomial equation f(x) = 0, we let K be the field generated by the coefficients of f(x), and let F be a splitting field for f(x) over K. Galois considered permutations of the roots that leave the coefficient field fixed. The modern approach is to consider the automorphisms determined by these permutations. We note that any automorphism of a field F must leave its prime subfield fixed.

13.1 Galois Group of Polynomial

Proposition: Let F be an extension field of K. The set of all automorphisms ϕ : F > F such that ϕ(a) = a for all a in K is a group under composition of functions.

Definition: Let F be an extension field of K. The set

$$\{\theta \text{ in Aut(F) } \mid \theta(a) = a \text{ for all a in K }\}$$

is called the **Galois group** of F over K, denoted by Gal(F/K).

Definition: Let K be a field, let f(x) be a polynomial in K[x], and let F be a splitting field for f(x) over K. Then Gal(F/K) is called the **Galois group of f(x) over K**, or the **Galois group of the equation f(x) = 0 over K**.

Proposition: Let F be an extension field of K, and let f(x) be a polynomial in K[x]. Then any element of Gal(F/K) defines a permutation of the roots of f(x) that lie in F.

Let f(x) be a polynomial in K[x] with no repeated roots and let F be a splitting field for f(x) over K. If ϕ : K > L is a field isomorphism that maps f(x) to g(x) in L[x] and E is a splitting field for g(x) over L, then there exist exactly [F:K] isomorphisms : F -> E such that (a) = (a) for all a in K.

Theorem: Let K be a field, let f(x) be a polynomial in K[x], and let F be a splitting field for f(x) over K. If f(x) has no repeated roots, then |Gal(F/K)| = [F:K].

Corollary: Let K be a finite field and let F be an extension of K with [F:K] = m. Then Gal (F/K) is a cyclic group of order m.

If we take K = $\mathbf{Z}_p$, where p is a prime number, and F is an extension of degree m, then the generator of the cyclic group Gal(F/K) is the automorphism ϕ : F -> F defined by $\phi(x) = x^p$, for all x in F. This automorphism is called the **Frobenius automorphism** of F.

A symmetric function on n variables $x_1,\ldots, x_n$ is a function that is unchanged by any permutation of its variables. In most contexts, the term "symmetric function" refers to a polynomial on n variables with this feature (more properly called a "symmetric polynomial"). Another type of symmetric functions is symmetric rational functions, which are the rational functions that are unchanged by permutation of variables.

The symmetric polynomials (respectively, symmetric rational functions) can be expressed as polynomials (respectively, rational functions) in the elementary symmetric polynomials. This is called the fundamental theorem of symmetric functions.

A function f(x) is sometimes said to be symmetric about the y-axis if f(–x) = f(x). Examples of such functions include |x| (the absolute value) and x^2 (the parabola).

13.2 Fundamental Theorem of Symmetric Functions

Any symmetric polynomial (respectively, symmetric rational function) can be expressed as a polynomial (respectively, rational function) in the elementary symmetric polynomials on those variables.

There is a generalization of this theorem to polynomial invariants of permutation groups G, which states that any polynomial invariant $f \in R[X_1,\ldots X_n]$ can be represented as a finite linear combination of special G-invariant orbit polynomials with symmetric functions as coefficients, i.e.,

$$f = \sum_{\text{r special}} p_1(\sigma_1,\ldots,\sigma_n)\,\text{orbit}_G(t),$$

where $p_1 \in R[X_1, \ldots, X_n]$,

and $\sigma_1, \ldots, \sigma_n$ are elementary symmetric functions, and $t = X_1^{e_1}, \ldots, X_n^{e_n}$ are special terms. Furthermore, any special term t has a total degree $\leq n(n-1)/2$, and a maximal variable degree $\leq n - 1$.

13.3 Symmetric Polynomial

A symmetric polynomial on n variables $x_1,\ldots, x_n$ (also called a totally symmetric polynomial) is a function that is unchanged by any permutation of its variables. In other words, the symmetric polynomials satisfy

$$f(y_1, y_2, \ldots, y_n) = f(x_1, x_2,\ldots, x_n), \qquad \ldots(1)$$

where $y_i = x_{\pi(i)}$ and π being an arbitrary permutation of the indices 1, 2, ..., n.

For fixed n, the set of all symmetric polynomials in n variables forms an algebra of dimension n. The coefficients of a univariate polynomial f(x) of degree n are algebraically independent symmetric polynomials in the roots of f, and thus form a basis for the set of all such symmetric polynomials.

There are four common homogeneous bases for the symmetric polynomials, each of which is indexed by a partition λ (Dumitriu et al., 2004). Letting l be the length of λ, the elementary functions e_λ, complete homogeneous functions h_λ, and power-sum functions p_λ are defined for l = 1 by

$$e_{\lambda_1} = \sum_{j_1 < j_2 < \ldots < j_{\lambda_1}} x_{j_1} \ldots x_{j_{\lambda\ 1}} \qquad \ldots(2)$$

$$h_{\lambda_1} = \sum_{m_1 + \ldots + mn = l1} \prod_{j=1}^{n} x^{mj} \qquad \ldots(3)$$

$$p_{\lambda_1} = \sum_{j=1}^{n} x^{\lambda_1}. \qquad \ldots(4)$$

and for l > 1 by

$$s_\lambda = \prod_{i=1}^{l} s_{\lambda_i} \qquad \ldots(5)$$

where s is one of e, h or p. In addition, the monomial functions mλ are defined as

$$m_\lambda = \sum_{\sigma \in S_\lambda} x_{\sigma\ (1)}^{\lambda_1} x_{s\ (2)}^{\lambda_2} \ldots x_{\sigma\ (m)}^{\lambda_m}, \qquad \ldots(6)$$

where S_λ is the set of permutations giving distinct terms in the sum and λ is considered to be infinite.

As several different abbreviations and conventions are in common use, care must be taken when determining which symmetric polynomial is in use.

The elementary symmetric polynomials Π_k $(x_1, \ldots, x_n)$ (sometimes denoted σ_k or e_λ) on n variables $\{x_1, \ldots, x_n\}$ are defined by

$$\Pi_1(x_1, \ldots, x_n) = \sum_{1 \le i \le n} x_i \qquad \ldots(7)$$

$$\Pi_2(x_1, \ldots, x_n) = \sum_{1 \le i \le j \le n} x_i x_j \qquad \ldots(8)$$

$$\Pi_3(x_1, \ldots, x_n) = \sum_{1 \le i \le j \le k \le n} x_i x_j x_k \qquad \ldots(9)$$

$$\Pi_4(x_1, \ldots, x_n) = \sum_{1 \le i \le j \le k \le l \le n} x_i x_j x_k x_l \qquad \ldots(10)$$

$$\vdots \qquad \ldots(11)$$

$$\Pi_5(x_1, \ldots, x_n) = \prod_{1 \le i \le n} x_i \qquad \ldots(12)$$

The kth elementary symmetric polynomial is implemented in Mathematica as Symmetric Polynomial [k, $\{x_1, \ldots, x_n\}$]. Symmetric Reduction [f, $\{x_1, \ldots, x_n\}$] gives a pair of polynomials {p, q} in $x_1, \ldots, x_n$ where is the symmetric part and is the remainder.

Alternatively, $\Pi_j(x_1,..., x_n)$ can be defined as the coefficient of x^{n-j} in the generating function $\prod_{1 \le i \le n}(x + x_i)$. ...(13)

For example, on four variables $x_1, ..., x_4$, the elementary symmetric polynomials are

$$\Pi_1(x_1, x_2, x_3, x_4) = x_1 + x_2 + x_3 + x_4 \quad ...(14)$$

$$\Pi_2(x_1, x_2, x_3, x_4) = x_1 x_2 + x_1 x_3 + x_1 x_4 + x_2 x_3 + x_2 x_4 + x_3 x_4 \quad ...(15)$$

$$\Pi_3(x_1, x_2, x_3, x_4) = x_1 x_2 x_3 + x_1 x_2 x_4 + x_1 x_3 x_4 + x_2 x_3 x_4 \quad ...(16)$$

$$\Pi_4(x_1, x_2, x_3, x_4) = x_1 x_2 x_3 x_4 \quad ...(17)$$

The power sum $S_p (x_1,..., x_n)$ is defined by

$$S_p(x_1, ..., x_n) = \sum_{k=1}^{n} x_k^p. \quad ...(18)$$

The relationship between * and $\Pi_1,...,\Pi_p$ is given by the so-called Newton-Girard formulas. The related function $s_p(\Pi_1, ..., \Pi_n)$ with arguments given by the elementary symmetric polynomials (not x_n) is defined by

$$s_p(\Pi_1,...,\Pi_n) = (-1)^{p-1} S_p (x_1,...,x_n) \quad ...(19)$$

$$= (-1)^{p-1} \sum_{k=1}^{n} x_k^p. \quad ...(20)$$

It turns out that $s_p (\Pi_1, ..., \Pi_n)$ is given by the coefficients of the generating function

$$\ln (1 + \Pi_1 t + \Pi_2 t^2 + \Pi_3 t^3 + ...) = \sum_{k=1}^{\infty} \frac{s_k}{k} t^k \quad ...(21)$$

$$= \Pi_1 t + \frac{1}{2}(-\Pi_1^2 + 2\Pi_2)t^2 + \frac{1}{3}(\Pi_1^3 - 3\Pi_1\Pi_2 + 3\Pi_3)t^3 + ...$$

so the first few values are

$$s_1 = \Pi_1 \quad ...(22)$$

$$s_2 = -\Pi_1^2 + 2\Pi_2 \quad ...(23)$$

$$s_3 = \Pi_1^3 - 3\Pi_1\Pi_2 + 3\Pi_3 \quad ...(24)$$

$$s_4 = -\Pi_1^4 + 4\Pi_1^2\Pi_2 - 2\Pi_2^2 - 4\Pi_1\Pi_3 + 4\Pi_4. \quad ...(25)$$

In general, s_p can be computed from the determinant

$$s_p = (-1)^{p-1} \begin{vmatrix} \Pi_1 & 1 & 0 & 0 & \cdots & 0 \\ 2\Pi_2 & \Pi_1 & 1 & 0 & \ddots & 0 \\ 3\Pi_3 & \Pi_2 & \Pi_1 & 1 & \ddots & 0 \\ 4\Pi_4 & \Pi_3 & \Pi_2 & \Pi_1 & \ddots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & 1 \\ p\Pi_p & \Pi_{p-1} & \Pi_{p-2} & \Pi_{p-3} & \dots & \Pi_1 \end{vmatrix} \quad ...(26)$$

(Littlewood 1958, Cadogan 1971). In particular,

$$S_1(x_1,\ldots, x_n) = \sum_{k=1}^{n} x_k = \Pi_1 \qquad \ldots(27)$$

$$S_2(x_1,\ldots, x_n) = \Pi_1^2 - 2\Pi_2 \qquad \ldots(28)$$

$$S_3(x_1,\ldots, x_n) = \Pi_1^3 - 3\Pi_1\Pi_2 + 3\Pi_3 \qquad \ldots(29)$$

$$S_4(x_1,\ldots, x_n) = \Pi_1^4 - 4\Pi_1^2\Pi_2 + 2\Pi_2^2 + 4\Pi_1\Pi_3 - 4\Pi_4 \qquad \ldots(30)$$

(Schroeppel 1972), as can be verified by plugging in and multiplying through.

13.4 Constructible Polygon

In mathematics, a **constructible polygon** is a regular polygon that can be constructed with compass and straightedge. For example, a regular pentagon is constructible with compass and straightedge while a regular heptagon is not.

Conditions for Constructibility

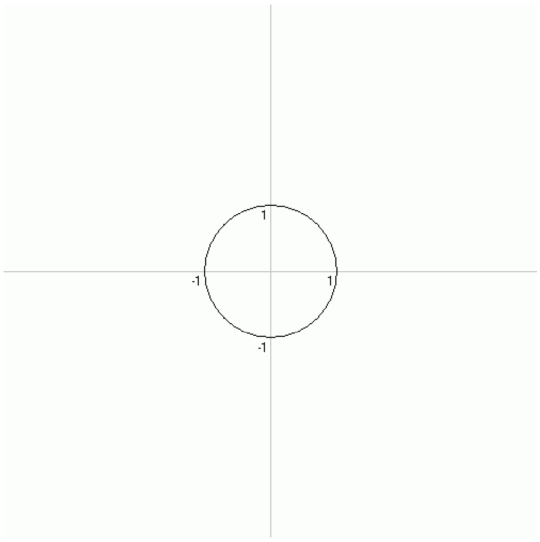
Some regular polygons are easy to construct with compass and straightedge; others are not. This led to the question being posed: is it possible to construct all regular n-gons with compass and straightedge? If not, which n-gons are constructible and which are not?

Carl Friedrich Gauss proved the constructability of the regular 17-gon in 1796. Five years later, he developed the theory of Gaussian periods in his Disquisitiones Arithmeticae. This theory allowed him to formulate a sufficient condition for the constructability of regular polygons.

A regular n-gon can be constructed with compass and straight edge if n is the product of a power of 2 and any number of distinct Fermat primes.

Gauss stated without proof that this condition was also necessary, but never published his proof. A full proof of necessity was given by Pierre Wantzel in 1837. The result is known as the **Gauss–Wantzel theorem**.

Figure 3.1



Construction of the regular 257-gon

Detailed results by Gauss' theory

Only five Fermat primes are known:

$F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, and $F_4 = 65537$ (sequence A019434 in OEIS)

The next twenty-eight Fermat numbers, F_5 through F_{32}, are known to be composite.

Thus an n-gon is constructible if

n = 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, … (sequence A003401 in OEIS),

while an n-gon is not constructible with compass and straightedge if

n = 7, 9, 11, 13, 14, 18, 19, 21, 22, 23, 25, … (sequence A004169 in OEIS).

13.5 Connection to Pascal's Triangle

There are 31 known numbers that are multiples of distinct Fermat primes, which correspond to the 31 odd-sided regular polygons that are known to be constructible. These are 3, 5, 15, 17, 51, 85, 255, 257, …, 4294967295. As John Conway commented in *The Book of Numbers*, these numbers, when written in binary, are equal to the first 32 rows of the modulo-2 Pascal's triangle, minus the top row. This pattern breaks down after there, as the 6th Fermat number is composite, so the following rows do not correspond to constructible polygons. It is unknown whether any more Fermat primes exist, and is therefore unknown how many odd-sided constructible polygons exist. In general, if there are x Fermat primes, then there are 2^{x}”1 odd-sided constructible polygons.

General Theory

In the light of later work on Galois Theory, the principles of these proofs have been clarified. It is straightforward to show from analytic geometry that constructible lengths must come from base lengths by the solution of some sequence of quadratic equations. In terms of field theory, such lengths must be contained in a field extension generated by a tower of quadratic extensions. It follows that a field generated by constructions will always have degree over the base field that is a power of two.

In the specific case of a regular *n*-gon, the question reduces to the question of constructing a length

$$\cos(2\pi/n).$$

This number lies in the n-th cyclotomic field — and in fact in its real subfield, which is a totally real field and a rational vector space of dimension

$$\tfrac{1}{2}\phi(n),$$

where $\varphi(n)$ is Euler's quotient function. Wantzel's result comes down to a calculation showing that $\varphi(n)$ is a power of 2 precisely in the cases specified.

As for the construction of Gauss, when the Galois group is 2-group it follows that it has a sequence of subgroups of orders

1, 2, 4, 8, ...

that are nested, each in the next something simple to prove by induction in this case of an abelian group. Therefore, there are subfields nested inside the cyclotomic field, each of degree 2 over the one before. Generators for each such field can be written down by Gaussian period theory.

For example for n = 17 there is a period that is a sum of eight roots of unity, one that is a sum of four roots of unity, and one that is the sum of two, which is cos(2π/17).

Each of those is a root of a quadratic equation in terms of the one before. Moreover, these equations have real rather than imaginary roots, so in principle can be solved by geometric construction: this because the work all goes on inside a totally real field.

In this way the result of Gauss can be understood in current terms; for actual calculation of the equations to be solved, the periods can be squared and compared with the 'lower' periods, in a quite feasible algorithm.

Compass and Straightedge Constructions

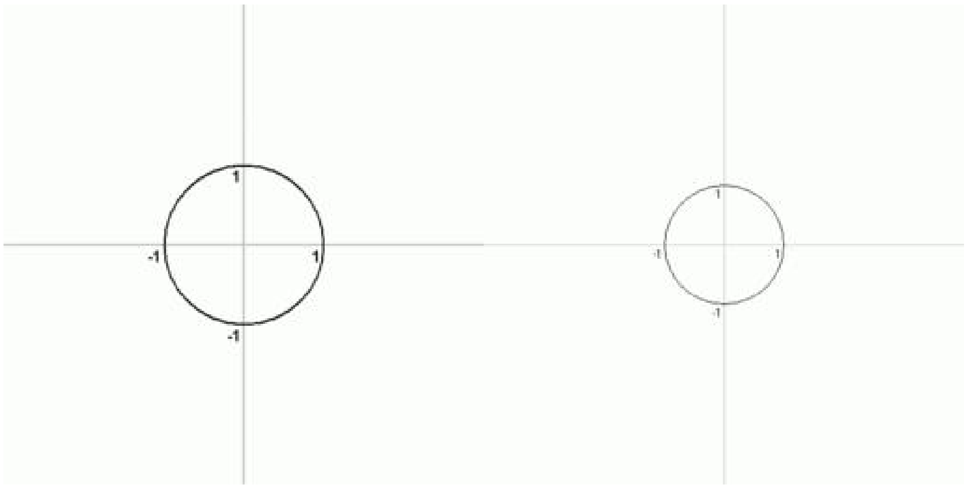
Compass and straightedge constructions are known for all constructible polygons. If $n = p \cdot q$ with p = 2 or p and q co-prime, an n-gon can be constructed from a p-gon and a q-gon.

- If p = 2, draw a q-gon and bisect one of its central angles. From this, a 2q-gon can be constructed.
- If p > 2, inscribe a p-gon and a q-gon in the same circle in such a way that they share a vertex. Because p and q are relatively prime, there exists integers a,b such that ap + bq = 1. Then $2a\pi/q + 2b\pi/p = 2\pi/pq$. From this, a p ·q-gon can be constructed.

Thus one only has to find a compass and straightedge construction for n-gons where n is a Fermat prime.

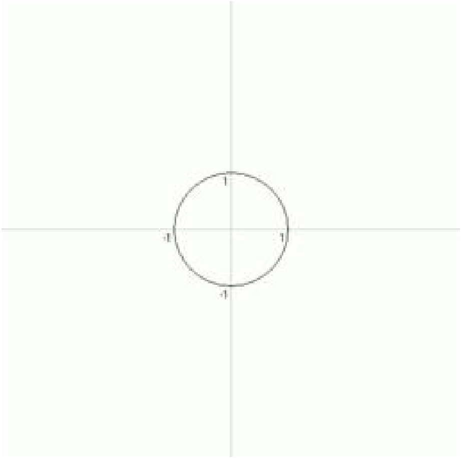
- The construction for an equilateral triangle is simple and has been known since Antiquity. Constructions for the regular pentagon were described both by Euclid and by Ptolemy.
- Although Gauss proved that the regular 17-gon is constructible, he didn't actually show how to do it. The first construction is due to Erchinger, a few years after Gauss' work.
- The first explicit construction of a regular 257-gon was given by Friedrich Julius Richelot (1832).
- A construction for a regular 65537-gon was first given by Johann Gustav Hermes (1894). The construction is very complex; Hermes spent 10 years completing the 200-page manuscript. (Conway has cast doubt on the validity of Hermes' construction, however.

Figure 13 .2



Notes

Figure 13 .3



From left to right, constructions of a 17-gon, 257-gon and 65537-gon.

Other Constructions

It should be stressed that the concept of constructible as discussed in this article applies specifically to compass and straightedge construction. More constructions become possible if other tools are allowed. The so-called neusis constructions, for example, make use of a *marked* rulers.The constructions are a mathematical idealization and are assumed to be done exactly.

Example: Determine the group of all automorphisms of a field with 4 elements.

Solution: The automorphism group consists of two elements: the identity mapping and the Frobenius automorphism.

As you know this field with 4 elements can be constructed as F = $Z_2[x]$ / < x^2+x+1 >. Letting a be the coset of x, we have F = {0, 1, a, 1+a}. Any automorphism of F must leave 0 and 1 fixed, so the only possibility for an automorphism other than the identity is to interchange a and 1+a. Is this an automorphism? Since x^2+x+1 0, we have x^2 -x-1 x+1, so a^2 = 1+a and $(1+a)^2$ = 1+2a+a^2 = a. Thus the function that fixes 0 and 1 while interchanging a and 1+a is in fact the Frobenius automorphism of F.

Example: Let F be the splitting field in C of x^4+1.

(i) Show that [F:Q] = 4.

Solution: The polynomial x^8-1 factors over Q as x^8-1 = (x^4-1)(x^4+1) = (x-1)(x+1)(x^2+1)(x^4 +1). The factor x^4 +1 is irreducible over Q by Eisenstein's criterion. The roots of x^4+1 are thus the primitive 8th roots of unity, $\pm\sqrt{2} / 2 \pm \sqrt{2} / 2i$, and adjoining one of these roots also gives the others, together with i. Thus, the splitting field is obtained in one step, by adjoining one root of x^4+1, so its degree over Q is 4.

It is clear that the splitting field can also be obtained by adjoining first $\sqrt{2}$ and then i, so it can also be expressed as Q($\sqrt{2}$, i).

(ii) Find automorphisms of F that have fixed fields Q($\sqrt{2}$), Q(i), and Q($\sqrt{2}$ i), respectively.

Solution: These subfields of Q($\sqrt{2}$, i) are the splitting fields of x^2-2, x^2+1, and x^2+2, respectively. Any automorphism must take roots to roots, so if is an automorphism of Q($\sqrt{2}$, i), we must have θ($\sqrt{2}$) = ± $\sqrt{2}$, and θ(i) = ± i. These possibilities must in fact define 4 automorphisms of the splitting field.

If we define $_1$ θ($\sqrt{2}$) = $\sqrt{2}$ and θ_1 (i) = -i, then the subfield fixed by θ_1 is Q($\sqrt{2}$). If we define θ_2($\sqrt{2}$) = – $\sqrt{2}$ and θ_2 (i) = i, then the subfield fixed by θ_2 is Q(i). Finally, for $\theta_3 = \theta_2\, \theta_1$ we have θ_3($\sqrt{2}$) = – $\sqrt{2}$ and θ(i) = –i, and thus θ_3 ($\sqrt{2}$ i) = $\sqrt{2}$ i, so θ_3 has Q($\sqrt{2}$ i) as its fixed subfield.

Example: Find the Galois groups of x^3 – 2 over the fields $\mathbf{Z}_5$ and $\mathbf{Z}_{11}$.

Solution: The polynomial is not irreducible over $\mathbf{Z}_5$, since it factors as x^3-2 = (x+2)(x^2-2x-1). The quadratic factor will have a splitting field of degree 2 over $\mathbf{Z}_5$, so the Galois group is cyclic of order 2.

A search in $\mathbf{Z}_{11}$ for roots of x^3-2 yields one and only one: x = 7. Then x^3-2 can be factored as x^3-2 = (x-7)(x^2+7x+5), and the second factor must be irreducible. The splitting field has degree 2 over $\mathbf{Z}_{11}$, and can be described as $\mathbf{Z}_{11}$[x] / < x^2+7x+5 >. Thus the Galois group is cyclic of order 2.

Example: Find the Galois group of x^4-1 over the field $\mathbf{Z}_7$.

Solution: We first need to find the splitting field of x^4-1 over $\mathbf{Z}_7$. We have x^4-1 = (x-1)(x+1)(x^2+1). A quick check of ±2 and ±3 shows that they are not roots of x^2+1 over $\mathbf{Z}_7$, so x^2+1 is irreducible over $\mathbf{Z}_7$. To obtain the splitting field we must adjoin a root of x^2+1, so we get a splitting field $\mathbf{Z}_7$[x] / < x^2+1 > of degree 2 over $\mathbf{Z}_7$.

The Galois group of x^4-1 over $\mathbf{Z}_7$ is cyclic of order 2.

Example: Find the Galois group of x^3-2 over the field $\mathbf{Z}_7$.

Solution: In this case, x^3-2 has no roots in $\mathbf{Z}_7$, so it is irreducible. We first adjoin a root a of x^3-2 to $\mathbf{Z}_7$. The resulting extension $\mathbf{Z}_7$(a) has degree 3 over $\mathbf{Z}_7$, so it has 7^3 = 343 elements, and each element is a root of the polynomial x^{343}-x. Let b> be a generator of the multiplicative group of the extension. Then $(b^{114})^3 = b^{342}$ = 1, showing that $\mathbf{Z}_7$(a) contains a non-trivial cube root of 1. It follows that x^3-2 has three distinct roots in $\mathbf{Z}_7$(a): a, ab^{114}, and ab^{228}, so therefore $\mathbf{Z}_7$(a) is a splitting field for x^3-2 over Z_7. Since the splitting field has degree 3 over Z_7, it follows the Galois group of the polynomial is cyclic of order 3.

Self Assessment

1. Galois considered .... of the roots that leave the coefficient field fixed.

   (a) polynomial (b) permutation

   (c) combination (d) range

2. The modern approach is to consider .... determined by permutation.

   (a) homomorphism (b) automorphism

   (c) isomorphism (d) ideal and subfield

Notes

3. Any automorphism of a field f must leave its prime .... fixed.

   (a) sub group (b) sub domain

   (c) sub field (d) sub range

4. Given [F : Q] is equal to ....

   (a) 7 (b) 5

   (c) 6 (d) 4

5. Automorphism of F that have fixed fields $Q(\sqrt{2}), Q(i)$ and $Q\sqrt{2}, i$ respectively.

   (a) $Q_1 = Q\sqrt{2}, Q_2 = Q(i), Q_3\sqrt{2}i = \sqrt{2}i$

   (b) $Q_1 = \sqrt{2}, Q_2 = i, Q_3\sqrt{2}i = 0$

   (c) $Q = Q_2 = Q_3$

   (d) $Q_1 = Q_2^{-1} = Q_3^{-1}$

13.6 Summary

- Let F be an extension field of K. The set of all automorphisms ϕ : F > F such that ϕ(a) = a for all a in K is a group under composition of functions.
- Let F be an extension field of K. The set

  {θ in Aut(F) | θ(a) = a for all a in K }

  is called the **Galois group** of F over K, denoted by Gal(F/K).
- Let K be a field, let f(x) be a polynomial in K[x], and let F be a splitting field for f(x) over K. Then Gal(F/K) is called the **Galois group of f(x) over K**, or the **Galois group of the equation f(x) = 0 over K**.
- Let F be an extension field of K, and let f(x) be a polynomial in K[x]. Then any element of Gal(F/K) defines a permutation of the roots of f(x) that lie in F.
- Let f(x) be a polynomial in K[x] with no repeated roots and let F be a splitting field for f(x) over K. If ϕ : K > L is a field isomorphism that maps f(x) to g(x) in L[x] and E is a splitting field for g(x) over L, then there exist exactly [F:K] isomorphisms : F -> E such that (a) = (a) for all a in K.
- Let K be a field, let f(x) be a polynomial in K[x], and let F be a splitting field for f(x) over K. If f(x) has no repeated roots, then |Gal(F/K)| = [F:K].
- Let K be a finite field and let F be an extension of K with [F:K] = m. Then Gal(F/K) is a cyclic group of order m.
- If we take K = $\mathbf{Z}_p$, where p is a prime number, and F is an extension of degree m, then the generator of the cyclic group Gal(F/K) is the automorphism ϕ : F -> F defined by $\phi(x) = x^p$, for all x in F. This automorphism is called the **Frobenius automorphism** of F.

13.7 Keywords

Galois Group: Let F be an extension field of K. The set

{θ in Aut(F) | θ(a) = a for all a in K }

is called the **Galois group** of F over K, denoted by Gal(F/K).

Galois Group of the Equation: Let K be a field, let f(x) be a polynomial in K[x], and let F be a splitting field for f(x) over K. Then Gal(F/K) is called the **Galois group of f(x) over K**, or the **Galois group of the equation f(x) = 0 over K**.

13.8 Review Questions

1. Let p be prime. Prove that there exists a polynomial f(x) ∈ Q[x] of degree p with Galois group isomorphic to S_p. Conclude that for each prime p with $p \geq 5$ there exists a polynomial of degree p that is not solvable by radicals.
2. Let p be a prime and $Z_p(t)$ be the field of rational functions over Z_p. Prove that $f(x) = x^p - t$ is an irreducible polynomial in Zp(t)[x]. Show that f(x) is not separable.
3. Let E be an extension field of F. Suppose that K and L are two intermediate fields. If there exists an element σ ∈ G(E/F) such that σ(K) = L, then K and L are said to be conjugate fields. Prove that K and L are conjugate if and only if G(E/K) and G(E/L) are conjugate subgroups of G(E/F).
4. Let σ ∈ Aut($\mathbb{R}$). If a is a positive real number, show that σ(a) > 0.
5. Let K be the splitting field of $x^3 + x^2 + 1 \in \mathbb{Z}_2[x]$. Prove or disprove that K is an extension by radicals.
6. Let F be a field such that char F ≠ 2. Prove that the splitting field of $f(x) = ax^2 + bx + c$ is $F(\sqrt{\alpha})$, where $a = b^2 - 4ac$.
7. Prove or disprove: Two different subgroups of a Galois group will have different fixed fields.
8. Let K be the splitting field of a polynomial over F. If E is a field extension of F contained in K and [E : F] = 2, then E is the splitting field of some polynomial in F[x].

Answers: Self Assessment

1. (b) 2. (b) 3. (c) 4. (d) 5. (a)

13.9 Further Readings

Books Dan Saracino: Abstract Algebra; A First Course.

Mitchell and Mitchell: An Introduction to Abstract Algebra.

John B. Fraleigh: An Introduction to Abstract Algebra (Relevant Portion).

Online links www.jmilne.org/math/CourseNotes/

www.math.niu.edu

www.maths.tcd.ie/

archives.math.utk.edu

Richa Nandra, Lovely Professional University

Unit 14: Solvability by Radicals

CONTENTS

Objectives

After studying this unit, you will be able to:

- Discuss the radical extension
- Explain that a polynomial equation is solvable by radical

Introduction

In most results, in this section we will assume that the fields have characteristic zero, in order to guarantee that no irreducible polynomial has multiple roots. When we say that a polynomial equation is solvable by radicals, we mean that the solutions can be obtained from the coefficients in a finite sequence of steps, each of which may involve addition, subtraction, multiplication, division, or taking *n*th roots. Only the extraction of an *n*th root leads to a larger field, and so our formal definition is phrased in terms of subfields and adjunction of roots of x^n-a for suitable elements a.

14.1 Radical Extension

Definition: An extension field F of K is called a **radical extension** of K if there exist elements $u_1, u_2, \ldots, u_m$ in F and positive integers $n_1, n_2, \ldots, n_m$ such that

(i) $F = K(u_1, u_2, \ldots, u_m)$, and

(ii) $u_1^{n_1}$ is in K and $u_i^{n_i}$ is in $K(u_1, \ldots, u_{i-1})$ for i = 2, ... , m .

14.2 Solvable by Radicals

For a polynomial f(x) in K[x], the polynomial equation f(x) = 0 is said to be **solvable by radicals** if there exists a radical extension F of K that contains all roots of f(x).

Proposition: Let F be the splitting field of $x^n - 1$ over a field K of characteristic zero. Then Gal(F/K) is an abelian group.

Theorem 1: Let K be a field of characteristic zero that contains all *n*th roots of unity, let a be an element of K, and let F be the splitting field of x^n-a over K. Then Gal(F/K) is a cyclic group whose order is a divisor of n.

Theorem 2: Let p be a prime number, let K be a field that contains all *p*th roots of unity, and let F be an extension of K. If [F:K] = |Gal(F/K)| = p, then F = K(u) for some u in F such that u^p is in K.

Lemma: Let K be a field of characteristic zero, and let E be a radical extension of K. Then there exists an extension F of E that is a normal radical extension of K.

Theorem 3: Let f(x) be a polynomial over a field K of characteristic zero. The equation f(x) = 0 is solvable by radicals if and only if the Galois group of f(x) over K is solvable.

S_n is not solvable for n ≥ 5, and so to give an example of a polynomial equation of degree n that is not solvable by radicals, we only need to find a polynomial of degree n whose Galois group over Q is S_n.

Lemma: Any subgroup of S_5 that contains both a transposition and a cycle of length 5 must be equal to S_5 itself.

Theorem 4: There exists a polynomial of degree 5 with rational coefficients that is not solvable by radicals

Example: Let f(x) be irreducible over Q, and let F be its splitting field over Q. Show that if Gal (F/Q) is abelian, then F = Q(u) for all roots u of f(x).

Solution: Since F has characteristic zero, we are in the situation of the fundamental theorem of Galois theory. Because Gal (F/Q) is abelian, every intermediate extension between Q and F must be normal. Therefore, if we adjoin any root u of f(x), the extension Q(u) must contain all other roots of f(x), since it is irreducible over Q. Thus Q(u) is a splitting field for f(x), so Q(u) = F.

Example: Find the Galois group of x^9-1 over Q.

Solution: We can construct the splitting field F of x^9-1 over Q by adjoining a primitive 9th root of unity to Q. We have the factorization

$$x^9-1 = (x^3-1)(x^6+x^3+1)$$

$$= (x-1)(x^2+x+1)(x^6+x^3+1).$$

Substituting x+1 in the last factor yields

$$(x+1)^6+(x+1)^3+1 = x^6+6x^5+15x^4+ 21x^3+18x^2+9x+3.$$

This polynomial satisfies Eisenstein's criterion for the prime 3, which implies that the factor x^6+x^3+1 is irreducible over Q. The roots of this factor are the primitive 9th roots of unity, so it follows that [F:Q] = 6. Gal (F/Q) is isomorphic to a subgroup of $Z_9^\times$ Since $Z_9^\times$ is abelian of order 6, it is isomorphic to Z_6. It follows that Gal (F/Q) ≃ Z_6.

Comment: The Galois group of x^n-1 over Q is isomorphic to $Z_n^\times$ and so the Galois group is cyclic of order φ(n) iff n = 2, 4, p^k, or $2p^k$, for an odd prime p.

Example: Show that $x^4-x^3+x^2-x+1$ is irreducible over Q, and use it to find the Galois group of x^{10}-1 over Q.

Solution: We can construct the splitting field F of x^{10}-1 over Q by adjoining a primitive 10th root of unity to Q. We have the factorization

$x^{10}-1 = (x^5-1)(x^5+1)$

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

Substituting x-1 in the last factor yields

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

$= (x^4-4x^3+6x^2-4x+1) - (x^3-3x^2+3x-1) + (x^2-2x+1) - (x-1) + 1$

$= x^4-5x^3+10x^2-10x+5.$

This polynomial satisfies Eisenstein's criterion for the prime 5, which implies that the factor $x^4-x^3+x^2-x+1$ is irreducible over Q.

The roots of this factor are the primitive 10th roots of unity, so it follows that [F:Q] = 4. The proof of Theorem 1 shows that Gal (F/Q) $\simeq Z_{10}^{\times}$ and so the Galois group is cyclic of order 4.

Example: Show that p(x) = x^5-4x+2 is irreducible over Q, and find the number of real roots. Find the Galois group of p(x) over Q, and explain why the group is not solvable.

Solution: The polynomial p(x) is irreducible over Q since it satisfies Eisenstein's criterion for p = 2. Since p(-2) = -22, p(-1) = 5, p(0) = 2, p(1) = –1, and p(2) = 26, we see that p(x) has a real root between -2 and -1, another between 0 and 1, and a third between 1 and 2. The derivative p′(x) = $5x^4$-4 has two real roots, so p(x) has one relative maximum and one relative minimum, and thus it must have exactly three real roots. It follows as in the proof of Theorem 2 that the Galois group of p(x) over Q is S_5, and so it is not solvable.

Self Assessment

1. Let F be splitting field of x^n – 1 over a field K of characteristic .... then G(F/K) is an abelian group.

   (a) 1 (b) 0

   (c) –1 (d) –2

2. Let K be a field of characteristic zero and let $\in$ be a .... of K. Thus there exists an extension of F of $\in$ that is normal radical extension.

   (a) radical extension (b) solvable group

   (c) Galois group (d) finite element

3. There exists a polynomial of degree .... with rational co-efficients that is not solvable by radical.

   (a) 4 (b) 5

   (c) 6 (d) 7

4. Any subgroup of S_5 that contains both a transposition and cycle of length .... must be equal to S_5 itself.

   (a) 4 (b) 5

   (c) 3 (d) 6

14.3 Summary

- An extension field F of K is called a **radical extension** of K if there exist elements $u_1, u_2, \ldots, u_m$ in F and positive integers $n_1, n_2, \ldots, n_m$ such that

  (i) $F = K(u_1, u_2, \ldots, u_m)$, and

  (ii) $u_1{}^{n}{}_1$ is in K and $u_i{}^{n}{}_i$ is in K ($u_1, \ldots, u_{i-1}$) for i = 2, ... , m .

  For a polynomial f(x) in K[x], the polynomial equation f(x) = 0 is said to be **solvable by radicals** if there exists a radical extension F of K that contains all roots of f(x).

- Let F be the splitting field of $x^n - 1$ over a field K of characteristic zero. Then Gal(F/K) is an abelian group.
- Let K be a field of characteristic zero that contains all *n*th roots of unity, let a be an element of K, and let F be the splitting field of x^n-a over K. Then Gal(F/K) is a cyclic group whose order is a divisor of n.
- Let p be a prime number, let K be a field that contains all *p*th roots of unity, and let F be an extension of K. If [F:K] = |Gal(F/K)| = p, then F = K(u) for some u in F such that u^p is in K.
- Let K be a field of characteristic zero, and let E be a radical extension of K. Then there exists an extension F of E that is a normal radical extension of K.
- Let f(x) be a polynomial over a field K of characteristic zero. The equation f(x) = 0 is solvable by radicals if and only if the Galois group of f(x) over K is solvable.
- S_n is not solvable for $n \geq 5$, and so to give an example of a polynomial equation of degree n that is not solvable by radicals, we only need to find a polynomial of degree n whose Galois group over Q is S_n.
- Any subgroup of S_5 that contains both a transposition and a cycle of length 5 must be equal to S_5 itself.
- There exists a polynomial of degree 5 with rational coefficients that is not solvable by radicals

14.4 Keywords

Radical Extension: An extension field F of K is called a **radical extension** of K if there exist elements $u_1, u_2, \ldots, u_m$ in F and positive integers $n_1, n_2, \ldots, n_m$ such that

(i) $F = K(u_1, u_2, \ldots, u_m)$

Solvable by Radicals: For a polynomial f(x) in K[x], the polynomial equation f(x) = 0 is said to be **solvable by radicals** if there exists a radical extension F of K that contains all roots of f(x).

14.5 Review Questions

1. We know that the cyclotomic polynomial

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1$$

is irreducible over $\mathbb{Q}$ for every prime p. Let w be a zero $\Phi_p(x)$, and consider the field $\mathbb{Q}(\omega)$.

(a) Show that $\omega, \omega^2, \ldots, \omega^{p-1}$ are distinct zeros of $\Phi_p(x)$, and conclude that they are all the zeros of $\Phi_p(x)$.

Notes

(b) Show that $G(\mathbb{Q}(w)/\mathbb{Q})$ is abelian of order $p - 1$.

(c) Show that the fixed field of $G(\mathbb{Q}(\omega)/\mathbb{Q})$ is $\mathbb{Q}$.

2. Let F be a finite field of characteristic zero. Let E be a finite normal extension of F with Galois group G(E/F): Prove that $F \subset K \subset L \subset E$ if and only if $\{id\} \subset G(E/L) \subset G(E/K) \subset G(E/F)$.

3. Let F be a field of characteristic zero and let $f(x) \in F[x]$ be a separable polynomial of degree n. If E is the splitting field of f(x), let $\alpha_1,...,\alpha_n$ be the roots of f(x) in E. Let $\Delta = \Pi_{i \neq j}(\alpha_i - \alpha_j)$. We define the discriminant of f(x) to be Δ^2.

(a) If $f(x) = ax^2 + bx + c$, show that $\Delta^2 = b^2 - 4ac$.

(b) If $f(x) = x^3 + px + q$, show that $\Delta^2 = -4p^3 - 27q^2$.

(c) Prove that Δ^2 is in F.

(d) If $\sigma \in G(E/F)$ is a transposition of two roots of f(x), show that $\sigma(\Delta) = -\Delta$.

(e) If $\sigma \in G(E/F)$ is an even permutation of the roots of f(x), show that $\sigma(\Delta) = \Delta$.

(f) Prove that G(E/F) is isomorphic to a subgroup of A_n if and only if $\Delta \in F$.

(g) Determine the Galois groups of $x^3 + 2x - 4$ and $x^3 + x - 3$.

Answers: Self Assessment

1. (b) 2. (a) 3. (b) 4. (b)

14.6 Further Readings

Books

Dan Saracino: Abstract Algebra; A First Course.

Mitchell and Mitchell: An Introduction to Abstract Algebra.

John B. Fraleigh: An Introduction to Abstract Algebra (Relevant Portion).

Online links

www.jmilne.org/math/CourseNotes/

www.math.niu.edu

www.maths.tcd.ie/

archives.math.utk.edu