

Algebra through examples

Or Dagmi - <http://digmi.org>

January 23, 2014

Contents

1	Introduction	5
1.1	Books	5
2	Commutative rings	7
2.1	The Axioms for a field	7
2.2	The Axioms for rings	7
2.3	Groups	8
2.4	Commutative ring	8
2.5	Quotient rings	9
2.6	Homomorphisms of rings	11
2.6.1	Homomorphism Theorem	11
2.7	Special properties of \mathbb{N}	12
2.8	Unit	13
2.9	Prime, Irreducible and Bézout's Lemma	13
2.10	Unique Factorization Domains	15
2.11	Euclidean Domains	16
2.11.1	Constructing gcds	17
3	Chinese Remainder Theorem	19
3.1	History	19
3.2	CRT in \mathbb{Z}	19
3.3	CRT for a commutative ring R	20
3.4	Proof	20
3.5	Application to Public-Key codes	22
4	Groups	23
4.1	Subgroup	23
4.2	Normal Subgroup	23
4.2.1	Quotient groups	23
4.3	Homomorphism Thm.	24
4.4	Cyclic groups	24
4.5	Lagrange's Thm.	25
4.6	Fundamental Thm. of finite abelian groups	26
5	Field Theory	27
5.1	Algebraic extension	27
5.2	Basic Extension Thm.	27

5.3	Splitting field	29
5.4	Characteristic	29
5.5	Prime field of F	30
5.5.1	Some more facts	30
5.6	Galois group	31
5.7	Separable Polynomial	32
5.8	Galois Extension	32
5.9	Cyclotomic extensions of \mathbb{Q}	35
5.9.1	Galois group of a cyclotomic field	38
5.10	Finite fields	39
5.10.1	Field's multiplicative group is cyclic	41
5.10.2	Finite fields of the same order are isomorphic	42
5.10.3	Existence of fields of order p^m	43
5.10.4	Factoring $x^n - 1$ over \mathbb{F}_p	43
6	Vector-spaces over \mathbb{F}_2 and Error-correcting codes	47
6.1	Introduction	47
6.2	Parity check digit	47
6.3	Hamming (7, 4)-code - single error correcting code.	48
6.3.1	Efficient decoding	48
6.4	Double-error correcting code - Bose-Chaudhuri-Hocquenghem code	50
7	Groups	55
7.1	$GL(n, q)$	55
7.1.1	Sylow subgroups	55
7.2	Conjugate classes in $GL(n, F)$	56
7.3	Conjugate classes in S_n	59
7.4	Solvable Groups	60
7.5	Classification of finite simple groups	61
7.5.1	The sporadic groups , the Fischer Griess Monster (1982)	62

Chapter 1

Introduction

22/10/2013

1.1 Books

1. Nathan Jacobson - Basic Algebra I & II.
2. Roger Carter - Simple groups of Lie type.
3. I.Martin Isaacs: Algebra: A Graduate Course.
4. Serge Lang: Algebra.
5. Simon Singh: The code Book.
6. John Derbyshire: An Unknown Quantity.

Chapter 2

Commutative rings

2.1 The Axioms for a field

A set F is a field if two binary operations, addition and multiplication, are defined on F so that it is closed under the operations and for all a, b and c in F :

Name	Addition	Multiplication
<u>Commutativity</u>	$a + b = b + a$	$ab = ba$
<u>Associativity</u>	$(a + b) + c = a + (b + c)$	$(ab)c = a(bc)$
<u>Existence of Identity</u>	$a + 0 = a = 0 + a$	$a \cdot 1 = a = 1 \cdot a$
<u>Existence of Inverses</u>	$a + (-a) = 0 = (-a) + a$	$aa^{-1} = 1 = a^{-1}a$ if $a \neq 0$

An axiom combining addition and multiplication:

Distributivity:

$$(a + b)c = ab + ac$$

One usually adds the axiom:

$$0 \neq 1$$

Common field examples:



Example 2.1.1 :

- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$
- $\mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_p$ (finite fields of prime order). $\{\bar{0}, \bar{1}\} = \mathbb{Z}_2$

2.2 The Axioms for rings

For rings all the above axioms, without the commutativity and existing of inverses for the multiplication exist.

A ring also doesn't have to contain a multiplication identity, a common notation for rings without identity is: Rng.

Common rings examples:

- \mathbb{Z} .
- $\mathbb{Z} \times \mathbb{Z}$ with component-wise operations $((a, b) \overset{+}{\cdot} (a', b') = \left(a \overset{+}{\cdot} a', b \overset{+}{\cdot} b' \right))$.
If R, S are rings then $R \times S$ is a ring.
- $F[x]$.

- $\mathbb{Z}[x]$.

Definition 2.2.1 A commutative ring is a ring which multiplication is commutative.

Examples:



Example 2.2.2 : Non-comm. rings:
 $M_n(F)$ - $n \times n$ matrices over a field F .
 Ring of quaternions.

2.3 Groups

If a group is multiplicative (meaning the operation is \cdot), it follow the Associativity, Existence of identity and existence of inverse.

If a group is additive, then it's a convention that the group is also commutative (abelian).

2.4 Commutative ring

Definition 2.4.1 If R is a ring and $\emptyset \neq S \subseteq R$ and S satisfies all the axioms of a ring with respect to the operations on R , $1_R \in S$, then S is a **subring**.

Definition 2.4.2 If an additive subgroup $I \subseteq R$ maintains that for every $a \in R$, $b \in I$: $a \cdot b, b \cdot a \in I$ then I is called **Ideal**.

Note that $R \cdot I \subseteq I$ and that $I \cdot R \subseteq I$.

Examples:

1. $0, R$ are trivial ideals (R is the ring).
2. Ideals in \mathbb{Z} :
 - $2\mathbb{Z}, m\mathbb{Z}$ for any $m \in \mathbb{Z}$.
 - In fact, we can show that if I ideal in \mathbb{Z} (notation: $I \triangleleft \mathbb{Z}$, $I \triangleleft R$) then $I = n\mathbb{Z}$ for some n in \mathbb{Z} .
 - If $I \neq \{0\}$ it contains a positive integer.
 - Let n be the smallest positive integer in I , if $k \in I$ we can write:

$$k = q \cdot n + r$$

where $q, r \in \mathbb{Z}$ and $0 \leq r \leq n$. But note that:

$$\underbrace{k - qn}_{\in I} = r$$

Hence $r \in I$ but is smaller than k ! Therefor $r = 0$ as n chosen to be smallest positive element of I and $k = qn$ so $I \subseteq n\mathbb{Z}$.

3. For the ring $M_2(\mathbb{R})$, The set $A = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{R} \right\}$ is a subring of $M_2(\mathbb{R})$ but **not** an ideal as: e.g.

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & * \\ 1 & * \end{pmatrix} \notin A$$

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & * \\ 1 & * \end{pmatrix} \notin A$$

For non-commutative ring R : If I is an additive subgroup s.t. $R \cdot I \subseteq I$, we say it is a left ideal. And if I is an additive subgroup s.t. $I \cdot R \subseteq I$, we say it is a right ideal.

Remarks 2.4.3 If $I \triangleleft R$, R ring and $1 \in I$ then $R = I$. In fact $1 \in I \iff R = I$.

Examples: Now, let's take a look at $B = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$. Note that:

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \begin{pmatrix} x & y \\ u & v \end{pmatrix} = \begin{pmatrix} ax + bu & ay + bv \\ 0 & 0 \end{pmatrix} \in B$$

Therefore B is a right ideal. But note that $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \notin B$, so B is not a subring. **BUT** $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ is an identity element. w.r.t multiplication in B so B is a ring but not a subring of $M_2(\mathbb{R})$.

Let's test for left ideal:

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \notin B$$

So B is not a left ideal.

Remarks 2.4.4 Fields have no non-trivial ideals. If F field, $0 \neq I \triangleleft F$ $0 \neq a \in I \subseteq F$ then $1 = a^{-1}a \in I$ so $I = F$.

Notation: The smallest **ideal** containing an element $a \in R$ defined by (a) . $aR, Ra, RaR \subseteq (a)$.

Notation: Set-theoretic multiplication R ring, $a \in R$: $Ra = \{ra \mid r \in R\}$.

A, B subsets of R : $A \cdot B = \{ab \mid a \in A, b \in B\}$.

Claim 2.4.5

If R commutative $a \in R$. $(a) = Ra$ as Ra closed under addition and is an additive subgroup and is an ideal called a principal ideal (generated by a).

2.5 Quotient rings

(comm/noncomm)

Definition 2.5.1 For any ring R , ideal I we define:

$$\begin{aligned} R/I &= \left\{ \underbrace{I + a}_{\text{cosets additive}} \mid a \in R \right\} \\ I + a &= \{b + a \mid b \in I\} \end{aligned}$$

(a is called coset representative).

Claim 2.5.2

Cosets are either equal or disjoint.

We will prove that claim in assignment 1.

Corollary 2.5.3

R/I is a partition of R .

Define operation on R/I to get a ring:

$$\begin{aligned} (I + a) + (I + b) &= I + (a + b) \\ (I + a) \cdot (I + b) &= I + a \cdot b \end{aligned}$$

This is a coset multiplication.

Remarks 2.5.4 Coset multiplication is not the same as set-theoretic multiplication.

Examples:**Example 2.5.5 :** $R = \mathbb{Z}$, $I = 2\mathbb{Z}$.

$$\begin{array}{rcl} 2\mathbb{Z} + 0 & = & 2\mathbb{Z} \\ (2\mathbb{Z} + 0) \underbrace{\cdot}_{\text{coset mult.}} (2\mathbb{Z} + 0) & = & 2\mathbb{Z} + 0 = 2\mathbb{Z} \end{array}$$

Set-theoretic multiplication:

$$2\mathbb{Z} \cdot 2\mathbb{Z} = 4\mathbb{Z}$$

Clearly they are not the same!

Remarks 2.5.6 The operations are well-defined i.e. do not depend on choice of reps.
We shall show for multiplication (addition - at home!).

Proof: $a, a' \in R$. **Proof:**

$$I + a = I + a' \iff a - a' \in I$$

$$a - a' = b \in I, a = a' + b.$$

$$I + a = I + a' + b \underbrace{=}_{\text{equality of sets!}} I + a'$$

Suppose $\begin{array}{l} I + a = I + a' \\ I + b = I + b' \end{array}$ then: $\begin{array}{l} \exists x \in I : a' = x + a \\ \exists y \in I : b' = y + b \end{array}$. By definition:

$$\begin{aligned} (I + a)(I + b) &= I + ab \\ I + a'b' &= I + (x + a)(y + b) = I + \underbrace{xy + ay + xb + ab}_{\in I} \subseteq I + ab \end{aligned}$$

By symmetry get also $I + ab \subseteq I + a'b'$ and also $I + ab = I + a'b'$. ■In R/I : I is the zero element, R/I is an additive group. $I + 1$ is the identity. ■**Examples of Quotient rings:****Example 2.5.7 :** \mathbb{Z} .

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

$$\begin{aligned} (5\mathbb{Z} + 1) + (5\mathbb{Z} + 3) &= 5\mathbb{Z} + 4 \\ (5\mathbb{Z} + 1) + (5\mathbb{Z} + 4) &= 5\mathbb{Z} \\ \underbrace{(5\mathbb{Z} + 2) \cdot (5\mathbb{Z} + 3)}_{\text{mult inverses}} &= 5\mathbb{Z} + 6 = 5\mathbb{Z} + 1 \end{aligned}$$

In fact, $\mathbb{Z}/5\mathbb{Z}$ is a field!We in fact have $\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$. $\overline{k} = k + 5\mathbb{Z}$ and operations mod 5.**Example 2.5.8 :** $F[X]$, where F is a field.

$$f(x) \in F[x].$$

$$F[x]/(f(x)) = F[x]/F[x] \cdot f(x)$$

e.g.

$$\underbrace{\mathbb{R}[x]/(x^2 - 3x + 2)}_{=I} = \{I + f(x) \mid f(x) \in \mathbb{R}[x]\}$$

$$(I + (x - 1)) \cdot (I + (x - 2)) = I + \underbrace{(x - 1)(x - 2)}_{=x^2 - 3x + 2} = I$$

2.6 Homomorphisms of rings

Definition 2.6.1 If R, S are both rings. $\varphi : R \rightarrow S$ is a **homomorphism of rings** if φ preserves the operations i.e.

$$\begin{aligned}\forall a, b \in R \quad \varphi(a) + \varphi(b) &= \varphi(a + b) \\ \forall a, b \in R \quad \varphi(a) \cdot \varphi(b) &= \varphi(a \cdot b) \\ \varphi(1_R) &= 1_S\end{aligned}$$

Remarks 2.6.2 If φ is additive and multiplication and $\varphi(1) = x \in S$ then:

$$x^2 = \varphi(1) \cdot \varphi(1) = \varphi(1 \cdot 1) = \varphi(1) = x$$

So $x^2 - x = 0 \Rightarrow x(x - 1) = 0$.

This does not always imply $x = 1$ or $x = 0$! if $x = 0$ then φ is the 0-map. If S has zero divisors $x(x - 1) = 0$ can hold also for $x \neq 0, 1$.

29/10/2013

Definition 2.6.3 Kernel: The kernel of a homomorphism φ is:

$$\ker \varphi = \{x \in R \mid \varphi(x) = 0\}$$

Remarks 2.6.4 This set is not empty, because $0 \in \ker \varphi$.

Claim 2.6.5

$\ker \varphi$ is an ideal in R .

We will prove this claim in the exercise.

Remarks 2.6.6 To prove a set is an ideal we need to:

1. Show that the set is not empty.
2. We have to prove that $R \cdot I \subseteq I$ and that $I \cdot R \subseteq I$.
3. Closed under $+$.
4. Existence of additive inverse (hence $0 \in I$).

2.6.1 Homomorphism Theorem

Definition 2.6.7 A homomorphism which is 1-1 and onto is an isomorphism.

Definition 2.6.8 Image: If φ homomorphism, the set $\text{Im} \varphi = \{\varphi(a) \mid a \in R\}$ —image of φ

Theorem 2.6.9 Homomorphism Theorem


For rings R, S .

1. If $\varphi : R \rightarrow S$ is a homomorphism of rings from R onto S then:

$$R/\ker \varphi \cong S$$


and the isomorphism is given by: $\ker \varphi + a \mapsto \varphi(a)$.

2. If $I \triangleleft R$ then the map $a \mapsto I + a$ ($\forall a \in R$) is a homomorphism of rings onto R/I and I = kernel of this homomorphism.

 **Example 2.6.10 :** $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$.

Why is it true?

We will take the homomorphism from $\mathbb{R}[x] \rightarrow \mathbb{C}$ s.t. $f(x) \in \mathbb{R}[x]$, $f(x) \mapsto f(i)$. Clearly it is surjective. Note that: $\ker \varphi = \{f \in \mathbb{R}[x] \mid f(i) = 0\} \supseteq (x^2 + 1)$. Later we will show that \subseteq as well.

 **Example 2.6.11 :** $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$.


From now on we will assume that all our rings are commutative.

Definition 2.6.12 Domain: A commutative ring R is a **domain** if $\forall a, b \in R$, $a \cdot b = 0$ implies $a = 0$ or $b = 0$.

 **Example 2.6.13 :** $\mathbb{Z}, \mathbb{R}[x]$ are domains, but $\frac{\mathbb{Z}}{6\mathbb{Z}}$ is not! and $\mathbb{Z} \times \mathbb{Z}$ is not a domain as well.

Definition 2.6.14 Principal Ideal Domain (PID): A domain R is a principal ideal domain (PID) if every ideal is principal.

i.e. of the form Ra for some $a \in R$.

 **Example 2.6.15 :** \mathbb{Z} is a PID.

$F[x]$, F field is a PID (Assignment #1).

but not $\mathbb{Z}[x]$ which is a domain.

as the ideal I = integer polynomials with even constant term $= (x, 2) = x \cdot \mathbb{Z}[x] + 2\mathbb{Z}[x]$.

Claim 2.6.16

I is not principal.

Proof: I is nonempty because $x \in I$. Assume it is principal and $f(x) \in I$ is a generator. Then:

$$f(x)\mathbb{Z}[x] = (f(x)) = I$$

So x is a multiple of $f(x)$, meaning: $g(x)f(x) = x$ for $g(x) \neq 0$. So: $1 = \deg(g(x)f(x)) \geq \deg f$. On the other hand 2 must be a multiple of $f(x)$, so: $\exists h(x) f(x)h(x) = 2$. So in fact $\deg f = 0$. and so $f(x)$ = even constant. But the cannot have $g(x) \cdot f = x$. ■

2.7 Special properties of \mathbb{N}

Euclidean property:

1. Given any $a, b > 0$ in \mathbb{N} , $\exists q, r \in \mathbb{N}$ s.t. $a = bq + r$ and $0 \leq r < b$.
2. Given any $a, b > 0$ in \mathbb{N} , there exists their greatest common divisor $d \in \mathbb{N}$ (denoted $\gcd(a, b) = (a, b)$).
 $d \mid a$ - Means a is a multiple of d .
 $d \mid b$ - Means b is a multiple of d .
 And d is greatest integer with respect to that property.
3. Unique factorization to prime numbers.

Remarks 2.7.1 In \mathbb{Z} the first property maintains.

The second one as well, only that instead of “greatest integer with respect...” we say that it is the maximum in sense that any other common divisor d' also divides d . meaning: $d' \mid a, b \Rightarrow d' \mid d$.

There is also the problem that it defines d up to a sign. Meaning that \gcd in \mathbb{Z} are unique up to a sign \pm or up to a multiple of ± 1 .

2.8 Unit

Definition 2.8.1 Unit: A “unit” is an invertible element in a ring.

Remarks 2.8.2 If $x = \varepsilon y$ and ε is a unit then: $\varepsilon^{-1}x = y$.

Proof: (in \mathbb{Z})

1. For \mathbb{N} , pick q to be largest integer s.t. $bq < a$. and then $0 \leq r = a - bq < a$.
For \mathbb{Z} we do the same thing.
2. Given $a, b \neq 0$ in \mathbb{Z} , we know that $\mathbb{Z}a + \mathbb{Z}b$ is an ideal. But \mathbb{Z} is PID, so it must be principal. so $\exists d \in \mathbb{Z} : \mathbb{Z}a + \mathbb{Z}b = \mathbb{Z}d$.
We shall show: $d = (a, b)$.

$$a = 1 \cdot a + 0 \cdot b \in \mathbb{Z}a + \mathbb{Z}b = \mathbb{Z}d \Rightarrow d \mid a$$

Similarly, $b \in \mathbb{Z}d$, so $d \mid b$.

Suppose now that d' is also a divisor of a and b . Meaning: $d' \mid a$ so $a \in \mathbb{Z}d'$ and $d' \mid b$ so $b \in \mathbb{Z}d'$. Meaning $\mathbb{Z}a \subseteq \mathbb{Z}d'$ and $\mathbb{Z}b \subseteq \mathbb{Z}d'$. Thus:

$$\mathbb{Z}d = \mathbb{Z}a + \mathbb{Z}b \subseteq \mathbb{Z}d'$$

$d \in \mathbb{Z}d'$ so $d' \mid d$. So d is gcd of a and b .

■

2.9 Prime, Irreducible and Bézout's Lemma

A consequence of this is the following lemma:

Lemma 2.9.1 Bézout's Lemma


Given $a, b \in \mathbb{Z}$. If $d = \gcd(a, b)$ then there exists $u, v \in \mathbb{Z}$ s.t. $au + bv = d$.

Remarks 2.9.2 gcds exists for any 2 elements in an PID and also Bézout's lemma as the only property of \mathbb{Z} we used was that it is a PID.

Definition 2.9.3 Prime element: If R is a ring, $p \neq 0$ not a unit in R is a **prime element** if whenever $p \mid a \cdot b$ (for $a, b \in R$) then $p \mid a$ or $p \mid b$.

Definition 2.9.4 Irreducible: If R is a ring, $x \neq 0$ not a unit in R is an **irreducible** element if whenever $x = a \cdot b$ for $a, b \in R$ then either a or b is a unit.

Remarks 2.9.5 Prime numbers in \mathbb{Z} are prime elements and also irreducible.

 **Example 2.9.6 :** Lets look at \mathbb{Z}_6 . Note that $\bar{2}$ is a prime element. If $\bar{2} \mid a \cdot b$ in \mathbb{Z}_6 so $\exists x \in \mathbb{Z}_6 : \bar{2}x = a \cdot b$. So $a \cdot b \in \{\bar{0}, \bar{2}, \bar{4}\}$ so one of a or b must be $\bar{0}, \bar{2}, \bar{4}$ and then $\bar{2} \mid a$ or $\bar{2} \mid b$. However, $\bar{2}$ is not irreducible, as we have: $\bar{2} = \bar{2} \cdot \bar{4}$ and neither $\bar{2}$ or $\bar{4}$ is a unit!

Claim 2.9.7


If R is a domain then $\text{prime} \Rightarrow \text{irreducible}$.

Remarks 2.9.8 By the above, we saw that $\text{irreducible} \not\Rightarrow \text{prime}$. Although \mathbb{Z}_6 is not a domain (it has zero divisors), but it is also true in domain.

Proof: Assume p is prime and $p = a \cdot b$ where $a, b \in R$. $p \mid ab$ so as p is prime: $p \mid a$ or $p \mid b$ wlog (without loss of generality) $p \mid a$ so $\exists u \in R$ s.t. $pu = a$. So we get:

$$p = pu \cdot b \Rightarrow p(1 - ub) = 0$$

But R is a domain so as $p \neq 0$ we must have $1 - ub = 0$, meaning $1 = ub$, so b is a unit. ■

 **Example 2.9.9 :** $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$. This is a subring of \mathbb{C} . This is a domain (as it is a subring of \mathbb{C}).

It contains irreducible that are not prime.

Remarks 2.9.10 It does contain prime elements.

Recall that for any complex number $x + iy$, $x, y \in \mathbb{R}$ we have $\|x + iy\| = \sqrt{x^2 + y^2}$ and if $z_1, z_2 \in \mathbb{C}$ we have $\|z_1\| \|z_2\| = \|z_1 z_2\|$.

In $\mathbb{Z}[\sqrt{-5}]$ if $a, b \in \mathbb{Z}$, $\|a + b\sqrt{-5}\|^2 = a^2 + 5b^2$ positive integer.

Claim 2.9.11

$\sqrt{-5}$ is a prime element in $\mathbb{Z}[\sqrt{-5}]$.

Proof: Assume $\sqrt{-5} \mid r \cdot s$ so $\exists x \in \mathbb{Z}[\sqrt{-5}]$ s.t. $\sqrt{-5}x = r \cdot s$. But:

$$5 = \|\sqrt{-5}\|^2 \mid \|r \cdot s\|^2 = \|r\|^2 \cdot \|s\|^2$$

So $5 \mid \|r\|^2$ or $5 \mid \|s\|^2$, wlog $5 \mid \|r\|^2$. Writing: $r = a + b\sqrt{-5}$ we have: $5 \mid a^2 + 5b^2$ in \mathbb{Z} , so $5 \mid a$.

So $a = 5a'$ for some $a' \in \mathbb{Z}$ and we get:

$$r = 5a' + b\sqrt{-5} = \underbrace{\sqrt{-5}(-a'\sqrt{-5} + b)}_{\text{in } \mathbb{Z}[\sqrt{-5}]}$$

So $\sqrt{-5} \mid r$. ■

Claim 2.9.12

2 is an irreducible element in $\mathbb{Z}[\sqrt{-5}]$ which is not prime.

Proof: First, we shall show that it is not a prime.

Note that: $2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.

We show $2 \nmid 1 \pm \sqrt{-5}$:

As if $2(a + b\sqrt{-5}) = 1 \pm \sqrt{-5}$ for $a, b \in \mathbb{Z}$ we would have $2a = 1$. Impossible.

We shall show 2 is **irreducible**.

Suppose $2 = r \cdot s$, where $r, s \in R$. write $r = a + b\sqrt{-5}$ where $a, b \in \mathbb{Z}$. Using complex norm:

$$4 = \|2\|^2 = \|r\|^2 \cdot \|s\|^2$$

since $\|r\|^2, \|s\|^2$ are both positive integers we must have either $\|r\|^2 = 2 = \|s\|^2$ or without loss of generality $\|r\|^2 = 1$ and $\|s\|^2 = 4$.

Let's look at the different cases:

$a^2 + 5b^2 = \|r\|^2 = 2$ - There are no $a, b \in \mathbb{Z}$ satisfying this!

So we must have $\|r\|^2 = 1, \|s\|^2 = 4$.

If $\|r\|^2 = 1$ we get $a^2 + 5b^2 = 1 \Rightarrow a = \pm 1$ and $b = 0$. So $r = \pm 1$ and it is a unit. ■

In a domain Prime \Rightarrow Irreducible but not necessarily Irreducible \Rightarrow Prime.

Claim 2.9.13

In a PID: Irreducible elements are prime.

Remarks 2.9.14 Because PID is also a domain we get Prime \iff Irreducible.

Proof: Let a be irreducible in a PID R . suppose $a \mid b \cdot c$ in R where $b, c \neq 0$.

We need to show that $a \mid b$ or $a \mid c$. Since R is a PID we have gcd. Denote $d = (a, b)$. Note that $d \mid a$ so we can write $a = da'$ where $a' \in R$. Since a is irreducible either d or a' is a unit.

Case 1: a' is a unit.

So $d = a(a')^{-1}$. so $a \mid d$, but we have $d \mid b$ then $a \mid b$.

Case 2: d is a unit.


So $dR = R$. and by Bézout: $R = aR + bR$.

$$\exists u, v \in R: 1 = au + bv \Rightarrow c = auc + bvc \quad \underbrace{\quad}_{vax=vbc} = auc + vax = a(uc + vx).$$

So $\exists x \in R$ s.t. $ax = bc$. So $a \mid c$ in R . ■

2.10 Unique Factorization Domains

Definition 2.10.1 Unique factorization domain (UFD): A domain R is a unique factorization domain (UFD) if every nonzero noninvertible element $a \in R$ can be written uniquely (up to ordering of factors and units) as a product of irreducibles.

 **Example 2.10.2 :** \mathbb{Z} (for example: $6 = (-2)(-3) = 3 \cdot 2$).
 $\mathbb{F}[x]$ (field \mathbb{F}), \mathbb{F} .

Claim 2.10.3

Any PID is a UFD.

We will prove this claim in assignment #2.

Remarks 2.10.4

1. $\mathbb{Z}[\sqrt{-5}]$ is not a UFD (or a PID). As $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. So these are two different factorizations into irreducibles.
2. $\mathbb{Z}[x]$ is a UFD. But not a PID!
 Meaning, PID \Rightarrow UFD but not the other way around.

The following claim is actually a lemma for assignment 2.

Claim 2.10.5

In a PID any increasing chain of ideals stabilizes.

i.e. given a PID R and $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$ s.t. $I_j \triangleleft R$. Then $\exists k$ s.t. $I_k = I_{k+1} = I_{k+2} = \dots$

Remarks 2.10.6 In \mathbb{Z} we have infinite properly **decreasing** chains of ideals.
 For example: $2\mathbb{Z} \supset 4\mathbb{Z} \supset 8\mathbb{Z} \supset 16\mathbb{Z} \supset \dots$

Proof: Define: $J = \bigcup_{n=1}^{\infty} I_n$. Note that $J \triangleleft R$ as if $a, b \in R$ there exists I_m, I_l s.t. $a \in I_m, b \in I_l$. wlog, if $m > l$ then $a, b \in I_m$ so $a \pm b \in I_m$, $ra \in I_m$ for any $r \in R$ etc.

Since R is PID then $\exists x \in R$ s.t. $J = Rx$. So $x \in J$. So $\exists k$ s.t. $x \in I_k$. So $J = Rx \subseteq I_k \subseteq J$. So $I_k = J$ and $I_{k+1} = I_k$ etc. ■

2.11 Euclidean Domains

Definition 2.11.1 Euclidean domains: R is a Euclidean domain if R is a domain and there exists a map (called a Euclidean norm) $\delta : R \setminus \{0\} \rightarrow \mathbb{N}$ such that for $a, b \neq 0$ in R , $\exists q, r \in R$ s.t. $a = bq + r$ and $\delta(r) < \delta(b)$ and $\delta(a) \leq \delta(a \cdot b)$ for all $a, b \neq 0$ in R (or $r = 0$).

This is Herstein's definition.



Example 2.11.2 :

1. \mathbb{Z} . where $\delta = |x|$.
2. $\mathbb{F}[x]$ where $\delta = \deg$.
3. \mathbb{F} field with $\delta(a) = 0$ for $a \neq 0$.

Claim 2.11.3

In a Euclidean domain, every 2 nonzero elements have a greatest common divisor.

Proof: The Euclid's algorithm.

Let $a, b \in R$ where $a, b \neq 0$. $b = bq_1 + r_1$. Where $\delta(r_1) < \delta(b)$ or $r_1 = 0$.

If $r_1 = 0$ then $b = \gcd(a, b)$. If not: $b = r_1q_2 + r_2$. And here $\delta(r_2) < \delta(r_1)$ or $r_2 = 0$.

If $r_2 \neq 0$ then $r_1 = r_2q_3 + r_3$ where $\delta(r_3) < \delta(r_2)$.

And so one...

If $r_k \neq 0$ for all k , we have an infinite descending sequence of positive integers because $\delta(r_1) > \delta(r_2) > \dots$ which is a contradiction. So $\exists k$ s.t. $r_k = 0$ and gcd can be shown to be r_{k-1} (if $r_1 = 0$, b is the gcd). ■



Example 2.11.4 :

1. $\mathbb{Z}[\sqrt{-5}]$ is not an Euclidean domain. As the elements $2(1 + \sqrt{-5})$ and 6 have no gcd.
2. $\mathbb{Z}[x]$ is a UFD, Not a PID. It is also not Euclidean. Every 2 elements do have a gcd. But $\mathbb{Z}[x]$ is not a Bézout ring, as $1 = (2, x)$ but have no $f(x), g(x) \in \mathbb{Z}[x]$: $1 = 2f(x) + xg(x)$.

Claim 2.11.5

If R is a Euclidean domain, then R is a PID.

Proof: Let $I \triangleleft R$. If $I \neq 0$. Let $a \in I$ be an element of minimal Euclidean norm.

It is easy to show $Ra = I$. ■



Example 2.11.6 : $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ is Euclidean. **Proof:** We choose $\delta = \|\cdot\|^2$ in \mathbb{C} then $\delta(x + yi) = x^2 + y^2 \in \mathbb{N}$. Let $0 \neq a, b \in \mathbb{Z}[i]$. We need to show $\exists q, r \in \mathbb{Z}[i]$ s.t. $a = bq + r$ and $r = 0$ or $\|r\|^2 < \|b\|^2$.

$ab^{-1} \in \mathbb{Q}[i] \subseteq \mathbb{C}$. So $\exists \alpha, \beta \in \mathbb{Q}$ s.t. $ab^{-1} = \alpha + \beta i$.

Every rational number lies at distance $\leq \frac{1}{2}$ from an integer. So, $\exists u, v \in \mathbb{Z}$ s.t. $\|u - \alpha\| \leq \frac{1}{2}$ and $\|v - \beta\| \leq \frac{1}{2}$. Let $q = u + iv$, so that:

$$\|ab^{-1} - q\| \leq \frac{1}{2}\sqrt{2} \Rightarrow \|ab^{-1} - q\|^2 \leq \frac{1}{2} \Rightarrow \left\| \underbrace{a - qb}_r \right\|^2 \leq \frac{1}{2} \|b\|^2 < \|b\|^2$$

$r = a - qb \in \mathbb{Z}[i]$. ■

Remaining question: Does $\text{PID} \Rightarrow \text{Euclidean}$?

We've seen examples of rings that are not euclidean, but they were also not PIDs.

The answer to that is actually no, But we will get back to it later.

Let's look at the following example:

 **Example 2.11.7 :** In $\mathbb{Z}[\sqrt{-5}]$, The ideal generated by 2 and $1 + \sqrt{-5}$ is non-principal.

$$I = 2\mathbb{Z}[\sqrt{-5}] + (1 + \sqrt{-5})\mathbb{Z}[\sqrt{-5}]$$

As if $a \cdot \mathbb{Z}[\sqrt{-5}] = I$ then $2 \in a\mathbb{Z}[\sqrt{-5}]$, so $a \mid 2$. But we know that 2 is irreducible. So either $a = \pm 2$ (wlog, could be 2 multiplied by invertible element) or $a = \pm 1$.

If $a = \pm 2$ then $1 + \sqrt{-5} \notin 2\mathbb{Z}[\sqrt{-5}]$ so we get a contradiction.

If $a = \pm 1$ then $I = R$ which is also a contradiction. Because we can show that there are elements which are not in I .


So as we said, PID doesn't mean that the domain is Euclidean. The counter example was found in 1949 by Motzkin. The ring $R = \mathbb{Z}\left[\frac{1}{2} + \frac{\sqrt{-19}}{2}\right]$ is a PID but not Euclidean.

Update: In 2004 it was shown that $\mathbb{Z}[\sqrt{14}]$ is Euclidean.

In fact: it is easy to show $\mathbb{Z}[\sqrt{-n}]$ is Euclidean $\iff n = 1$ or 2 .

2.11.1 Constructing gcds

1. In a Bézout(PID) ring we have $a, b \in R$: $Ra + Rb = Rd$ and $d = \gcd(a, b)$.
2. In a UFD, we factor a and b to irreducibles, then the \gcd = Product of common factors.
3. In a Euclidean domain we use Euclid's algorithm.

 **Example 2.11.8 :** $R = \mathbb{Z}\left[x, \frac{x}{2}, \frac{x}{3}, \frac{x}{4}, \dots\right] = x\mathbb{Q}[x] + \mathbb{Z}$. This is a subring of $\mathbb{Q}[x]$.

It turns out that this subring has some interesting properties.

It's clear that $R \neq \mathbb{Q}[x]$ as $\frac{1}{2} \notin R$. It's easy to prove that this is a ring.

Notice that $n \mid x$ for every integer n . Because: $x = \left(\frac{x}{n}\right) \cdot n$. Meaning that x has no decomposition into a product of irreducibles.

R is not a PID. e.g. if we take ideal I generated by $\left\{x, \frac{x}{2}, \frac{x}{3}, \dots\right\}$ ($I = x\mathbb{Q}[x]$) - it is not principal (and is not $R!$). Any polynomial will have 0 constant term.

Clearly, any element that could be a generator would have degree ≥ 1 and $\exists n$ s.t. $\frac{x}{n} \notin (f(x))$ and $\deg f \geq 1$.

Remarks 2.11.9 Any finitely generated ideal in R is principal!

R is not a UFD.

x has no factorization to irreducibles as: $n \mid x$ for all $0 \neq n \in \mathbb{Z}$. x is infinitely divisible.

12/11/2013

Summing up:

$$\text{Euclidean} \xrightarrow{\swarrow} \text{PID} \xrightarrow{\swarrow} \text{UFD}$$

Definition 2.11.10 Bézout domain: Domain in which every 2 nonzero, non-units a, b have a \gcd d , $\exists u, v$ in ring $d = au + bv$.

Remarks 2.11.11 At the last example, R is a Bézout domain.

And it maintains that:

$$\text{PID} \xrightarrow{\swarrow} \text{Bézout} \xleftarrow{\swarrow} \text{UFD}$$

Chapter 3

Chinese Remainder Theorem

3.1 History

The following problem was posed by Sunzi [Sun tsu] (4th century AD) in the book Sunzi Suanjing:

An old women goes to market and a horse steps on her basket and crashes the eggs. The rider offers to pay the damages and asks her how many eggs she had brought. She does not remember the exact number, but when she had taken them out two at a time, there was one egg left. The same happened when she picked 3, 4, 5, 6 at a time, but when she took seven at a time they came out even. What is the smallest number of eggs she could have had?

Solution: x must be $2 \pmod{3}$, $3 \pmod{5}$ and $2 \pmod{7}$

We can take $x = 23$ for example.

Oystein Ore mentions a puzzle with a dramatic element from Brahama-Sphuta-Siddhanta (Brahma's Correct System) by Brahmagupta (born 398 AD):


An old woman goes to market and a horse steps on her basket and crashes the eggs. The rider offers to pay for the damages and asks her how many eggs she had brought. She does not remember the exact number, but when she had taken them out two at a time, there was one egg left. The same happened when she picked them out three, four, five, and six at a time, but when she took them seven at a time they came out even. What is the smallest number of eggs she could have had?

3.2 CRT in \mathbb{Z}

The conditions to the Chinese Remainder Theorem in \mathbb{Z} :

Let n_1, \dots, n_k be pairwise mutually prime, i.e.: $\forall i \neq j : (n_i, n_j) = 1$.

And $r_1, \dots, r_k \in \mathbb{Z}$ be arbitrary elements. Then there exists $x \in \mathbb{Z}$ s.t. $x \equiv r_i \pmod{n_i}$ for $1 \leq i \leq k$.

 **Example 3.2.1 :** $n_1 = 3, n_2 = 5, n_3 = 14$.

$r_1 = 4, r_2 = 4, r_3 = -3$

Then:

$$\begin{aligned}x &\equiv 4 \pmod{3} \\x &\equiv 4 \pmod{5} \\x &\equiv -3 \pmod{14} \equiv 11 \pmod{14}\end{aligned}$$

So:

$$x = 25 + k \cdot 3 \cdot 5 \cdot 14 \quad \forall k \in \mathbb{Z}$$

3.3 CRT for a commutative ring R

The conditions to the Chinese Remainder Theorem in R :

Theorem 3.3.1 Chinese Remainder Theorem

Let I_1, \dots, I_n be pairwise coprime ideals in R , i.e.: $\forall k \neq j : I_k + I_j = R$.

Note that in \mathbb{Z} :

$$\mathbb{Z}_{n_i} + \mathbb{Z}_{n_j} = \mathbb{Z}$$

So these are pairwise coprime ideals. So this condition is the same for the one in \mathbb{Z} .

And $a_1, \dots, a_n \in R$ arbitrary then there exists $x \in R$:

$$x \equiv a_k \pmod{I_k} \quad \forall 1 \leq k \leq n$$

3.4 Proof

Proof:

1. For $n = 2$:

We have:

$$I_1 + I_2 = R$$

So $\exists b_j \in I_j : b_1 + b_2 = 1 \Rightarrow \begin{cases} b_1 \equiv 1 \pmod{I_2} \\ b_2 \equiv 1 \pmod{I_1} \end{cases}$. Take x to be $x = a_2 b_1 + a_1 b_2$. If we will look at $\pmod{I_1}$ of x we get:

$$x \equiv \underbrace{a_2 b_1}_{\in I_1} + a_1 b_2 = a_1 b_2 \equiv a_1 \cdot 1 \equiv a_1 \pmod{I_1}$$

And similarly:

$$x \equiv a_2 \pmod{I_2}$$

2. For arbitrary $n > 2$:

We need to define the product of ideals:

Let I and J be ideals:

$$\{ab \mid a \in I, b \in J\} = A$$

Clearly $R \cdot A \subseteq A$.

But A is not necessarily closed under addition.

Define product of ideals $I \cdot J$ = additive subgroup generated by $\{ab \mid a \in I, b \in J\}$. Then $I \cdot J$ is an ideal.



Example 3.4.1 : $I = 3\mathbb{Z}, J = 5\mathbb{Z}$. In this case, the product itself is an ideal. We get:

$$I \cdot J = 15\mathbb{Z}$$

Remarks 3.4.2 Note that we always have:

$$I \cdot J \subseteq I \cap J$$

But is it equal? In the example it is. But it's not always the case.



Example 3.4.3 : $I = 2\mathbb{Z}, J = 2\mathbb{Z}$. $I \cdot J = 4\mathbb{Z}$ but $I \cap J = 2\mathbb{Z}$.

Remarks 3.4.4 But if $p\mathbb{Z}, q\mathbb{Z}$ where p, q are distinct primes, then $p\mathbb{Z} \cdot q\mathbb{Z} = p\mathbb{Z} \cap q\mathbb{Z}$.

So, if $I_1 + I_k = R$ for all $k \geq 2$. For each $k \geq 2$ we can find $c_k \in I_1, b_k \in I_k$ s.t.:

$$c_k + b_k = 1$$

Look at:

$$1 = \prod_{k=2}^n (c_k + b_k) = \underbrace{\text{sums of multiples of } c_k}_{I_1} + \underbrace{b_2 \cdot b_3 \cdot \dots \cdot b_k}_{\in I_2 \cdot \dots \cdot I_k = J_1}$$

So I_1 and J_1 are mutually coprime ideals. Then: $\exists y_1 \in R$ $\begin{cases} y_1 \equiv 1 \pmod{I_1} \\ y_1 \equiv 0 \pmod{J_1} \end{cases}$. By the case for $n = 2$:

$y_1 \in J_1 \subseteq I_2 \cap I_3 \cap \dots \cap I_n$, So $y_1 \equiv 0 \pmod{I_k}$ for $2 \leq k \leq n$.

In a similar way for i we can show I_1 and $J_i = \prod_{k \neq i} I_k$ are mutually prime, and find $y_i \in R$ s.t.:

$$\begin{aligned} y_i &\equiv 1 \pmod{I_i} \\ y_i &\equiv 0 \pmod{J_i} \end{aligned}$$

and so also $y_i \equiv 0 \pmod{I_k} \forall k \neq i$.

Define $x = a_1 y_1 + a_2 y_2 + \dots + a_n y_n$. For any k :

$$y_i \equiv 0 \pmod{I_k} \quad \forall i \neq k$$

So:

$$x \equiv a_k y_k \pmod{I_k} \quad \underbrace{\equiv}_{y_k \equiv 1 \pmod{I_k}} \quad a_k \pmod{I_k}$$

Remarks 3.4.5 Any element of coset $x + I_1 \cdot I_2 \cdot \dots \cdot I_n$ will also satisfy all our congruences.

■

Corollary 3.4.6

Let R be a commutative ring, I_1, \dots, I_n pairwise coprime ideals.

Then:

$$R/(I_1 \cap \dots \cap I_n) \cong (R/I_1) \times \dots \times (R/I_n)$$

In particular: Let $m \in \mathbb{Z}$ and $m = p_1^{r_1} \cdot \dots \cdot p_n^{r_n}$, p_i distinct primes, $r_i \geq 1$. Then:

$$\mathbb{Z}/m\mathbb{Z} \cong (\mathbb{Z}/p_1^{r_1}\mathbb{Z}) \times \dots \times (\mathbb{Z}/p_n^{r_n}\mathbb{Z})$$

This is in fact equivalent to the CRT for \mathbb{Z} . **Proof:** We define a ring homomorphism from R onto $(R/I_1) \times \dots \times (R/I_n)$.

$$a \mapsto (I_1 + a, I_2 + a, \dots, I_n + a)$$

Check to verify this φ is a ring homomorphism.

$$\ker \varphi = \{a \mid (I_1 + a, I_2 + a, \dots, I_n + a) = (I_1, I_2, \dots, I_n)\} = I_1 \cap \dots \cap I_n$$

To show isomorphism in the corollary, it remains only to show φ is surjective (and then the corollary follows by the homomorphism theorem).

Let $(I_1 + a_1, \dots, I_n + a_n) \in (R/I_1) \times \dots \times (R/I_n)$ arbitrary $a_i \in R$. We want $a \in R$ s.t $\varphi(a) = (I_1 + a_1, \dots, I_n + a_n)$. i.e. such that:

$$\begin{aligned} I_1 + a &= I_1 + a_1 \\ I_2 + a &= I_2 + a_2 \\ &\vdots \\ I_n + a &= I_n + a_n \end{aligned}$$

But that means:

$$\begin{aligned} a &\equiv a_1 \pmod{I_1} \\ &\vdots \\ a &\equiv a_n \pmod{I_n} \end{aligned}$$

The existence of such an a is guaranteed by the CRT. ■

3.5 Application to Public-Key codes

RSA in 1976

The idea of public-key is: you encode publicly, but the decoding is secret!

Let p_1, p_2 be two “very large” primes.

Remarks 3.5.1 In 2008 a merssen prime with 12.9 million digits was the largest prime number known. This year (2013) a new prime was found with 17.4 million digits.

Let $d = p_1 \cdot p_2$. Factoring d without knowledge of p_1, p_2 is considered computationally (practically) impossible.

Let $e = (p_1 - 1)(p_2 - 1) = p_1 p_2 - p_1 - p_2 + 1 = \varphi(d)$ (Where φ is the Euler function).

Pick r to be any large integer prime to e . By Bézout, exists $s, t \in \mathbb{Z}$ s.t. $sr + te = 1$, $sr \equiv 1 \pmod{e}$.

Remarks 3.5.2 $(\mathbb{Z}/m\mathbb{Z})^*$ = Multiplicative group of units in $\mathbb{Z}/m\mathbb{Z}$.

We publish d and r but not e, p_1, p_2 and s .

Encode: $a \in \mathbb{Z}$ message and assume $a < d$. So we encode as: $a^r \pmod{d} \equiv b$

Claim 3.5.3

$$b^s \pmod{d} \equiv a$$

So decode by calculating $b^s \pmod{d}$. **Proof:**

Case 1: $(a, d) = 1$. Easy.

Case 2: $(a, d) \neq 1$

wlog assume $(a, d) = p_1$ and $(a, p_2) = 1$. And look at:

$$\mathbb{Z}/d\mathbb{Z} \cong \mathbb{Z}/p_1\mathbb{Z} \times \mathbb{Z}/p_2\mathbb{Z}$$

and use CRT.

(Leave as exercise!). ■

Remarks 3.5.4 In order to do this, we need:

Let G be a finite group, the order of $G = |G| = \#$ of elements in G . Then for all $x \in G$, $x^n = 1$.

In particular: $G = (\mathbb{Z}/p\mathbb{Z})^*$ where p is a prime ($|G| = p - 1$). Then for any $a \neq 0$ in \mathbb{Z} :

$$(a + p\mathbb{Z})^{p-1} = 1 + p\mathbb{Z}$$

or:

$$a^{p-1} \equiv 1 \pmod{p}$$

This is Fermat’s Little Theorem.

So if $d = p_1 p_2$ then:

$$(\mathbb{Z}/d\mathbb{Z})^* = \text{set of units in } \mathbb{Z}/d\mathbb{Z} = \{a + d\mathbb{Z} \mid (a, d) = 1\}$$

$$|(\mathbb{Z}/d\mathbb{Z})^*| = \varphi(d) = \# \text{ of positive integers prime to } d \text{ and smaller than } d = (p_1 - 1)(p_2 - 1) = e$$

So that for $x + d\mathbb{Z}$ in $(\mathbb{Z}/d\mathbb{Z})^*$, $(x + d\mathbb{Z})^e = 1 + d\mathbb{Z}$ by our claim. Or equivalently: $x^e \equiv 1 \pmod{d}$.

Chapter 4

Groups

4.1 Subgroup

Let H be a subgroup of a group G (Subgroup is a subset of the group G which is closed in respect to the operation of G).

$Ha, a \in G$ is a coset of H in G .

Claim 4.1.1

If $Ha \cap Hb \neq \emptyset$ then $Ha = Hb$.

Proof: If $ha = h'b \in Ha \cap Hb$ where $h, h' \in H$. Then: $(h')^{-1}ha = b$ Thus: $Ha \supseteq Hb$.

Similarly $a = h^{-1}h'b$, So $Ha \subseteq Hb$. Thus: $Ha = Hb$. ■

Remarks 4.1.2 $Ha = Hb \iff ba^{-1} \in H$. (Proof by easy verification).

4.2 Normal Subgroup

Definition 4.2.1 Normal Subgroup: A subgroup N of G is normal if $Na = aN$ for all $a \in G$.

The notation is: $N \triangleleft G$.

Equivalently we can say that $N^a = a^{-1}Na = N$ for all $a \in G$.

Remarks 4.2.2 $a \notin N$, Na is not a subgroup as $1 \notin N$. But N^a is a subgroup. It's easy to show: $(a^{-1}na)(a^{-1}n'a) = a^{-1}nn'a \in a^{-1}Na$. And the inverse is easy to show as well.

4.2.1 Quotient groups

We want to look at the set: $G/N = \{Na \mid a \in G\}$. And define an operation so it will be a group.

Definition 4.2.3 $Na \cdot Nb = Nab$.

One has to show that:

1. The operation is well defined. Meaning that if one takes different representatives, one shall receive the same cosets.
2. This multiplication defines a group called the quotient group G/N .



Example 4.2.4 : If G is commutative (=abelian), Then every subgroup is normal.

Definition 4.2.5 Simple Group: A group with no nontrivial normal subgroup ($\neq 1, G$) is called simple.

4.3 Homomorphism Thm.

Definition 4.3.1 Homomorphism: A homomorphism of group $\varphi : G \rightarrow H$ is a map sat. $\forall a, b \in G : \varphi(ab) = \varphi(a) \cdot \varphi(b)$.

Remarks 4.3.2 We can show easily that if φ is homomorphism then $\varphi(1_G) = 1_H$.

There are many homomorphism theorems, But we will only give one (The first).

Theorem 4.3.3 Homomorphism Thm

Let G, H be group and $\varphi : G \rightarrow H$ be a surjective homomorphism.

Then if $\ker \varphi = \{g \in G \mid \varphi(g) = 1_H\}$.

Then $\ker \varphi \triangleleft G$ and: $G/\ker \varphi \cong H$.

Moreover, every normal subgroups gives a homomorphism to some H .

Notation: If G/N is finite: order of the group $G/N = |G/N| = \#$ cosets of N in $G = |G : N| =$ "index of N in G ".



Example 4.3.4 :

1. $G = \text{GL}(n, F)$, F field. This is the set of $n \times n$ matrices over F of $\det \neq 0$. Called the general linear. We can define $\varphi : G \rightarrow F^*$ =multiplication group of the field $= F \setminus \{0\}$, by $\varphi(A) = \det A$. ($\varphi(AB) = \det(AB) = \det A \det B = \varphi(A) \varphi(B)$).

It's easy to see that φ is surjective as if $x \in F^*$ then we take: $\det \begin{pmatrix} x & & 0 \\ & 1 & \\ & & \ddots \\ 0 & & & 1 \end{pmatrix} = x$.

Now, note that: $\ker \varphi = \{A \in \text{GL}(n, F) \mid \det A = 1\} = \text{GL}(n, F)$ (special linear). By the homomorphism thm. $\text{SL}(n, F) \triangleleft \text{GL}(n, F)$ and:

$$\text{GL}(n, F)/\text{SL}(n, F) \cong F^*$$

2. Suppose H is a subgroup of G and $|G : H| = 2$ then $H \triangleleft G$.
If $|G : H| = 2$ there are 2 cosets, H and Ha where $a \notin H$.
So $G = H \cup Ha$ so $Ha = G \setminus H$. Similarly $G = H \cup aH$ so $aH = G \setminus H$. and so $Ha = aH$ (of course $Hh = hH = H$ for any $h \in H$).
3. $G = S_n$ symmetric group (= group of all permutations on $\{1, 2, \dots, n\}$). $\sigma \in S_n$,

$$\text{sgn}(\sigma) = \begin{cases} 1 & \text{if number of pairs of indices } i, j \text{ s.t. } i < j \text{ but } \sigma(i) > \sigma(j) \text{ is even.} \\ -1 & \text{Otherwise.} \end{cases}$$

If $\text{sgn}(\sigma) = 1$ we say σ is even, if $\text{sgn}(\sigma) = -1$ we say σ is odd

We have $\text{sgn}(\sigma\tau) = \text{sgn}\sigma \cdot \text{sgn}\tau \forall \sigma, \tau \in S_n$. Look at $\varphi : G \rightarrow \{\pm 1\}$ defined as $\varphi(\sigma) = \text{sgn}(\sigma)$. φ is onto as $\sigma(I) = 1$ and if σ switches only 1&2 then σ is odd.

So $S_n/\ker \varphi \cong \{\pm 1\}$. $\ker \varphi = \underbrace{\text{Set of even permutations}}_{A_n} \triangleleft G$ called the alternating group.

4.4 Cyclic groups

Definition 4.4.1 Cyclic group: G is a cyclic group if $\exists x \in G$ s.t.:

$$G = \{x^k \mid k \in \mathbb{Z}\} \underbrace{=}_{\text{Notation}} \langle x \rangle = \text{group generated by } x$$



Example 4.4.2 : $G = \langle \mathbb{Z}, +, 0 \rangle$ is an inf. cyclic additive group generated by 1 (or -1).

$$G = \{k \cdot 1 \mid k \in \mathbb{Z}\}$$

In fact, every cyclic infinite group is isomorphic to \mathbb{Z} .

Suppose G is infinite cyclic generated by x , define $\varphi(x) = 1$. $\varphi(x^2) = \varphi(x) + \varphi(x) = 2$ etc.

Remarks 4.4.3 $\varphi(x^k) = k$ so φ is surjective.

We note that $x^k \neq x^l$ for $k \neq l$ wlog $k > l$. As if: $x^k = x^l$ then $x^{k-l} = 1$. Then the set $\{x^n \mid n \in \mathbb{Z}\}$ would be finite. As x is an element of finite order. Which is a contradiction as G is infinite cyclic. Clearly φ is therefore also 1-1.

Remarks 4.4.4 φ is homomorphism, then φ is 1-1 $\iff \ker \varphi = \{1\}$.

In our case if $x^m \in \ker \varphi$ then $\varphi(x^m) = 0$. Then $m = 0$. So, $x^m = 1$.

Claim 4.4.5

Every subgroup H of a cyclic group G is cyclic.

Proof: Suppose that $G = \langle x \rangle$, If $H = \{1\}$ we are done. Now assume $H \neq \{1\}$.

Let k be the smallest positive integer s.t. $x^k \in H$. (If $x^n \in H$ then $x^{-n} \in H$!). Clearly $\langle x^k \rangle \in H$.

Now let $h \in H$. $\exists n \in \mathbb{Z}$ s.t. $h = x^n$. We can write: $n = kq + r$ where $0 \leq r < k$. $h = x^n = x^{kq} \cdot x^r$. But $x^{-kq}h = x^r \in H$. So by choice of k , $r = 0$ and $n = kq$ and $H \subseteq \langle x^k \rangle$. So $H = \langle x^k \rangle$ as required. ■

4.5 Lagrange's Thm.

Theorem 4.5.1 Lagrange's Thm

If G is finite, H is subgroup of G , then $|H| \mid |G|$.

Proof: For all $a \in G$, $|Ha| = |H|$. So $G =$ disjoint union of n cosets all of size $|H|$. So $|G| = n|H|$ so $|H| \mid |G|$. ■

Remarks 4.5.2 Note also: $n = |G : H|$ also divides $|G|$. And $|G : H| = \frac{|G|}{|H|}$.

Remarks 4.5.3 If $N \triangleleft G$ then $|G/N| = |G : N| = \frac{|G|}{|N|}$.

Corollary 4.5.4

If $|G| = n$ then $x^n = 1$ for all $x \in G$.

Proof: Look at $H = \langle x \rangle$. This is a subgroup of G , $m = |H| \mid |G|$ and $|H| =$ smallest k s.t. $x^k = 1$. But $m \mid n$ so $x^n = 1$. ■

From this fact we deduced Fermat's little thm:

Theorem 4.5.5 Fermat's Little Thm.

$a^{p-1} \equiv 1 \pmod{p}$ for any $(a, p) = 1$ in \mathbb{Z} .

Proof: As $|(\mathbb{Z}/p\mathbb{Z})^*| = p - 1$ ■

Claim 4.5.6

If G is finite cyclic of order n . Then, for every $k \mid n$ there exists a unique subgroup H of order k .

Remarks 4.5.7 This is not true for tributary finite groups. Or even for arbitrary abelian finite groups.

Proof: Suppose $G = \langle x \rangle$. If $k = 1$ we are done. Now assume $k > 0$. Clearly $\langle x^{\frac{n}{k}} \rangle$ is a subgroup of order k . Now suppose H is a subgroup of order k , we want to show that $H = \langle x^{\frac{n}{k}} \rangle$. By a previous claim we showed that H is cyclic, so exists $t > 0$ s.t. $H = \langle x^t \rangle$. We know that $x^{tk} = 1$, So $n \mid tk$ and $k \mid n$ is given. So $\exists k' \mid n = k \cdot k'$. Meaning: $k \cdot k' \mid t \cdot k \Rightarrow k' \mid t$. So $x^k \in \langle x^{k'} \rangle = \langle x^{\frac{n}{k}} \rangle$. Clearly $H \subseteq \langle x^{\frac{n}{k}} \rangle$. But both are finite sets of order k , so they are equal. ■

4.6 Fundamental Thm. of finite abelian groups

If we have a finite abelian group, Its structure is determined.

Theorem 4.6.1

If G is finite abelian of order n , then G is of the form: $G = C_{n_1} \times C_{n_2} \times \dots \times C_{n_k}$ where C_{n_i} is cyclic of order n_i and $\prod_{i=1}^k n_i = n$.



Example 4.6.2 : $G = C_4 \times C_2$.

Note that G has a subgroup isomorphic to C_4 and a subgroup isomorphic to $C_2 \times C_2$, both of order 4 but they are not isomorphic.

In fact, for finite abelian groups, if $k \mid |G|$, G contains a subgroup of order k .

It is easy to characterize all group of order 1,2,3,4 (It can be shown that every group of order 4 is abelian, we know that the two possibilities are $C_2 \times C_2$ and C_4), 5 (prime...), 6 (C_6 and S_3), 7 (prime).

But we want to talk about 8. We want to characterize all groups of order 8 up to isomorphism.

Abelian cases:

- C_8
- $C_4 \times C_2$
- $C_2 \times C_2 \times C_2$

Non-abelian case:

Remarks 4.6.3 In any group G , if $a^2 = 1$ for all a in the group the group is abelian.

Suppose $a, b \in G$. So $(ab)^2 = 1$. $abab = 1$. $a = a^{-1}$, $b = b^{-1}$ (as $a^2 = 1 = b^2$)

So $ab = b^{-1}a^{-1} = ba$.

Suppose now G is non-abelian of order 8. By the above, not every element satisfies $x^2 = 1$ and have no element of order 8. So, we must have an element a of order $|\langle a \rangle| = 4$ and $\langle a \rangle \triangleleft G$.

Let $b \notin \langle a \rangle$. Note that $G = \langle a, b \rangle$ as $G = N \cup Nb$.

If $b^{-1}ab = 1$ then $ab = b$ and $a = 1$ but $|\langle a \rangle| = 4$, hence a contradiction.

If $b^{-1}ab = a$ then a and b commute and G is abelian.

If $b^{-1}ab = a^2$ then $(b^{-1}ab)^2 = a^4 = 1$. But $(b^{-1}ab)^2 = b^{-1}a^2b = 1$, Hence $a^2 = 1$, contradiction.

So we are left with only: $b^{-1}ab = a^3 = a^{-1}$. Turns out that there exactly 2 options:

1. b is of order 4. Then: $G = \langle a, b \mid a^4 = 1, a^2 = b^2, b^{-1}ab = a^{-1} \rangle$ and $G \cong Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ quaternion group where $ij = k, i^2 = j^2 = k^2 = -1$.
2. b is of order 2. Then: $G = \langle a, b \mid a^4 = b^2 = 1, b^{-1}ab = a^{-1} \rangle = D_8$ dihedral group of order 8 = Group of symmetric of a square.

Chapter 5

Field Theory

5.1 Algebraic extension

Algebraic extension of fields, $F \subseteq K$ field.

Definition 5.1.1 Algebraic element: $\alpha \in K$ is algebraic over F if α is the root of a polynomial in $F[x]$.

Definition 5.1.2 Algebraic Field: K is algebraic over F if every element of K is algebraic over F .

Notation: K/F



Example 5.1.3 :

1. $\mathbb{Q} \subseteq \mathbb{C}$ - i is algebraic as a root of $x^2 + 1$.
2. $\mathbb{Q} \subseteq \mathbb{R}$ - $\sqrt{2}$ is algebraic over \mathbb{Q} , root of $x^2 - 2$, and any element in \mathbb{Q} is algebraic over \mathbb{Q} , root of $x - r$.
 $\alpha = \sqrt[3]{7 + \sqrt[17]{8}}$ algebraic over \mathbb{Q} .

$$\alpha^3 = 7 + \sqrt[17]{8} \Rightarrow \alpha^3 - 7 = \sqrt[17]{8} \Rightarrow (\alpha^3 - 7)^{17} = 8$$

But note that $(x^3 - 7)^{17} - 8$ is polynomial over \mathbb{Z} and α is a root.

Definition 5.1.4 Transcendental Element: Any element which is not algebraic, is called transcendental.



Example 5.1.5 : Famous examples for transcendental elements in \mathbb{R} are: π, e (Proof: Lindemann's thm.).

For any α over F , we can construct $F(\alpha)$ =smallest field containing F and α . $F[\alpha]$ =smallest ring that contains F and α .

If α is transcendental over F :

$$f(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} \mid f, g \in F[\alpha] \right\} = \text{field of rational functions in } \alpha.$$

In Assignment #3 we will prove the following claim:

Claim 5.1.6

$F(\alpha) = F[\alpha] \iff \alpha \text{ is algebraic over } F.$

5.2 Basic Extension Thm.

Theorem 5.2.1 Basic extension thm.

Let $p(x) \in F[x]$ be irreducible, Then there exists a field $K \supset F$ in which $p(x)$ has a root. If K is a minimum w.r.t this property, then K is unique up to isomorphism.

Proof: Let $K = F[u]/p(u)F[u]$, u is indeterminate variable.

We can regard $F \subseteq K$ by identifying elements a of F with $a + (p(u))$.

Denote $I = (p(u))$

K is a field, because suppose we have $g(u) = F[u]$, $g(u) \notin I$ so $(g(u), p(u)) = 1$. By Bézout, we have $r(u), s(u)$ such that:

$$g(u)r(u) + p(u)s(u) = 1$$

Then:

$$(g(u) + I)(r(u) + I) = 1 + I$$

So $g(u) + I$ has an inverse in K .

So K is a field as required. We now want to show that p as a root in K . Look at:

$$p(x) = \sum a_i x^i \quad a_i \in F$$

We show that $u + I$ is a root of $p(x)$.

$$p(u + I) = \sum a_i (u + I)^i = \underbrace{\sum a_i u^i}_{p(u)} + I = I \equiv 0 \text{ in } K$$

As required. It remains to show that K is unique up to isomorphism.

Suppose $K \supseteq F$ field and $\exists c \in L$ s.t. $p(c) = 0$. Construct a map from $K \rightarrow L$ as follows:

$$g(u) + I \mapsto g(c)$$

For any $g \in F[u]$. $g(c) \in L$ because $L \supseteq F$ and the coefficients of g are in F .

We need to show that this map is well-defined and that it is a field monomorphism. We will show that it is well-defined:

Suppose $g(u) + I = g'(u) + I$, then $g(u) - g'(u) \in I$ and so it is a multiple of $p(u)$. So $g(c) - g'(c) = p(c) \cdot (\dots) = 0$. Meaning: $g(c) = g'(c)$. ■

 **Example 5.2.2 :** $\mathbb{Q}[x]/(x^2-2) = \mathbb{Q}(\sqrt{2})$

In fact, it is easy to show here that $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}]$. For any polynomial $f \in \mathbb{Q}[x]$ have:

$$f(x) = q(x)(x^2 - 2) + r(x)$$


(deg $r \leq 1$).

So $f(x) + I = r(x) + I$. So we map $ax + b + I \xrightarrow[\phi]{\cong} a\sqrt{2} + b$, where $a, b \in \mathbb{Q}$.

$$\varphi[(ax + b + I)(cx + d + I)] = \varphi[acx^2 + (ad + bc)x + bd + I] \equiv_{\text{mod } I} \varphi[(ad + bc)x + (2ac + bd) + I]$$

$$(a\sqrt{2} + b)(c\sqrt{2} + d) = 2ac + bc\sqrt{2} + ad\sqrt{2} + bd = \varphi(\text{RHS})$$


Remarks 5.2.3 $\mathbb{Q}(\sqrt{2})$ contains both roots of $x^2 - 2$, so $x^2 - 2$ factors completely over $\mathbb{Q}(\sqrt{2})$. By field theory, there is no difference between $\sqrt{2}$ and $-\sqrt{2}$, we could use both just the same.

 **Example 5.2.4 :** $\mathbb{R}/(x^2+1) \cong \mathbb{C}$.

5.3 Splitting field

Definition 5.3.1 Splitting Field: A *splitting field* for a polynomial $f(x) \in F[x]$ is the minimal field extension of F over which $f(x)$ factors to linear factors.

In the previous sections, we show two samples of a splitting fields. We will see an example of an extension which is not splitting field:

 **Example 5.3.2 :** Look at $x^3 - 2$ over \mathbb{Q} . Construct: $K = \mathbb{Q}[x]/(x^3 - 2)$ contains a root of $x^3 - 2$: $\sqrt[3]{2}$. Assume this is the real root. We want to factor over K :

$$x^3 - 2 = (x - \sqrt[3]{2}) (x^2 + \sqrt[3]{2}x + \sqrt[3]{2}^2)$$

But the second term, $(x^2 + \sqrt[3]{2}x + \sqrt[3]{2}^2)$, is irreducible over K as the remaining 2 roots are non-real.

$$\frac{-\sqrt[3]{2} \pm \sqrt{(\sqrt[3]{2})^2 - 4(\sqrt[3]{2})^2}}{2} = \frac{-\sqrt[3]{2} \pm i\sqrt[3]{2}\sqrt{3}}{2} \notin K$$

So K is not a splitting field for $x^3 - 2$.

We can do the extension once more, and get an splitting field of the polynomial.

Theorem 5.3.3

Given a polynomial $f(x)$ over a field F , there exists an extension field K of F which is a splitting field for $f(x)$ and it is unique up to isomorphism.

Proof: If $f(x)$ factors completely over F , then F is a s.f. (splitting field).

Using the **Basic Extension Thm**, extend F (if necessary) to K_1 , containing root a_1 of $f(x)$ and then over K_1 : $f(x) = (x - a_1) f_1(x)$, where $f_1(x) \in K_1[x]$ and $\deg f_1 < \deg f$.

Repeat until we have a full factorization of $f(x)$, since $\deg f$ is finite, the process is finite. ■

Remarks 5.3.4 In the proof we used the fact that if $f(a) = 0$ then $(x - a) \mid f(x)$.

Over a field F , a is a root of $f(x) \iff x - a \mid f(x)$ over F . This follows from dividing $f(x)$ by $x - a$ with remainder:

$$f(x) = q(x)(x - a) + r$$

But r is a constant because $0 = f(a) = q(a)(a - a) + r \Rightarrow r = 0$.

By consideration of degree, it follows that the number of roots of $f(x) \leq \deg f$.

Over rings, we can have polynomials with more roots than the degree, we will see it in future assignment.

5.4 Characteristic

Definition 5.4.1 Characteristic: In a field F , if $\exists n \in \mathbb{N}$, $n > 0$ s.t.

$$\underbrace{1 + \cdots + 1}_{n \text{ times}} = 0$$

We say F has *finite characteristic*.

It is easy to show that the smallest such n must be prime:

Lemma 5.4.2

The characteristic of F , $\text{char} F$, is a prime number.

Proof: If $n = mk$, $1 < m$, $k < n$

$$\underbrace{(1 + \dots + 1)}_{m \text{ times}} \underbrace{(1 + \dots + 1)}_{k \text{ times}} = \underbrace{1 + \dots + 1}_{n \text{ times}} = 0$$

So $\underbrace{(1 + \dots + 1)}_{m \text{ times}} = 0$ or $\underbrace{(1 + \dots + 1)}_{n \text{ times}} = 0$ contradiction of minimality of n . ■

If no such n exists we say F is of characteristic 0.

5.5 Prime field of F

Denote F_0 = smallest subfield contained in F = intersection of all subfields of F . $0, 1 \in F_0$.

$$\begin{aligned} 1 + 1 &\in F_0 \\ 1 + 1 + 1 &\in F_0 \\ 1 + 1 + 1 + 1 &\in F_0 \end{aligned}$$

Notation: $\overline{n} = \underbrace{1 + \dots + 1}_{n \text{ times}} \in F$.

Case 1: $\text{char} F = 0$. In that case: $\overline{n} \neq \overline{m}$ for all $n \in \mathbb{N}$, so F_0 contains a copy of \mathbb{N} . Similarly $-\overline{n} \in F_0$ for all $n \in \mathbb{N}$ so F_0 contains a copy of \mathbb{Z} .

Similarly, F_0 must contain all elements of type $n, m \in \mathbb{N}$, $m \neq 0$, $\overline{n} \overline{m}^{-1}$. So $F_0 \cong \mathbb{Q}$.

Case 2: $\text{char} F = p$ where p is a prime. Look at:

$$\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \dots, \overline{p-1}\} \subseteq F_0$$

It is easy to show that:

$$\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \dots, \overline{p-1}\} \cong \mathbb{Z}/p\mathbb{Z}$$

e.g.

$$(1 + 1)(1 + 1 + 1) = (1 + 1 + 1 + 1 + 1 + 1)$$

$$\overline{2} \cdot \overline{3} = \overline{6}$$

Distributivity.

Corollary 5.5.1

Every field contains a prime field isomorphic either to \mathbb{Q} or to $\mathbb{Z}/p\mathbb{Z}$ for some prime p .

5.5.1 Some more facts

Definition 5.5.2 If α is algebraic over a field F , Then the monic polynomial of minimal degree, $p(x) \in F[x]$ s.t. α is a root of p is called the minimal polynomial of α .

- Minimal polynomials are unique and irreducible.

Lemma 5.5.3

If α is a root of $f(x) \in F[x]$, then $p(x) \mid f(x)$ over F .

Proof: If we write:

$$f(x) = p(x)q(x) + r(x)$$

Then: $\deg r < \deg p$ or $r \equiv 0$. Substitute α and we get:

$$0 = f(\alpha) = p(\alpha)q(\alpha) + r(\alpha)$$

So α is a root of $r(x)$ - contradicting the minimality of degree of $p(x)$. So $r = 0$ and $p(x) \mid f(x)$. ■

Claim 5.5.4

If $p(x) \in F[x]$ irreducible. $K = F[x]/(p(x))$, Then K is a vector space of dimension $\deg p(x)$ over F .

Remarks 5.5.5 In general, if $F \subseteq K$ fields, then K is a vector space over F . The main concept here is that the dimension of K over F is $\deg p(x)$.

Remarks 5.5.6 $p(x)$ is minimal polynomial of $x + I$ ($I = (p(x))$) over F .

Proof: The cosets determined by $1, x, x^2, \dots, x^{n-1}$ are linear independent over F and span K . ■

Notation: $[K : F] = \dim$ of K over F as a vector space.

Corollary 5.5.7

If $F \subseteq K$ fields and $[K : F] = \text{finite}$. Then K/F is an algebraic extension.

Proof: Let $\alpha \in K$, Look at the set:

$$1, \alpha, \alpha^2, \alpha^3, \dots$$

As $[K : F] = n$, then $1, \alpha, \alpha^2, \alpha^3, \dots, \alpha^n$ must be linear dependent set over F . i.e. $\exists a_i \in F$ not all 0 s.t.

$$\sum_{i=0}^n a_i \alpha^i = 0$$

and then α is a root of $\sum a_i x^i$. ■

5.6 Galois group

Definition 5.6.1 If $K \supseteq F$ fields,

$\text{Gal}(K/F) = \text{Galois group of } K \text{ over } F = \text{Set of all automorphisms of } K \text{ that fix every element of } F$

$\varphi : K \rightarrow K$ automorphism. $\varphi(a) = a, \quad \forall a \in F$.

$\text{Gal}(K/F)$ is a group.



Example 5.6.2 : $\varphi \in \text{Gal}(\mathbb{C}/\mathbb{R})$ then:

$$\varphi(a + ib) = \varphi(a) + \varphi(i)\varphi(b)$$

But φ fixes \mathbb{R} element-wise then:

$$= a + \varphi(i)b$$

But what $\varphi(i)$ equals to? Note that:

$$\varphi(i)\varphi(i) = \varphi(i^2) = \varphi(-1) = -1$$

So $\varphi(i)$ is a square root of -1 , hence $\varphi(i) = \pm i$.

If $\varphi(i) = i$ then $\varphi = \text{Id}$. If $\varphi(i) = -i$ then $\varphi = \text{Complex conjugation}$.

$$z \mapsto \overline{z}$$

$\text{Gal}(\mathbb{C}/\mathbb{R}) \cong C_2 = \langle \psi \rangle, \psi^2 = \text{Id}$.

5.7 Separable Polynomial

Galois group of polynomial over a field \mathbb{F} = Galois group of the s.f. of the polynomial over \mathbb{F} .

 **Example 5.7.1 :** $x^3 - 2$ over \mathbb{Q} , The splitting field is $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$ because the roots (other than $\sqrt[3]{2}$) are:

$$\sqrt[3]{2} \left(\frac{-1 \pm i\sqrt{3}}{2} \right)$$

The Galois group of $x^3 - 2$ over \mathbb{Q} is: $\text{Gal}(\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})/\mathbb{Q})$.

Galois theory gives a 1-1 correspondence between “**normal** subfields” of K/F (algebraic extension) and a normal subgroup of $\text{Gal}(K/F)$.

Definition 5.7.2 Separable polynomial: A polynomial is called separable if its irreducible factors have distinct roots.

Remarks 5.7.3 This is always the case in char 0 but not in char p . An example will be in assignment 4.


5.8 Galois Extension

Definition 5.8.1 Galois Extension: A Galois Extension of a field is an algebraic extension which is the splitting field of a separable polynomial.

Theorem 5.8.2 Galois

If E/F is a Galois Extension then:

$$|\text{Gal}(E/F)| = |E : F| = \dim_F E$$

 **Example 5.8.3 :** $E = \mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$, $F = \mathbb{Q}$.

$|E : \mathbb{Q}| = |E : \mathbb{Q}(\sqrt[3]{2})| |\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}|$, But we already know that: $|\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}| = 3$. But what is: $|E : \mathbb{Q}(\sqrt[3]{2})|$? We know that $\pm i\sqrt{3}$ are the roots of $x^2 + 3$ which is irreducible over $\mathbb{Q}(\sqrt[3]{2})$, Thus: $|E : \mathbb{Q}(\sqrt[3]{2})| = 2$. So:

$$|\text{Gal}(\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})/\mathbb{Q})| = 6$$

Remarks 5.8.4 If φ is an automorphism of E then $\varphi(2) = 2$ (because $2 \in \mathbb{Q}$, and we are talking about automorphisms that fix every element of \mathbb{Q}). So if $\varphi(\sqrt[3]{2}) = \xi$, then: $\varphi(2) = (\varphi(\sqrt[3]{2}))^3 = \xi^3$. In other words: ξ must be one of the cubed root of 2 in E : $\sqrt[3]{2}$ or $\sqrt[3]{2} \left(\frac{-1 \pm i\sqrt{3}}{2} \right)$. So φ permutes these roots.

There are 3 roots and 6 automorphisms, and the image of the roots fixed automorphism (as every element is a polynomial in the 3 roots with coefficients in \mathbb{Q}) \Rightarrow The automorphisms group must therefore be the full group of permutations on the 3 roots. Thus: $\text{Gal}(E/F) \cong S_3$.

Claim 5.8.5

If φ is an automorphism of some extension field of \mathbb{Q} , then φ fixes \mathbb{Q} element-wise.

Proof: $\varphi(1) = 1$, so $\varphi(1+1) = 1+1 = 2$. Inductively $\varphi(n) = n$ for all $n \in \mathbb{N}$. By the additivity of homomorphisms. But also: $\varphi(-n) = -\varphi(n) = -n$ (as $\varphi(n + (-n)) = \varphi(0) = 0$) so φ fixes \mathbb{Z} element-wise.

For $0 \neq n \in \mathbb{Z}$, $\varphi(n^{-1}) = \varphi(n)^{-1}$ (as $1 = \varphi(1) = \varphi(n^{-1}n) = \varphi(n^{-1})\varphi(n)$). So for $\frac{p}{q} \in \mathbb{Q}$ for $p, q \neq 0 \in \mathbb{Z}$ we get:

$$\varphi\left(\frac{p}{q}\right) = \frac{\varphi(p)}{\varphi(q)} = \frac{p}{q}$$

Similarly, if φ automorphism of an extension of $\mathbb{Z}/p\mathbb{Z}$, it fixes $\mathbb{Z}/p\mathbb{Z}$ element-wise. ■

Claim 5.8.6

K, F are fields, If $f(x) \in F[x]$ and $K \supseteq F$ contains a root of F . Then $\text{Gal}(K/F)$ permutes the roots of f in K .

Proof: Suppose α is a root of f in K and $\varphi \in \text{Gal}(K/F)$, $f(\alpha) = 0$ so $\varphi(f(\alpha)) = 0$.


But note that if $f(x) = \sum a_i x^i$, then:


$$\varphi(f(\alpha)) = \varphi\left(\sum a_i \alpha^i\right) \underset{\text{Additivity}}{=} \sum \varphi(a_i \alpha^i) \underset{\text{Fixing } F}{=} \sum a_i \varphi(\alpha^i) = \sum a_i \varphi(\alpha)^i$$

So $\varphi(\alpha)$ is a root of f . ■

Corollary 5.8.7

If K is a s.f. of some polynomial $f(x)$ over F then as K is generated over F by roots of $f(x)$ and these roots are permuted by $\text{Gal}(K/F)$, we have that the images of the roots determine the automorphisms. And $\text{Gal}(K/F)$ can be considered a subgroup of the group of permutations on the set of roots.

 **Example 5.8.8 :** $\varphi \in \text{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$, The elements of $\mathbb{Q}(\sqrt[3]{2})$ are of the form: $a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2$ for $a, b, c \in \mathbb{Q}$. But $\varphi(\sqrt[3]{2}) = \sqrt[3]{2}$ as $\mathbb{Q}(\sqrt[3]{2})$ contains only one root of $x^3 - 2$. So $\varphi = \text{Id}$.

 **Example 5.8.9 :** $f(x) = x^4 - 2$ over \mathbb{Q} .
The roots are: $\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}$. (We can write: $x^4 - 2 = (x^2 - \sqrt{2})(x^2 + \sqrt{2})$, The first two roots are the roots of the first term, and the later are for the second term).
The s.f. is $E = \mathbb{Q}(\sqrt[4]{2}, i)$.

$$|E : \mathbb{Q}| = \overbrace{\left[E : \mathbb{Q}(\sqrt[4]{2}) \right]}^2 \cdot \overbrace{\left[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q} \right]}^4 = 8$$

$x^2 + 1$ is irreducible over $\mathbb{Q}(\sqrt[4]{2})$ and E is it's s.f. $x^4 - 2$ is irreducible over \mathbb{Q}

$\text{Gal}(E/\mathbb{Q})$ is isomorphic to a subgroup of S_4 .

S_4 contains no element of order 8, so $\text{Gal}(E/\mathbb{Q}) \not\cong C_8$.

 **Example 5.8.10 :** Let φ be the complex conjugation. So $\varphi \in \text{Gal}(E/F)$. $\varphi^2 = \text{Id}$.

$$\begin{aligned} \varphi\left(\sqrt[4]{2}\right) &= \sqrt[4]{2} \\ \varphi\left(-\sqrt[4]{2}\right) &= -\sqrt[4]{2} \end{aligned}$$

As φ fixing all real numbers.

But:

$$i\sqrt[4]{2} \xrightarrow{\varphi} -i\sqrt[4]{2}$$

Claim 5.8.11

The map ψ sending $\sqrt[4]{2} \mapsto i\sqrt[4]{2}$ but fixing i is an automorphism.

Proof:

$$\psi\left(a + b\sqrt[4]{2} + ci\sqrt[4]{2} + d\sqrt{2} + ei\sqrt{2}\right) = a + bi\sqrt[4]{2} - c\sqrt[4]{2} - d\sqrt{2} - ei\sqrt{2}$$

Need to show it is additive, mult, etc.

$$\begin{aligned} \psi^2\left(\sqrt[4]{2}\right) &= \psi\left(i\sqrt[4]{2}\right) = -\sqrt[4]{2} \\ \psi^4\left(\sqrt[4]{2}\right) &= \psi\left(-\sqrt[4]{2}\right) = -i\sqrt[4]{2} \\ \psi^4\left(\sqrt[4]{2}\right) &= \psi\left(-i\sqrt[4]{2}\right) = \sqrt[4]{2} \end{aligned}$$

ψ is of order 4.

$$\begin{aligned}\varphi\psi\left(\sqrt[4]{2}\right) &= \varphi\left(i^4\sqrt{2}\right) = -i\sqrt{2} \\ \psi\varphi\left(\sqrt[4]{2}\right) &= \psi\left(\sqrt[4]{2}\right) = i\sqrt[4]{2}\end{aligned}$$

So $\text{Gal}(E/\mathbb{Q})$ is non-abelian.

Turns out that $\varphi^{-1}\psi\varphi = \psi^3$. So in-fact $\text{Gal}(E/\mathbb{Q}) \cong D_8$. ■

Lemma 5.8.12

If $f(x) \in \mathbb{Z}[x]$ and monic, then every rational root is an integer.

Remarks 5.8.13 This is a special case of Gauss' Lemma.

Proof: If $\frac{r}{s} \in \mathbb{Q}$ is a root, $r, s \neq 0 \in \mathbb{Z}$ s.t. $(r, s) = 1$. Write:

$$f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0$$

Then:

$$\left(\frac{r}{s}\right)^n + a_{n-1}\left(\frac{r}{s}\right)^{n-1} + \dots + a_0 = 0$$

Multiply by s^n and we get:


$$r^n + a_{n-1}sr^{n-1} + a_{n-2}s^2r^{n-2} + \dots + a_0s^n = 0$$

So we got:

$$-r^n = s(a_{n-1}r^{n-1} + a_{n-2}sr^{n-2} + \dots + a_0s^{n-1}) \Rightarrow s \mid r^n$$

If p is a prime divisor of s , then $p \mid r^n$ and so $p \mid r$, but $(r, s) = 1$ - contradiction!

So s has no prime divisors, so $s = \pm 1$ and we get: $\frac{r}{s} \in \mathbb{Z}$ as required. ■

 **Example 5.8.14 :** $f(x) = x^3 + 2x + 1$ over \mathbb{Q} .

Claim 5.8.15

f is irreducible over \mathbb{Q} .

Proof: f is irreducible over \mathbb{Q} as it has no roots in \mathbb{Q} as by our Lemma, it is sufficient to show it has no integer roots.

Let's look at some values:

$$\begin{aligned} f(0) &= 1 \\ f(-1) &= -2 \end{aligned}$$

Which means it changes signs between 0 and -1 . As a real function $f(x) = x^3 + 2x + 1$ is continuous and so there exists a real root α s.t. $-1 < \alpha < 0$.

Now, Note that:

$$f'(x) = 3x^2 + 2 > 0$$

For all real x , so $f(x)$ is an increasing function for all real x . Therefore α is it's only real root. But it's clear that $\alpha \notin \mathbb{Z}$ as it lies between -1 and 0 . So $\alpha \notin \mathbb{Q}$. ■

We extend to $\mathbb{Q}(\alpha)$. We know that $|\mathbb{Q}(\alpha) : \mathbb{Q}| = 3$ as f is irreducible.

Factoring f over $\mathbb{Q}(\alpha)$ we get:

$$x^3 + 2x + 1 = (x - \alpha)(x^2 + \alpha x + (2 + \alpha^2))$$

Because:

$$-\alpha(2 + \alpha^2) = 1 \Rightarrow -\alpha^3 - 2\alpha = 1$$

Holds as $\alpha^3 + 2\alpha + 1 = 0$.

The roots of $x^2 + \alpha x + (2 + \alpha^2)$ are:

$$\frac{-\alpha \pm \sqrt{\alpha^2 - 4(2 + \alpha^2)}}{2} = \frac{-\alpha \pm \sqrt{-3\alpha^2 - 8}}{2}$$

Note that the square root is negative, as we expected, thus the roots are β and $\bar{\beta}$, complex numbers. $\beta, \bar{\beta}$ are remaining non-real roots.

The s.f. of $x^3 + 2x + 1$ is: $\mathbb{Q}(\alpha, \beta)$ and:

$$x^3 + 2x + 1 = (x - \alpha)(x - \beta)(x - \bar{\beta})$$

$$|\text{Gal}(\mathbb{Q}(\alpha, \beta)/\mathbb{Q})| = |\mathbb{Q}(\alpha, \beta) : \mathbb{Q}| = \underbrace{|\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)|}_2 \cdot \underbrace{|\mathbb{Q}(\alpha) : \mathbb{Q}|}_3 = 6$$


Thus $\text{Gal}(\mathbb{Q}(\alpha, \beta)/\mathbb{Q})$ permutes $\alpha, \beta, \bar{\beta}$ and so $\cong S_3$.

5.9 Cyclotomic extensions of \mathbb{Q}

Cyclotomic extensions are extensions of \mathbb{Q} obtained by adjoin roots of unity.

Denote: $\sqrt[n]{1} = e^{\frac{2\pi i}{n}}$ = "primitive n -th root of 1".

We want to explore $\mathbb{Q}(\sqrt[n]{1})$.

 **Example 5.9.1 :** $\mathbb{Q}(i)$, $i = \sqrt[4]{1}$

Denote: minimal polynomial of $\sqrt[n]{1}$ over \mathbb{Q} by $\lambda_n(x)$ = The n -th cyclotomic polynomial. We know that $\lambda_n(x) \mid x^n - 1$ over \mathbb{Q} as $\sqrt[n]{1}$ is a root of $x^n - 1$.

$\mathbb{Q}(\sqrt[n]{1})$ is a Galois extension.

Over this field, $x^n - 1$ factors completely: $\prod_{i=0}^{n-1} (x - \xi^i) = x^n - 1$, $1, \xi, \dots, \xi^{n-1}$ all distinct.

Question:

1. What are $\lambda_n(x)$?
2. How does $x^n - 1$ factor over \mathbb{Q} into irreducibles?
3. What is $\text{Gal}(\mathbb{Q}(\sqrt[n]{1})/\mathbb{Q})$?
4. What is the degree of $\lambda_n(x)$?



Example 5.9.2 : $n = 1$: $x - 1 = \lambda_1(x)$
 $n = 2$: $x + 1 = \lambda_2(x)$, and indeed $x^2 - 1 = (x - 1)(x + 1)$
 $n = 3$: $x^3 - 1 = (x - 1) \underbrace{(x^2 + x + 1)}_{\text{Irreducible over } \mathbb{Q}}$, $\lambda_3(x) = x^2 + x + 1$, $\omega, \bar{\omega}$ are its roots and $\sqrt[3]{1} = \omega = \frac{-1+i\sqrt{3}}{2}$.
 $n = 4$: $x^4 - 1 = (x^2 - 1) \underbrace{(x^2 + 1)}_{\text{Irreducible over } \mathbb{Q}} = (x - 1)(x + 1) \underbrace{(x^2 + 1)}_{\text{Irreducible over } \mathbb{Q}}$, $\lambda_4(x) = x^2 + 1$.

It turns out by Gauss' lemma, that if $f(x), g(x) \in \mathbb{Q}[x]$ and $f(x)g(x) = x^n - 1$, then $f(x), g(x) \in \mathbb{Z}[x]$.

Question: Is it true that all factors of $x^n - 1$ over \mathbb{Q} have coefficients in the set $\{0, +1, -1\}$?

It turns out that it is true up to $n = 104$!

Fails for $n = 105$: (1883) Migotti: If h has at most 2 distinct prime factors then coefficients of $\lambda_n(x) \in \{0, \pm 1\}$.



Example 5.9.3 : Let's take a look at $\mathbb{Q}(i)$. Note that $[\mathbb{Q}(i) : \mathbb{Q}] = 2$. If we will look at $\mathbb{Q} \times \mathbb{Q}$, we can find out that the addition is the same as in this vector space: $a + ib \mapsto (a, b)$. And we add the multiplication rule:

$$(a, b)(c, d) = (ac - bd, bc + ad)$$

Thus $(0, 1)$ is a root of $(-1, 0)$.



Example 5.9.4 : If now we will take: $\mathbb{Q}(\omega)$ s.t. $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$ and those are the complex roots of the polynomial: $x^3 - 1 = (x - 1) \underbrace{(x^2 + x + 1)}_{\text{minimal polynomial of } \omega}$, so:

$$\omega^2 + \omega + 1 = 0 \Rightarrow \omega^2 = -1 - \omega$$

Thus:

$$\mathbb{Q}(\omega) = \{a + \omega b \mid a, b \in \mathbb{Q}\}$$

We got the addition same is in $\mathbb{Q} \times \mathbb{Q}$ again, where: $a + \omega b \mapsto (a, b)$.

And we got the multiplication rule:

$$(a, b)(c, d) = (ac - bd, bc + ad - bd)$$

Because:

$$(a + \omega b)(c + \omega d) = ac + \omega^2 bd + (bc + ad)\omega = ac + (-1 - \omega)bd + (bc + ad)\omega$$

And, in this field $(0, 1)$ is a primitive cubed root of $(1, 0)$



Example 5.9.5 : $\mathbb{Q}(\sqrt{2})$, Again $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. Similar to the above examples.

There infinite many nonsiomorphic ways to define multiplication on $\mathbb{Q}^{(2)}$ to get a field!

Now, Lets look at $\lambda_n(x)$ = The minima polynomial of $\sqrt[n]{1}$. (Hence: $\lambda_n(x) \mid x^n - 1$).

Let's focus on the case where $n = 5$, $x^5 - 1 = (x - 1) \underbrace{(x^4 + \dots + 1)}_{\text{irreducible}}$. Infact, for $n = p$ prime we will get:

$$x^p - 1 = (x - 1) \underbrace{(x^{p-1} + x^{p-2} + \dots + x + 1)}_{\text{irreducible} = \lambda_p(x)}$$

The irreducibility follows from Eisenstein's criterion.

 **Example 5.9.6 :** Now, Let's look at the case where $n = 6$:

$$x^6 - 1 = (x^3 - 1)(x^3 + 1) = \underbrace{(x - 1)}_1 \underbrace{(x^2 + x + 1)}_{\omega, \omega^2} \underbrace{(x + 1)}_{-1} \underbrace{(x^2 - x + 1)}_{\text{irreducible over } \mathbb{Q}=\lambda_6(x)}$$


So infact:

$$|\mathbb{Q}(\sqrt[6]{1}) : \mathbb{Q}| = 2$$

$-\omega$ is in fact a primitive 6-th root of 1. $(-\omega)^6 = 1$. So: $\mathbb{Q}(\sqrt[6]{1}) = \mathbb{Q}(\omega)$.

Theorem 5.9.7

$|\mathbb{Q}(\sqrt[n]{1}) : \mathbb{Q}| = \varphi(n) = \text{Euler } \varphi\text{-function.}$

 **Example 5.9.8 :** As we've seen: $\varphi(3) = 2$, $\varphi(p) = p - 1$ where p prime, $\varphi(6) = |\{1, 5\}| = 2$. And note that also: $\varphi(4) = 2$ and we can continue like so.

Proof: We will not go over the entire proof. Just a quicq review:

We show that $\deg \lambda_n(x) = \varphi(n)$. It turns out that if $\xi = \sqrt[n]{1}$ then for every k prime to n , ξ^k is a root of $\lambda_n(x)$. Moreover, these are all the roots over \mathbb{C} :

$$\lambda_n(x) = \prod_{\substack{1 \leq k < n \\ (k, n) = 1}} (x - \xi^k)$$

Note that from Gauss's Lemma, $\lambda_n(x)$ are actually polynomial over \mathbb{Z} .

Remarks 5.9.9 If $d \mid n$ then any d -th rot of 1 is also an n -th root of 1. Consequently, $\lambda_d(x) \mid x^n - 1$ over \mathbb{Z} .


Conversely, suppose $p(x)$ is irreducible factor of $x^n - 1$, Then any root of $p(x)$ in $\mathbb{Q}(\sqrt[n]{1})$ must also be a root of $x^n - 1$, as if $p(\alpha) = 0$ then $\alpha^n - 1 = 0$.

So α is a root of 1 for some d and since $\alpha^n = 1$, must have $d \mid n \Rightarrow$ The irreducible factors of $x^n - 1$ over \mathbb{Q} are precisely $\{\lambda_d(x) \mid d \mid n\}$. i.e.:

$$x^n - 1 = \prod_{d \mid n} \lambda_d(x)$$

 **Example 5.9.10 :**

$$x^6 - 1 = \prod_{d \mid 6} \lambda_d(x) = \lambda_1(x) \lambda_2(x) \lambda_3(x) \lambda_6(x)$$

 **Example 5.9.11 :** $n = 12$:

$$x^{12} - 1 = (x^6 - 1)(x^6 + 1) = (x^6 - 1) \underbrace{(x^2 + 1)}_{\text{irreducible over } \mathbb{Q}} \underbrace{(x^4 - x^2 + 1)}_{\text{irreducible over } \mathbb{Q}} = \lambda_1(x) \lambda_2(x) \lambda_3(x) \lambda_6(x) \lambda_4(x) \lambda_{12}(x)$$

This gives a nice number theory formula:

$$n = \sum_{d \mid n} \varphi(d)$$

5.9.1 Galois group of a cyclotomic field

We want to ask, what is $\text{Gal}(\mathbb{Q}(\sqrt[n]{1})/\mathbb{Q})$?

We know that:

$$|\text{Gal}(\mathbb{Q}(\sqrt[n]{1})/\mathbb{Q})| = \varphi(n)$$

Assume that $\varphi \in \text{Gal}(\mathbb{Q}(\sqrt[n]{1})/\mathbb{Q})$ permutes the roots of $\lambda_n(x)$ and it is a s.f. for $\lambda_n(x)$. $\xi = \sqrt[n]{1}$, the image of ξ determines φ . $\varphi(\xi) = \xi^k$ for some k s.t. $(k, n) = 1$. Denote this by ψ_k . Each k s.t. $(k, n) = 1$ indeed yields an automorphism. Since $|G| = \varphi(n)$ every element is of this form.

Let l, k be prime to n , Lets look at:

$$\begin{aligned}\psi_l \psi_k(\xi) &= \psi_l(\xi^k) = (\psi_l(\xi))^k = \xi^{lk} \\ \psi_k \psi_l(\xi) &= \psi_k(\xi^l) = \xi^{lk}\end{aligned}$$

So that, $\psi_k \psi_l = \psi_l \psi_k$ and G is abelian. If $l \cdot k \equiv m \pmod{n}$ we have that $\psi_l \psi_k = \psi_m$. We infact have an isomorphism between G and $(\mathbb{Z}/n\mathbb{Z})^*$ = group of units of $\mathbb{Z}/n\mathbb{Z}$. Meaning: $\psi_k \mapsto k$. So $G \cong (\mathbb{Z}/n\mathbb{Z})^*$.


 **Example 5.9.12 :** $n = 6$. $\xi = \sqrt[6]{1} = \omega$.

$$- \underbrace{\omega^2}_{=\xi^5=\xi^{-1}} (-\omega) = 1$$

The 2 options are:

- $\xi \xrightarrow{\text{Id}} \xi$.
- $\xi \xrightarrow{\psi} \xi^5 = \xi^{-1}$.

ψ is of order 2. $\text{Gal}(\mathbb{Q}(\sqrt[6]{1})/\mathbb{Q}) \cong C_2$.

 **Example 5.9.13 :** $n = 12$. $\xi = \sqrt[12]{1}$.

There are few options:

- $\xi \xrightarrow{\text{Id}} \xi$.
- $\xi \xrightarrow{\tau} \xi^5$.
- $\xi \xrightarrow{\psi\tau} \xi^7$.
- $\xi \xrightarrow{\psi} \xi^{11} = \xi^{-1}$.

Remarks 5.9.14 If $\xi = \sqrt[n]{1}$ then $\xi^{-1} = \bar{\xi}$, meaning ψ =complex conjugation.

Note that:

$$\tau^2(\xi) = \tau(\xi^5) = \xi^{25} = \xi$$

Because:

$$5^2 \equiv 1 \pmod{12}$$

So ψ is of order 2.

$$\psi\tau(\xi) = \psi(\xi^5) = \xi^{55} = \xi^7$$

And of course:

$$7^2 \equiv 1 \pmod{12}$$

Thus we have:

$$\text{Gal}(\mathbb{Q}(\sqrt[12]{1})/\mathbb{Q}) \cong (\mathbb{Z}/12\mathbb{Z}) = \{1, 5, 7, 11\}$$

All the elements in $\text{Gal}(\mathbb{Q}(\sqrt[12]{1})/\mathbb{Q}) \cong C_2 \times C_2$ are of order 2.

5.10 Finite fields

Definition 5.10.1 Prime field: A prime field has to be of the form $\mathbb{Z}/p\mathbb{Z}$ (and then $\text{char} = p$).

The big difference in the case of finite field is the following theorem:

Theorem 5.10.2

There is only one field of a given order - up to isomorphism.

We will prove the following theorem:

Theorem 5.10.3

A finite field is of order p^k for some prime p and $1 \leq k \in \mathbb{N}$. And for any prime p and $1 \leq k \in \mathbb{N}$, there exists a unique field of that order (up to isomorphism). Denote $\text{GF}(p^k)$, Galois field.

We will prove this gradually. **Proof:** Let F be finite. It has a prime $\text{char} = p$ and some field $F_0 \cong \mathbb{Z}/p\mathbb{Z}$. F is a vector space over F_0 , and because F is finite, it has a finite dimension k . So $F \cong F_0^{(k)}$ as a vector space.

So F has p^k elements (= number of linear combinations of a given basis over $\mathbb{Z}/p\mathbb{Z}$). ■



Example 5.10.4 : $\mathbb{Z}/2\mathbb{Z}$ unique field of order 2.

$x^2 + x + 1$ is irreducible of $\mathbb{Z}/2\mathbb{Z}$ (because it is a 2 degree polynomial with no roots in the field).

Look at:

$$\mathbb{Z}/2\mathbb{Z}[x]/(x^2+x+1) \cong \mathbb{Z}/2\mathbb{Z}[x]$$

This is a quadratic extension of $\mathbb{Z}/2\mathbb{Z}$, denote it by K .

Note that:

$$|K : \text{GF}(2)| = 2$$

So, $|K| = 4$. Elements can be considered to be linear polynomials in x , with addition and multiplication mod $(x^2 + x + 1)$ over $\mathbb{Z}/2\mathbb{Z}$.

The addition is defined by:

+	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

And the multiplication:

·	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

(Note that $(x+1)^2 \equiv x^2 + 1 = x$)

It can be shown directly that this is the only field of order 4 up to isomorphism.

Remarks 5.10.5 $x^2 + x + 1$ is in fact the only irreducible quadratic over $\mathbb{Z}/2\mathbb{Z}$. The other reducibles are:

$$\begin{aligned} x^2 &= x \cdot x \\ x^2 + 1 &= (x+1)^2 \end{aligned}$$

Remarks 5.10.6 The identity $(x+1)^2 \equiv x^2 + 1$ is more general, in fact:

$$(x+1)^p \equiv x^p + 1 \pmod{p}$$

 **Example 5.10.7 :** $x^4 + x^3 + 1$ over $\text{GF}(2)$. It is in fact irreducible over $\text{GF}(2)$.

- It has no linear factors.
- It has no quadratic factors as only candidate is $x^2 + x + 1$ and $(x^2 + x + 1)^2 = x^4 + x^2 + 1$.

So $K = \text{GF}(2)[x]/(x^4 + x^3 + 1)$ = field of order 16. Elements can be considered to be polynomials of degree ≤ 3 over $\text{GF}(2)$ with addition mod 2 and multiplication mod $(x^4 + x^3 + 1)$.

For example:

If we take $(x^2 + x) + (x^3 + x^2 + 1) = x^3 + x + 1$

And:

$$(x^2 + x)(x^3 + x^2 + 1) = x^5 + 2x^4 + x^3 + x^2 + x \equiv_{\text{mod } 2} x^5 + x^3 + x^2 + x \equiv_{\text{mod } (x^4 + x^3 + 1)} (x^4 + x^3 + 1)(x + 1) + (x^2 + 1) \equiv_{\text{mod } (x^4 + x^3 + 1)} x^2 + 1$$

Similarly:

$$x^3(x + 1) = x^4 + x^3 \equiv_{\text{mod } (x^4 + x^3 + 1)} -1 \equiv_{\text{mod } 2} 1$$

So $x^3 = (x + 1)^{-1}$ in K .

Another notation: Consider elements to be 4-tuples over $\text{GF}(2) : \text{GF}(2)^{(4)}$. e.g.: $ax^3 + bx^2 + cx + d \mapsto (a, b, c, d)$.

Lets look at: $(x^2 + x) + (x^3 + x^2 + 1)$. We get:

$$(0, 1, 1, 0) + (1, 1, 0, 1) = (1, 0, 1, 1)$$

Again, addition is easy, multiplication is not.

A 3rd notation: Denote: $\alpha = x + (x^4 + x^3 + 1)$.

We know that α is a root of $x^4 + x^3 + 1$ in K . α is an element in the multiplication group of the field $K^* = K \setminus \{0\}$ so $\alpha^{15} = 1$. $\alpha \neq 1$, so $|\alpha| = 3, 5, 15$.

We want to check what the order of α is.

Clearly, $\alpha^3 \neq 1$, as if so we would have: $\alpha^3 \equiv 1 \pmod{x^4 + x^3 + 1}$, but $1, x, x^2, x^3$ are linear independent as $x^4 + x^3 + 1$ is minimal polynomial.

In other words $\alpha^3 - 1 = 0$ which is impossible.

Note that $\alpha^4 = \alpha^3 + 1$, as $x^4 + x^3 + 1 = 0$ in quotient ring (K) .

$\alpha^5 = \alpha(\alpha^4 + 1) = \alpha^4 + \alpha \neq 1$ otherwise α root of $x^4 + x + 1$ and $x^4 + x^3 + 1 \nmid x^4 + x + 1$.

So α is of order 15.

So $0, 1, \alpha, \alpha^2, \dots, \alpha^{14}$ are all the elements of K . So this is another representation of K , but here it is easy to multiply because: $\alpha^i \cdot \alpha^j = \alpha^{i+j}$.

We also denote: $\text{GF}(16) \cong \mathbb{F}_2[x]/(x^4 + x^3 + 1)$.

So to summerize, these are the representations we've seen:

I	II	III
0	0	(0, 0, 0, 0)
1	1	(0, 0, 0, 1)
α	x	(0, 0, 1, 0)
α^2	x^2	(0, 1, 0, 0)
α^3	x^3	(1, 0, 0, 0)
α^4	$x^3 + 1$	(1, 0, 0, 1)
α^5	\vdots	(1, 0, 1, 1)
α^6		(1, 1, 1, 1)
α^7		(0, 1, 1, 1)
α^8		(1, 1, 1, 0)
α^9		(0, 1, 0, 1)
α^{10}		(1, 0, 1, 0)
α^{11}		(1, 1, 0, 1)
α^{12}		(0, 0, 1, 1)
α^{13}		(0, 1, 1, 0)
α^{14}		(1, 1, 0, 0)

Because $x^4 \cong x^3 + 1$.

Note that for addition it is easy to use the column III mod 2. But for multiplication it is easy to use column I as: $\alpha^i \cdot \alpha^j = \alpha^{i+j \pmod{15}}$.



Example 5.10.8 : So if, for example we want to add $\alpha^6 + \alpha^7$ what will we get?

If we will look at the table we will translate the elements to the third column and we will get:

$$\underbrace{(1, 1, 1, 1)}_{\alpha^6} + \underbrace{(0, 1, 1, 1)}_{\alpha^7} = \underbrace{(1, 0, 0, 0)}_{\alpha^3}$$

And of course:

$$\alpha^7 \cdot \alpha^6 = \alpha^{13}$$

Another example is to multiply $(1, 1, 0, 0) \cdot (1, 0, 1, 1)$, here we will translate the items to the first column and we will get: $\alpha^{14} \cdot \alpha^5 = \alpha^{19} = \alpha^4 = (1, 0, 0, 1)$.

5.10.1 Field's multiplicative group is cyclic

Theorem 5.10.9

The multiplicative group of a finite field is cyclic.

Proof: Using the fundamental theorem for abelian groups (Which we didn't prove, but can be found at Basic Algebra I), we know that $F^* \cong$ direct product of cyclic groups of prime power orders.

Group together those corresponding to same prime power, p_i , to get:

$$F^* \cong H_1 \times H_2 \times \dots \times H_r$$

With: $H_i =$ direct product of cyclic groups of orders power of p_i .

Thus:

$$H_i = C_{p_i^{k_{i_1}}} \times C_{p_i^{k_{i_2}}} \times \dots \times C_{p_i^{k_{i_t}}}$$

WLOG, we have: $k_{i_1} \geq k_{i_2} \geq \dots \geq k_{i_t}$. Hence, every element in H_i satisfies: $a^{p_i^{k_{i_1}}} = 1$. Thus, a is a root of the polynomial $x^{p_i^{k_{i_1}}} - 1$. As $a \in F$, there are at most $p_i^{k_{i_1}}$ roots to this polynomial in F . So $|H_i| \leq p_i^{k_{i_1}}$. Meaning: $k_{i_2} = k_{i_3} = \dots = k_{i_t} = 0$ (otherwise there will be too many roots to that polynomial!). So H_i is cyclic!

Thus, F^* is a product of cyclic groups of mutually prime orders, and is therefore cyclic as required. ■

Remarks 5.10.10 $\text{GF}(16)$ was obtained as an extension field of $\text{GF}(2)$ in which $x^4 + x^3 + 1$ has a root: α . Note that: $(x^4 + x^3 + 1)^2 \underset{\text{mod } 2}{=} x^8 + x^6 + 1$. So α^2 is a root of $x^4 + x^3 + 1$, because:

$$0 = (\alpha^4 + \alpha^3 + 1) = \alpha^8 + \alpha^6 + 1$$

But we can do it again:

$$0 = (\alpha^8 + \alpha^6 + 1)^2 = \alpha^{16} + \alpha^{12} + 1$$

So α^4 is another root.

Similarly α^8 is a root.

So $\text{GF}(16)$ is a splitting field for $x^4 + x^3 + 1$, so it factors completely:

$$x^4 + x^3 + 1 = (x - \alpha)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8)$$

Remarks 5.10.11 If F is a field, and if $|F| = q = p^k$ (with p prime), then every element of F^* is a root of $x^{q-1} - 1$. So every element of F is a root of $x^q - x$. This polynomial has at most q roots, but every element of F is a root for this polynomial, and it has q elements.

We can conclude that F is a splitting field for $x^q - x$ as it contains q distinct roots of this polynomial. Moreover, every element of F is a root.

So that over F : $x^q - x = \prod_{a \in F} (x - a)$.

Corollary 5.10.12

If $a \in F$, then its minimal polynomial over $\text{GF}(p)$ divides $x^q - x$.



Example 5.10.13 : In $\text{GF}(16)$, we get that $x^4 + x^3 + 1 \mid x^{16} - x$.

5.10.2 Finite fields of the same order are isomorphic

Theorem 5.10.14

Any 2 finite fields F, \tilde{F} of equal order are isomorphic.

Proof: Both are splitting fields of $x^q - x$ over $\text{GF}(p)$ where $q = p^k$ and so are isomorphic. But we shall construct an isomorphism explicitly.

We know that F^* is cyclic, so let $\langle \alpha \rangle = F^*$, in other words, α is the generator of F^* . Let $m(x)$ be its minimal polynomial over $\text{GF}(p)$. $m(x) \mid x^q - x$ over $\text{GF}(p)$.

And since \tilde{F} is also a s.f. of $x^q - x$, \tilde{F} must contain a root β of $m(x)$. Map: $\begin{cases} \alpha^i \mapsto \beta^i \\ 0 \end{cases}$ for $0 \leq i \leq q-1$. φ is clearly a multiplicative map.

Claim 5.10.15

φ is onto \tilde{F} .

Proof: Suppose $\beta^r = 1$ for $r < q-1$, so β is a root of $x^r - 1$ so its minimal polynomial divides $x^r - 1$, thus $m(x) \mid x^r - 1$. But as $m(\alpha) = 0$ in F we get $\alpha^r - 1 = 0$ and $\alpha^r = 1$. Contradiction as $\langle \alpha \rangle = F^*$. ■

To complete our proof that φ is an isomorphism we show that it is additive, clearly $(\alpha^i + 0) = \varphi(\alpha^i)$. We need to check that for any i, j $\varphi(\alpha^i + \alpha^j) = \varphi(\alpha^i) + \varphi(\alpha^j)$.

There are two cases we need to check:

1. $\alpha^i + \alpha^j = \alpha^l$ for some l .
2. $\alpha^i + \alpha^j = 0$.

We will dill with the first case:

$$\begin{aligned}\varphi(\alpha^i + \alpha^j) &= \varphi(\alpha^l) = \beta^l \\ \varphi(\alpha^i) + \varphi(\alpha^j) &= \beta^i + \beta^j\end{aligned}$$

We need to show that $\beta^i + \beta^j = \beta^l$. α is a root of the polynomial $x^i + x^j - x^l$, so $m(x) \mid x^i + x^j - x^l$, so β is a root of $x^i + x^j - x^l$ as well, giving $\beta^i + \beta^j = \beta^l$ as required.

The second case is remained to the reader. ■

5.10.3 Existence of fields of order p^m

Theorem 5.10.16

For any prime p and integer $m > 0$ there exists a unique field of order p^m (denoted by $\text{GF}(p^m)$).

Proof: Take $\mathbb{Z}/p\mathbb{Z}$ and contrsuct a splitting field over it for the polynomial $x^{p^m} - x$. This gives a field F of order q . Since the set of roots is of order p^m , $p^m \leq q$.

But the set of roots is in fact a field, so by minimality of the splitting field, $p^m = q$. ■

Corollary 5.10.17

For any integer $n > 0$ and a prime p there exists an irreducible polynomial of degree n over \mathbb{F}_p .

Proof: Let F be the field of order p^n . F^* is cyclic so it has a generator α .

α has a minimal polynomial $m(x)$ over \mathbb{F}_p and we know that: $F = \mathbb{F}_p(\alpha) = \mathbb{F}_p[x]/(m(x))$ and that $|\mathbb{F}_p(\alpha) : \mathbb{F}_p| = \deg m(x)$, So $m(x)$ is irreducible of degree n . ■

5.10.4 Factoring $x^n - 1$ over \mathbb{F}_p

Remarks 5.10.18 Can always factor over \mathbb{Q} (which in fact over \mathbb{Z}) and reduce mod p to get a partial factorisation.

We write $n = p^r \cdot m$ with $(m, p) = 1$.

Recall that:

- $(a + b)^p = a^p + b^p$ over \mathbb{F}_p . $\Rightarrow (a + b)^{p^k} = a^{p^k} + b^{p^k}$
- $(-1)^p = -1$ over \mathbb{F}_p for p odd.
- $(-1)^2 = -1$ over \mathbb{F}_2 .

And we can conclude that: $(a - b)^{p^k} = a^{p^k} - b^{p^k}$ over \mathbb{F}_p .

So $x^m - 1 = x^{mp^r} - 1 = (x^m - 1)^{p^r}$. So it is enough to look at the case $x^n - 1$ where $(n, p) = 1$.

Claim 5.10.19

If $(n, p) = 1$ there exists a positive integer k s.t. $n \mid p^k - 1$.

Proof: $p + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^*$. By abuse of notation, we write $p \in (\mathbb{Z}/n\mathbb{Z})^*$. $(\mathbb{Z}/n\mathbb{Z})^*$ is finite (in fact of order $\varphi(n)$, but it doesn't matter). The fact that it is finite means that $\exists k > 0$ s.t. $p^k \equiv 1 \pmod{n}$ and so $n \mid p^k - 1$.

Suppose $f(x) \in \mathbb{F}_p[x]$ is an irreducible polynomial of $x^n - 1$ and $n \mid p^k - 1$. Let α be a root of f in some extension field of \mathbb{F}_p .

$f(x) \mid x^n - 1$ so α is a root of $x^n - 1$. So $\alpha^n = 1$ but $n \mid p^k - 1$ so also $\alpha^{p^k - 1} = 1$ or $\alpha^{p^k} = \alpha$. Let $q = p^k$, We can regard α as an element of $\text{GF}(q) = \mathbb{F}_q$. So it's minimal polynomial $f(x) \mid x^q - x$.

So, to factor $x^n - 1$ where $(n, p) = 1$ we need to know how to factor $x^q - x$ where $q = p^k$ (and $n \mid p^{k-1}$), any factor of $x^n - 1$ is a factor of $x^q - x$.

So we reduce to the case of factoring $x^q - x$ over \mathbb{F}_p . ■

$q = 16$.

$$x^4 + x^3 + 1 \mid x^{16} - x.$$

The roots of $x^4 + x^3 + 1$ are: $\alpha, \alpha^2, \alpha^4, \alpha^8$.

$$x^{16} - x = \underbrace{x}_0 \underbrace{(x+1)}_1 \underbrace{(x^4 + x^3 + 1)}_{\alpha, \alpha^2, \alpha^4, \alpha^8} h(x)$$

So $h(x)$ is of degree 10, we need to factor $h(x)$.

Using \mathbb{Q} :

$$x^{16} - x = x(x^{15} - 1) = x(x^5 - 1)(x^{10} + x^5 + 1)$$

Also over \mathbb{F}_2 . And:

$$x^5 - 1 = (x - 1) \underbrace{(x^4 + x^3 + x^2 + x + 1)}$$

another factor of $x^{16} - x$ and a factor of $h(x)$
and is not irreducible over \mathbb{F}_2
and it has no roots in \mathbb{F}_2 and is not a product
of 2 irreducible quadratics as only irreducible
quadratic is $x^2 + x + 1$ and:
 $(x^2 + x + 1)^2 = x^4 + x^2 + 1$

Another option is to use reciprocal polynomials:

Definition 5.10.20 Let $f(x)$ be a polynomial of degree m . Its reciprocal $g(x) \underbrace{=}_{\text{formally}} x^m \cdot f(x^{-1})$.

 **Example 5.10.21 :**

$$\begin{aligned} f(x) &= 3x^5 + 2x^2 - 7x \\ g(x) &= x^5(3x^{-5} + 2x^{-2} - 7x^{-1}) = 3 + 2x^3 - 7x^4 \end{aligned}$$

Claim 5.10.22

- The reciprocal of a polynomial $f(x)$ is a polynomial in x .
- If constant term of $f(x) \neq 0$ then its reciprocal has degree equal to $\deg f$.
- If β is a root of f then β^{-1} is a root of reciprocal.
- If $f(x)$ is irreducible \iff its reciprocal is irreducible.

We will prove this claim in Assignment 4.

Another claim that is not in the assignment:

Claim 5.10.23

If constant term of f is $\neq 0$ then the reciprocal of the reciprocal is f .

Since $\alpha^{-1} \in \text{GF}(16)$, its minimal polynomial is the reciprocal of $x^4 + x^3 + 1$ and also divides $x^{16} - x$ so we get: $x^4(x^{-4} + x^{-3} + 1) = 1 + x + x^4$. This polynomial is irreducible and its roots are $\alpha^{-1}, \alpha^{-2}, \alpha^{-4}, \alpha^{-8}$. So we found some more polynomials by starting from the roots.

Look at the polynomial $x^{16} - x$, The factorization is:

$$x^{16} - x = x(x+1)(x^4 + x^3 + 1)(x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1)$$

The roots of the polynomial are:

$$0; 1; \alpha, \alpha^2, \alpha^4, \alpha^8; \alpha^{14}, \alpha^{13}, \alpha^{11}, \alpha^7; \alpha^3, \alpha^6, \alpha^{12}, \alpha^9; \alpha^5, \alpha^{10}$$

Only the last element added α^5, α^{10} because they are of order 3, thus the roots of $x^3 - 1$.

Note that $\alpha^{15} = 1$.

Corollary 5.10.24

GF (16) contains the subfield GF (2), GF (4) but not GF (8).

GF (8) is the s.f. of an irreducible polynomial of degree 3 over GF (2) and no such polynomial divides $x^{16} - x$.

Lemma 5.10.25

$$x^m - 1 \mid x^n - 1 \iff m \mid n \text{ (over any prime field).}$$

Proof:

$$x^n - 1 = (x^m - 1)(x^{n-m} + x^{n-2m} + \dots + x^{n-km}) + (x^{n-km} - 1)$$

With $n \geq km$ but $n < (k+1)m$.

$$\text{But } (x^{n-km} - 1) = 0 \iff n - km = 0 \iff m \mid n. \quad \blacksquare$$

Corollary 5.10.26

$$\text{GF}(p^m) \subseteq \text{GF}(p^n) \iff m \mid n.$$

Proof: If $m \mid n$ then by the Lemma $p^m - 1 \mid p^n - 1$ and so again by the Lemma:

$$x^{p^m-1} - 1 \mid x^{p^n-1} - 1$$

and so:

$$x^{p^m} - x \mid x^{p^n} - x$$

So GF (p^n) which contains all roots of $x^{p^n} - x$ and so all roots of $x^{p^m} - x$ which form the field GF (p^m).

Now, if $\text{GF}(p^m) \subseteq \text{GF}(p^n)$ then GF (p^n) is a vector space over GF (p^m) of finite dimension k . Thus:

$$|\text{GF}(p^n) : \text{GF}(p^m)| = k$$

Buy then $\text{GF}(p^n) \cong \text{GF}(p^m)^{(k)}$ as a vector sapce $\Rightarrow p^n = p^{mk} \Rightarrow m \mid n. \quad \blacksquare$

The Frobenius automorphism

Let φ be the Frobenius automorphism, that is:

In a field F of char p , the map: $a \mapsto a^p$ is an automorphism.

If $m \mid n$, In GF (p^n) the set of elements that are fixed points under p^m is the subfield GF (p^m).

Theorem 5.10.27

Over $\mathbb{Z}/p\mathbb{Z}$: $x^{p^n} - x = \text{product of all monic irreducible polynomials over } \mathbb{Z}/p\mathbb{Z} \text{ of degrees dividing } n.$

Remarks 5.10.28 Constructing GF (16) as an extension field of GF (2) using $x^4 + x^3 + x^2 + x + 1$ gives a root β of this polynomial $\beta^5 = 1$. So $\langle \beta \rangle \neq \text{GF}(16)^*$. But $\mathbb{F}_2(\beta) = \text{GF}(16)$.

i.e. not every element in $\text{GF}(16)^*$ can be written as a power of β . But every element is a polynomial in β (of degree ≤ 3).

Proof: Let $f(x)$ be irreducible of degree m where $m \mid n$. Extend \mathbb{F}_p using f to a field of order p^m . By the last theorem, $\text{GF}(p^m) \subseteq \text{GF}(p^n)$ as $m \mid n$. So f is the minimus polynomial of some element in $\text{GF}(p^n)$ and every element in $\text{GF}(p^n)$ is a root of $x^{p^n} - x$ and so $f(x) \mid x^{p^n} - x$.

Conversely, if $f(x)$ is an irreducible constituent of $x^{p^n} - x$ of degree m , then if β is a root of $f(x)$, $\beta \in \text{GF}(p^n)$. Adjoining β to \mathbb{F}_p gives a field $\text{GF}(p^m)$ but β is a root of $x^{p^n} - x$ and so also an element of $\text{GF}(p^n)$. Every element in $\text{GF}(p^m) = \mathbb{F}_p(\beta)$ can be written as a polynomial in β over \mathbb{F}_p and so we get $\text{GF}(p^m) \subseteq \text{GF}(p^n)$ which means $m \mid n$. ■

Remarks 5.10.29 Each factor in the factorisation above appears only once as all roots of $x^{p^n} - x$ are distinct.

Chapter 6

Vector-spaces over \mathbb{F}_2 and Error-correcting codes

6.1 Introduction

The idea over Error-correcting codes are a method to transmit information in such a way that it will be able to correct itself. Meaning if there is some disturbance on the line, it will be able to recover the original data. More-or-less like a spell check. For example if we take the word “elephant”, there is only one way to fix it to a valid word in english with changing only one letter.

So, the idea is:

Transmit information, with enough redundancy to enable reconstruction of original message even after errors appear.

The information assumed to binary.



Example 6.1.1 : We can transmit 11010111 3 times, and maybe we have error in some bits, and we got:

0	1	1	0	0	1	0	1
1	1	0	1	0	1	1	1
1	0	1	1	0	1	1	1

My using majority we will get:

1	1	1	1	0	1	1	1
---	---	---	---	---	---	---	---

We got only a error in one bit... but that was only a quick example.

This method is not very efficient, we transmit 3 times the amount of data that is required. We will see some better mechanisms.


6.2 Parity check digit

We transmit an extra digit:

$$\begin{cases} 1 & \text{if the number of 1s in the message is odd} \\ 0 & \text{if the number of 1s in the message is even} \end{cases}$$

So in the last example, we will send: 1 1 1 1 0 1 1 1 0.

The receiver can do a parity check to see if have an even number of 1s can conclude if there was an error if this is not the case.

 **Example 6.2.1 :** A famous example for parity check is the ID last digit:
For example, we have Aviv's ID:

$$\begin{array}{cccccc} 0 & 3 & 6 & 5 & 1 & 7 & 6 & 6 \\ 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 \\ 0 & 6 & 6 & 1 & 1 & 5 & 6 & 3 \end{array}$$

(We are multiplying the first line by the second modulu 10) So we sum it up and we get:

$$0 + 6 + 6 + 1 + 1 + 5 + 6 + 3 = 28$$

So the validity digit will be: $10 - 8 = 2$.

6.3 Hamming (7, 4)-code - single error correcting code.

We have 4 infomation digit. Let p be the probability of an error in transmission of a digit.

So, the probability of 4 correct digits is $(1 - p)^4$. The probability of 7 information digits containing ≤ 1 error is: $(1 - p)^7 + 7p(1 - p)^6$.

Note that if $p = 0.1$ then: $(1 - p)^4 = 0.6561$ but $(1 - p)^7 + 7p(1 - p)^6 = 0.8503$, thus the latter has higher probability (and it is true for a bunch of p).

Take the matrix:

$$\begin{array}{l} v_1 \\ v_2 \\ v_3 \\ v_4 \end{array} \begin{pmatrix} 1 & 0 & 0 & 0 & | & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & | & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & | & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & | & 1 & 1 & 1 \end{pmatrix}$$

The first 4 bits are the original bits, and the latter three are the correction.

Now sapce of this matrix over \mathbb{F}_2 is code.

This is a "linear code" i.e. set of codewords is a vector space. There are 16 codewords.

 **Example 6.3.1 :**

$$1 \ 1 \ 0 \ 1 \iff v_1 + v_2 + v_4 = 1 \ 1 \ 0 \ 1 \ 0 \ 0 \ 1$$

6.3.1 Efficient decoding

Take the vectors:

$$\begin{array}{lcl} a & = & (0 \ 0 \ 0 \ 1 \ 1 \ 1 \ 1) \\ b & = & (0 \ 1 \ 1 \ 0 \ 0 \ 1 \ 1) \\ c & = & (1 \ 0 \ 1 \ 0 \ 1 \ 0 \ 1) \end{array}$$

Use an analogue to scalar products between vectors in \mathbb{F}_2 :

$$(x_1, \dots, x_n) \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \sum_{i=1}^n x_i y_i$$

(Matrix multiplication and it is a bilinear form).

Remarks 6.3.2 $\vec{v} \cdot \vec{v} = 0$ does not imply $v = 0$!

 **Example 6.3.3 :** $(1, 1, 0, 1) \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} = 1 + 1 = 0.$

Suppose our received message is:

$$y^* = (1 \ 1 \ 0 \ 1 \ 1 \ 1 \ 0)$$

Note that:

$$(1 \ 1 \ 0 \ 0 \ 1 \ 1 \ 0) = v_1 + v_2$$

So the message differs from a codeword by 1 digit.

Note that:

$$\begin{aligned} y^* \cdot a &= (1 \ 1 \ 0 \ 1 \ 1 \ 1 \ 0) \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = 1 \\ y^* \cdot b &= (1 \ 1 \ 0 \ 1 \ 1 \ 1 \ 0) \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} = 0 \\ y^* \cdot c &= (1 \ 1 \ 0 \ 1 \ 1 \ 1 \ 0) \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} = 0 \end{aligned}$$

We look at the binary number $100_{(2)} = 4$, so the error is in the 4-th digit which is true!

How does it work? Recall that if $W \subseteq V$ subspace of a vector space V over F , then if $B : V \times V \rightarrow F$ is a bilinear form, we can define:

$$w^\perp = \{v \in V \mid B(u, v) = 0 \ \forall u \in W\}$$

Remarks 6.3.4 Since we have:

$$B(\alpha u_1 + \beta u_2, v) = \alpha B(u_1, v) + \beta B(u_2, v)$$

It follows that w^\perp is a vector space.

Theorem 6.3.5

$$\dim W + \dim W^\perp = \dim V.$$

Remarks 6.3.6 Need not have $W \cap W^\perp = \{0\}$ (It is only valid for char 0, not in general, for example over \mathbb{F}_2 take a vector with even number of ones and you will get that it is orthogonal to itself).



Example 6.3.7 : If $W = \text{span}\{(0, 1, 0, 1)\}$ then $W \subsetneq W^\perp$, they are not equal because $\dim W^\perp = 3$.

Remarks 6.3.8 The vectors: a, b, c are orthogonal to all rows of the code matrix and they are linear independent, and so they span the orthogonal complement of the code.

Remarks 6.3.9 $(W^\perp)^\perp = W$.

So we conclude: $y \in C \iff y \cdot a = y \cdot b = y \cdot c = 0$.

Now, the matrix whose columns are a basis for C^\perp is called the parity check matrix. Write a, b, c as columns:

$$H = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$

We have: $y \cdot H = (0 \ 0 \ 0) \iff y \in C$.

Suppose y^* has 1 error in position i so: $y^* = y + e_i$, where $y \in C$. So:

$$y^* H = yH + e_i H = \text{row } i \text{ in matrix } H = i \text{ in binary form!}$$

Remarks 6.3.10 Code can correct single errors only if codewords differ from each other in more than 2 digits.

We had: $H =$ columns of H basis for C^\perp . If y^* contained single error in position i then: Hy^* gave us the row i of H .

Words in the Hamming code differ by at least 3 digits. So, single errors lead to self-correction.

If that wasn't the case then there might have 2 words: $y_1, y_2 \in C$ s.t. $y_2 + e_j = y^* = y_1 + e_i$. Giving: $Hy^* = \text{row } i$ of $H = \text{row } j$ of H . In our case, rows of H are distinct so this doesn't happen.

Definition 6.3.11 For v, w vectors in $\mathbb{F}_2^{(n)}$ define Hamming distance d to be:

$$d(v, w) = \# \text{ of places where } v \text{ and } w \text{ differ}$$

To have a single error correction need $d(v, w) \geq 3$ for all v, w in code.

To have correction of errors need $d(v, w) \geq 2r + 1$ for all v, w in code.



Example 6.3.12 : For Hamming (7, 4) code:

Had 16 codewords.

In vector space we have $2^7 = 128$ vectors. $\#$ vectors with ≤ 1 error $= 16 + 7 \cdot 16 = 16 \cdot 8 = 127$

6.4 Double-error correcting code - Bose-Chaudhuri-Hocquenghem code

This code uses $\text{GF}(16)$.

Had α root of $x^4 + x^3 + 1$, $\langle \alpha \rangle = \text{GF}(16)^*$.

We construct code indirectly, by first constructing parity check matrix whose rows will span C^\perp . And then we have $H \cdot y = 0 \iff y \in C$.

We want multiplication by H to detect ≤ 2 errors.

Eventually the code we define will be a subspace of $\mathbb{F}_2^{(15)}$.

H will be 8×15 of the form:

$$H = \begin{pmatrix} \vec{b}_1 & \vec{b}_2 & \dots & \vec{b}_{15} \\ \vec{c}_1 & \vec{c}_2 & \dots & \vec{c}_{15} \end{pmatrix}$$

b_i and c_i are vectors in $\mathbb{F}_2^{(4)}$ and so can be considered elements of $\text{GF}(16)$.

For convenience we use $H' = 2 \times 15$ matrix whose entries are powers of α (each power corresponds to vector in $\mathbb{F}_2^{(4)}$).

Suppose $x = \begin{pmatrix} x_1 \\ \vdots \\ x_{15} \end{pmatrix}$ message, $x_i \in \{0, 1\}$:

$$Hx = \begin{pmatrix} \sum \vec{b}_i x_i \\ \sum \vec{c}_i x_i \end{pmatrix}$$

If $x = x_c + e_i + e_j$, with x_c a codeword (i.e. x has errors in positions i and j). We get:

$$Hx = \begin{pmatrix} b_i + b_j \\ c_i + c_j \end{pmatrix}$$

We want to be able to determine i and j uniquely from $\begin{cases} b = b_i + b_j \\ c = c_i + c_j \end{cases}$.

Denote:

$$H = \begin{pmatrix} 1 & \alpha & \dots & \alpha^{14} \\ & & & \end{pmatrix}$$

If $c_i = (b_i)^2$ then since we are in char2 we get:

$$\begin{aligned} b &= b_i + b_j \\ c &= b_i^2 + b_j^2 = (b_i + b_j)^2 \end{aligned}$$

So c doesn't add information. So we take:

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{14} \\ 1 & \alpha^3 & \alpha^6 & \dots & \alpha^{42} = \alpha^{12} \end{pmatrix}$$

Claim 6.4.1

Being given $b_i + b_j$ and $b_i^3 + b_j^3$ we can recover i and j uniquely.

Proof:

$$c = b_i^3 + b_j^3 = \underbrace{(b_i + b_j)}_b (b_i^2 + b_i b_j + b_j^2) = b \left(\underbrace{b_i^2 + b_j^2}_{b^2} + b_i b_j \right)$$

Note $b \neq 0$ as columns are distinct.

So we get:

$$b^{-1}c + b^2 = b_i b_j$$

b_i and b_j are roots of the quadratic polynomial over $\text{GF}(16)$.

$$(x + b_i)(x + b_j) = x^2 + \underbrace{(b_i + b_j)}_b x + \underbrace{b_i b_j}_{b^{-1}c + b^2}$$

Given the vector $\begin{pmatrix} b \\ c \end{pmatrix}$ construct the polynomial:

$$x^2 + bx + (b^{-1}c + b^2)$$

and solve over $\text{GF}(16)$. If cannot be solved - must have > 2 errors. ■

 **Example 6.4.2 :** Suppose y is a received message with 2 errors in position i and j and that:

$$Hy = \begin{pmatrix} \alpha^5 \\ \alpha^7 \end{pmatrix} = \begin{pmatrix} b \\ c \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

Form the polynomial: $x^2 + \alpha^5 x + \alpha^8$ we get:

$$b^{-1}c + b^2 = \alpha^{-5}\alpha^7 + \alpha^{10} = \alpha^2 + \alpha^{10} = (0 \ 1 \ 0 \ 0) + (1 \ 0 \ 1 \ 0) = (1 \ 1 \ 1 \ 0) = \alpha^8$$

So:

$$\begin{aligned} \alpha^5 &= b_i + b_j = \alpha^{i-1} + \alpha^{j-1} \\ \alpha^8 &= b_i b_j = \alpha^{i-1+j-1} \\ 8 &\equiv i + j - 2 \pmod{15} \\ i + j &\equiv 10 \pmod{15} \end{aligned}$$

Now we simply check pairs and we will get $i = 3, j = 7$ works! as $\alpha^2 + \alpha^6 = \alpha^5$.

What if y contains a single error in position i ?

$$\begin{pmatrix} b \\ c \end{pmatrix} = \begin{pmatrix} b_i \\ b_i^3 \end{pmatrix}$$

This is only situation in which $c = b^3$. So don't form polynomial. Simply determine i from $b = b_i$.

Could happen get: $b = 0$ and $c \neq 0$ in which case also have > 2 errors.

Having constructed H we now construct a matrix for the code and determine its dimension.

Claim 6.4.3

$\text{rank} H = 8$ (So the code is of dimension 7).

Proof: We show that field of 8 columns of H are linear independent (So $\text{rank} H = 8$) over \mathbb{F}_2 as elements of \mathbb{F}_2^8 .

Assume not, so have $a_i \in \mathbb{F}_2$ s.t.

$$\sum_{i=1}^8 a_i \begin{pmatrix} b_i \\ b_i^3 \end{pmatrix} = 0$$

$$\text{So: } \sum_{i=1}^8 a_i \begin{pmatrix} \alpha^{i-1} \\ \alpha^{3i-3} \end{pmatrix} = 0 \iff \begin{cases} \sum_{i=1}^8 a_i \alpha^{i-1} = 0 & \iff \sum a_i \alpha^i = 0 \\ \sum_{i=1}^8 a_i \alpha^{3i-3} = 0 & \iff \sum a_i \alpha^{3i} = 0 \end{cases}.$$

So α is a root of $\sum_{i=1}^8 a_i x^i$, α has $x^4 + x^3 + 1$ as it's minimal polynomial.

Also α^3 is a root of $\sum_{i=1}^8 a_i x^i$, so $x^4 + x^3 + 1 \mid \sum_{i=0}^7 a_{i-1} x^i$.

The minimal polynomial of α^3 is $x^4 + x^3 + x^2 + x + 1$ so:

$$x^4 + x^3 + 1, x^4 + x^3 + x^2 + x + 1 \mid \underbrace{\sum_{i=0}^7 a_{i-1} x^i}_{\text{of degree at most 7}}$$

(Those two element are irreducible and mutually prime).

We get that $\sum_{i=0}^7 a_{i-1}x^i \equiv 0$ polynomial, otherwise get a contradiction! so $a_i = 0$ for all i . ■

We now construct code matrix so that last 7 columns are $I_{7 \times 7}$.

$$C = (\text{Redundancy digits} \mid I_{7 \times 7})$$

We know: $\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} \alpha \\ \alpha^3 \end{pmatrix}, \dots, \begin{pmatrix} \alpha^7 \\ \alpha^{21} \end{pmatrix}$ these are the first 8 columns of H , they span all the columns of H . So there exist $s_0, s_1, \dots, s_7 \in \{0, 1\}$ s.t.:

$$\sum_{i=0}^7 s_i \begin{pmatrix} \alpha^i \\ \alpha^{3i} \end{pmatrix} = \begin{pmatrix} \alpha^8 \\ \alpha^{24} \end{pmatrix}$$

So the row vector:

$$(s_0 \ s_1 \ \dots \ s_7 \ 1 \ 0 \ \dots \ 0)$$

(6 zeroes at the end) is orthogonal to all columns of H .

There exists $t_0, \dots, t_7 \in \{0, 1\}$:

$$\sum_{i=0}^7 t_i \begin{pmatrix} \alpha^i \\ \alpha^{3i} \end{pmatrix} = \text{column 9 of } H = \begin{pmatrix} \alpha^9 \\ \alpha^{27} \end{pmatrix}$$

So row vector:

$$(s_0 \ s_1 \ \dots \ s_7 \ 0 \ 1 \ 0 \ \dots \ 0)$$

(5 zeroes at the end) is orthogonal to all columns of H . similarly for columns 10, ..., 15 of H .

Get:

$$\left(\begin{array}{ccc|ccc} s_0 & \dots & s_7 & 1 & 0 & \dots & \dots & 0 \\ t_0 & \dots & t_7 & 0 & 1 & 0 & \dots & 0 \\ \vdots & & & \vdots & & \ddots & & \end{array} \right)$$

Remarks 6.4.4 Out of topic: Fields of fraction

If R is a commutative domain, we can construct a field $F \supseteq R$ which is minimal, called its field of fractions.

Define an equivalent relation on ordered pairs - $R \times (R \setminus \{0\})$. $(a, b) \approx (c, d) \iff ad = bc$.

Look at equivalent classes: For any $a \in R$, $b \in R \setminus \{0\}$, $\frac{a}{b} = \left\{ (c, d) \mid (a, b) \approx (c, d) \quad c, \underbrace{d}_{\neq 0} \in R \right\}$.

Define addition and multiplication on equivalent classes: $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$, $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ (need to show well-defined), get a field F .

$R \cong \left\{ \frac{a}{1} \mid a \in R \right\}$.



Example 6.4.5 : $R = F[x]$, F field. The field of fraction is called field of rational functions.

Chapter 7

Groups

7.1 $\text{GL}(n, q)$

Last lesson we've calculated the order of the group:

$$\begin{aligned}\text{GL}(n, q) &= (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1}) \\ &= q^{1+2+3+\dots+n-1} (q^n - 1)(q^{n-1} - 1) \cdots (q - 1) \\ &= q^{\frac{n(n-1)}{2}} (q^n - 1) \cdots (q - 1)\end{aligned}$$

Now, note that:

$$\text{GL}(n, q)/\text{SL}(n, q) \cong F^*$$

And:

$$|\text{SL}(n, q)| = q^{\frac{n(n-1)}{2}} (q^n - 1)(q^{n-1} - 1) \cdots (q - 1)$$

7.1.1 Sylow subgroups

Now, assume that $q = p^k$ for some prime p .

What are the Sylow p -subgroups where $p = \text{char} F_q$? Any Sylow p -subgroup of $\text{SL}(n, q)$ will also be a Sylow p -subgroup of $\text{GL}(n, q)$.

Look at the subgroup:

$$H = \left\{ \begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \right\}$$

Clearly H is a subgroup of $\text{GL}(n, q)$ and it's clear that $H \subseteq \text{SL}(n, q)$.

Moreover, it is obvious that:

$$|H| = q^{1+2+\dots+n-1} = q^{\frac{n(n-1)}{2}}$$

We have q choices for each position in the matrix above the main diagonal. So, $H \in \text{Syl}_p(\text{SL}(n, q))$.

We can also take:

$$H^T = \left\{ \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ * & & 1 \end{pmatrix} \right\}$$

It is also of the same order, so $n_p \neq 1$.

Denote:

$$\text{SL}(n, q)/Z(\text{SL}(n, q)) = \text{PSL}(n, q)$$

14/01/2014
Missing a l

Where:

$$Z(SL(n, q)) = \text{set of scalar matrices } \begin{pmatrix} \alpha & & 0 \\ & \ddots & \\ 0 & & \alpha \end{pmatrix} \text{ where } \alpha^n = 1$$

$\alpha \in GF(q)^*$, and $|GF(q)| = q - 1$.

So if $(n, q - 1) = 1$ then $\alpha^n = 1 \iff \alpha = 1$ for $\alpha \in \mathbb{F}_q^*$. and then $PSL(n, q) = SL(n, q)$.

But in general, if $(n, q - 1) = d$ then $|Z(SL(n, q))| = d$.

Theorem 7.1.1

$PSL(n, q)$ are simple groups for all $n > 2$ and for $n = 2$ except when $q = 2$ or $q = 3$.

7.2 Conjugate classes in $GL(n, F)$

Theorem 7.2.1

2 matrices are similar (i.e. conjugate) in $GL(n, \overline{F}) \iff$ they have the same Jordan form over \overline{F} (The algebraic closure of F).



Example 7.2.2 : $GL(2, \mathbb{C})$.

We may as well take representative of classes to be in Jordan form.

The possible Jordan forms, for $\alpha \neq 0$:

$$\underbrace{\begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}}_{\text{central elements}}, \underbrace{\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}}_{\alpha \neq \beta}, \begin{pmatrix} \alpha & 1 \\ 0 & \alpha \end{pmatrix}$$

Each central element constitutes a class:

$$\text{cl} \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} \right\} = \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} \right\}$$

In case that $\alpha \neq \beta$:

$$\text{cl} \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \right\} = \text{cl} \left\{ \begin{pmatrix} \beta & 0 \\ 0 & \alpha \end{pmatrix} \right\} = \text{all matrices whose char polynomial is } (x - \alpha)(x - \beta)$$

Since:

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} \beta & 0 \\ 0 & \alpha \end{pmatrix}$$

And for last:

$$\text{cl} \left\{ \begin{pmatrix} \alpha & 1 \\ 0 & \alpha \end{pmatrix} \right\} = \text{set of all matrices whose char polynomial is } (x - \alpha)^2 \text{ but are not diagonalizable.}$$

Theorem 7.2.3

2 matrices are conjugate in $GL(n, q)$ if and only if they have the same Jordan form in $GL(n, \overline{\mathbb{F}}_q)$.

For example, let's take a look at: $GL(2, 3)$.

First note that the order of the group is:

$$|GL(2, 3)| = (3^2 - 1)(3^2 - 3) = 8 \cdot 6 = 48 = \boxed{16 \cdot 3}$$

A sylow 3-subgroup = $\left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{F}_3 \right\}$ of order 3, there might be more than one sylow 3-subgroup, in fact $n_3 \neq 1$, so according to sylow third theorem we will get that $n_3 \mid 16$ so: $n_3 = 4$ or 16 .

Sylow 2-subgroup of order 16: $n_2 \mid 3$ and $n_2 \equiv 1 \pmod{2}$ so $n_2 = 1$ or 3 .

Remarks 7.2.4 All char polynomials are quadratic (as matrices are 2×2). Moreover, every monic quadratic polynomial is the char polynomial of a matrix as if:

$$A = \begin{pmatrix} 0 & 1 \\ -b & -a \end{pmatrix} = \text{The companion matrix of } \lambda^2 + a\lambda + b$$

We get that:

$$|A - \lambda I| = \begin{vmatrix} -\lambda & 1 \\ -b & -a - \lambda \end{vmatrix} = (a + \lambda)\lambda + b = \boxed{\lambda^2 + a\lambda + b}$$

Case 1: Char polynomial factors over \mathbb{F}_3 .

This gives 3 possible forms:

1. $\begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}$ with $\alpha \neq 0$.
2. $\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$ with $\alpha \neq \beta$.
3. $\begin{pmatrix} \alpha & 1 \\ 0 & \alpha \end{pmatrix}$ with $\alpha \neq 0$.

Denote $GF(3) = \{0, 1, 2\}$, and analyze each of this forms:

1. We have 2 classes of central elements:

$$\underbrace{\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}}_{\text{of order 1}}, \underbrace{\left\{ \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \right\}}_{\text{of order 2}}$$

2. In this case we have only one class:

$$\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$$

Because $\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$ is conjugate to this. So we only have one conjugate class. Elements are of order 2 as:

$$\left| \text{cl} \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \right\} \right| = \frac{|G|}{\left| C_G \left(\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \right) \right|}$$

Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = A \in C_G \left(\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \right)$ if and only if:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \iff \begin{pmatrix} a & 2b \\ c & 2d \end{pmatrix} = \begin{pmatrix} a & b \\ 2c & 2d \end{pmatrix} \iff \begin{cases} c = 0 \\ b = 0 \end{cases}$$

Meaning that:

$$C_G \left(\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \right) = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \mid a, d \neq 0 \right\} \Rightarrow \left| C_G \left(\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \right) \right| = 4$$

So:

$$\left| \text{cl} \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \right\} \right| = 12$$

3. Here we have 2 classes:

$$\underbrace{\text{cl} \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\}}_{\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ of order 3}}, \underbrace{\text{cl} \left\{ \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix} \right\}}_{\begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix} \text{ of order 6}}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \iff \begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix} \iff \begin{cases} a = d \\ c = 0 \end{cases}$$

So:

$$C_G \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \right\} \Rightarrow \left| C_G \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right| = 6$$

Thus:

$$\left| \text{cl} \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\} \right| = 8$$

Also:

$$\left| \text{cl} \left\{ \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix} \right\} \right| = 8$$

Case 2: char polynomials does not factor over $\text{GF}(3)$.

So it factors over $\text{GF}(q)$ and the roots are distinct. The possibilities for quadratic polynomials that does not factor over $\text{GF}(3)$ are:

$$\begin{cases} x^2 + x + 2 \\ x^2 + 2x + 2 \\ x^2 + 1 \end{cases}$$

Let α be the root of $x^2 + x + 2$. So $\alpha \in \text{GF}(q)^*$, can check to see $\alpha^2 \neq 1$, $\alpha^4 \neq 1$ so $\langle \alpha \rangle = \text{GF}(q)^*$.

So the roots of $x^2 + x + 2$ are α, α^3 and we will fill the roots simply by checking:

$$\begin{cases} x^2 + x + 2 & \alpha, \alpha^3 \\ x^2 + 2x + 2 & \alpha^5, \alpha^7 \\ x^2 + 1 & \alpha^2, \alpha^6 \end{cases}$$

From the companion matrix, we can find a class representative for each of the polynomials:

$$\begin{cases} x^2 + x + 2 & \alpha, \alpha^3 & \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix} \\ x^2 + 2x + 2 & \alpha^5, \alpha^7 & \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \\ x^2 + 1 & \alpha^2, \alpha^6 & \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix} \end{cases}$$

In $\text{GF}(2, q)$ we get that: $\begin{pmatrix} \alpha & 0 \\ 0 & \alpha^3 \end{pmatrix}$ is conjugate to $\begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}$, so we know the order of the elements:

$$\begin{array}{ccc} \text{Class sizes} & & \\ \underbrace{6} & \begin{cases} x^2 + x + 2 & \alpha, \alpha^3 & \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix} & \text{order: 8} \\ 6 & \begin{cases} x^2 + 2x + 2 & \alpha^5, \alpha^7 & \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} & \text{order: 8} \\ 6 & \begin{cases} x^2 + 1 & \alpha^2, \alpha^6 & \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix} & \text{order: 4} \end{cases} \end{cases} \end{array}$$

If we count, we see that: $6 + 6 + 6 + 1 + 1 + 8 + 8 + 12 = 48$. So, we've got everything.

We can conclude that $n_2 = 3$ as there are more than 15 2-elements.

What about elements of order 3? In each 3 group we have exactly 2 elements of order 3. The only class of order 3 is $\text{cl} \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\}$. And this class have 8 elements. Thus, each 2 sylow 3-subgroups intersect trivially. So $n_3 = 4$.

In $\text{SL}(n, q)$ 2 matrices, A, B , are conjugate if and only if $\exists P \in \text{SL}(n, q)$ s.t. $P^{-1}AP = B$.

7.3 Conjugate classes in S_n

Notation: If i_1, \dots, i_k are distinct elements in $\{1, \dots, n\}$ we denote $(i_1 \ i_2 \ \dots \ i_k)$ permutation that is the cycle $i_1 \mapsto i_2 \mapsto i_3 \mapsto \dots \mapsto i_k \mapsto i_1$ and fixes all other indices.

Fact: Any permutation can be written as a product of distinct cycles.



Example 7.3.1 :

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 4 & 5 & 2 & 1 & 6 \end{pmatrix} = (1 \ 3 \ 5)(2 \ 4)$$

We write action of σ on i , $\sigma(i)$ as i^σ . The action of permutations is read left to right:

$$i^{\sigma\tau} = (i^\sigma)^\tau$$

So left-most permutation acts first.

Claim 7.3.2

If $\sigma \in S_n$ and $(i_1 \ \dots \ i_k)$ a cycle in S_n then:

$$\sigma^{-1} (i_1 \ \dots \ i_k) \sigma = (i_1^\sigma \ i_2^\sigma \ \dots \ i_k^\sigma)$$

Proof: We need to show that both sides of the equation give the same permutation.

Let $j \in \{1, 2, \dots, n\}$.

Case 1: $j \notin \{i_1^\sigma, \dots, i_k^\sigma\}$.

So $j(i_1^\sigma \ \dots \ i_k^\sigma) = j$, and ofcourse $j^{\sigma^{-1}} \notin \{i_1, \dots, i_k\}$ as permutations are 1-1. So: $j^{\sigma^{-1}}(i_1 \ \dots \ i_k)^{\sigma^\sigma} = j^{\sigma^{-1}\sigma} = j$ as $j^{\sigma^{-1}}(i_1 \ \dots \ i_k) = j^{\sigma^{-1}}$.

Case 2: $j \in \{i_1^\sigma, \dots, i_k^\sigma\}$ wlog $j = i_1^\sigma$ so $j^{\sigma^{-1}} = i_1$:

$$\begin{cases} j^{\sigma^{-1}}(i_1 \ \dots \ i_k)^\sigma = i_1(i_1 \ \dots \ i_k)^\sigma = i_2^\sigma \\ j(i_1^\sigma \ \dots \ i_k^\sigma) = i_2^\sigma \end{cases}$$

Corollary 7.3.3

2 permutations are conjugate if and only if they have the same cycle structure when decomposed as a product of disjoint cycles.

Remarks 7.3.4 This follows from the fact that any 2 cycles of the same length are conjugate as if we have:


$$(i_1 \ \dots \ i_k), (j_1 \ \dots \ j_k)$$

Where the i_1, \dots, i_k are distinct and the j_1, \dots, j_k are distinct. Taking σ to be the permutation s.t.:

$$\begin{aligned} i_1 &\mapsto j_1 \\ i_2 &\mapsto j_2 \\ &\vdots \\ i_k &\mapsto j_k \end{aligned}$$

and fixing everything else. Then we have:

$$\sigma^{-1} (i_1 \ \dots \ i_k) \sigma = (j_1 \ \dots \ j_k)$$

 **Example 7.3.5 :** Supposing we have:

$$\begin{aligned}\sigma &= (2 \ 4 \ 5)(1 \ 3)(6 \ 7) \\ \tau &= (1 \ 6 \ 2)(3 \ 4)(5 \ 7)\end{aligned}$$

Take:

$$\chi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 1 & 4 & 6 & 2 & 5 & 7 \end{pmatrix}$$

Then: $\chi^{-1}\sigma\chi = \tau$.

 **Example 7.3.6 :** S_4 .

In S_4 the class representative will be: $\text{Id}, (1 \ 2), (1 \ 2 \ 3), (1 \ 2 \ 3 \ 4), (1 \ 2)(3 \ 4)$.
And that's it. This is the only way we can partition S_4 .

Remarks 7.3.7 $(i_1 \ \dots \ i_k)$ is of order k . Cycles of odd length are even permutations.

7.4 Solvable Groups

Definition 7.4.1 G is solvable if there exists a normal series:

$$1 = G_1 \triangleleft G_2 \triangleleft \dots \triangleleft G_n$$

s.t. $G_i \triangleleft G_{i+1}$ and G_{i+1}/G_i abelian for all i .

 **Example 7.4.2 :**

$$1 \triangleleft H \triangleleft V_4 \triangleleft A_4 \triangleleft S_4$$

Remarks 7.4.3 If we have such a series we can always find a normal series in which the quotients are cyclic.

 **Example 7.4.4 :** More examples:

- S_4
- Any abelian group is solvable.
- Any nonabelian simple group is not solvable e.g. A_5 is not solvable.
- S_5 is not solvable. Because $A_5 \triangleleft S_5$. If we had:

$$1 = G_1 \triangleleft G_2 \triangleleft \dots \triangleleft G_n = S_5$$

We will get a normal series:

$$1 = G_1 \cap A_5 \triangleleft G_2 \cap A_5 \triangleleft \dots \triangleleft G_n \cap A_5 = A_5$$

So, using the fact that A_5 is not solvable we can deduce that so is S_5 .

Claim 7.4.5

Finite p -groups are solvable.

Proof: If our group is abelian then it is solvable. Assume not.

We showed already that the center of a p -group is nontrivial.

We take $G_2 = Z(G)$. If the quotient $G/Z(G)$ is abelian we are done.

If not, as it is also a p -group, its center $Z(G/Z(G))$ is non trivial.

By the homomorphism theorem, this group is of the form $G_3/Z(G)$ where $G_3 \triangleleft G$.

Hence we have now: $1 = G_1 \triangleleft Z(G) = G_2 \triangleleft G_3$

If G/G_3 is abelian, we are done - if not we continue by taking its nontrivial center.

We reach G in finite number of steps because in each step the order is strictly increasing. ■

Remarks 7.4.6 This series is called the center series, in every group that we can do that is called a nilpotent group.

The notion of a solvable group goes back to Galois, and is of great importance in his proof that the general polynomial equation of degree n is not solvable by radicals.

Theorem 7.4.7

If $\text{char} F = 0$ and F contains a primitive n -th root of unity (i.e. $F \supseteq \mathbb{Q}(\sqrt[n]{1})$) then:

$\text{Gal}(K/F)$ is cyclic of order $n \iff K = F(\alpha)$ and α is a primitive n -th root of some element a of F

(In this situation: K is the s.f. of the polynomial $x^n - a$).

Corollary 7.4.8

If $f(x) \in \mathbb{Q}[x]$ and K is its s.f. then we get that $G = \text{Gal}(K/\mathbb{Q})$ is solvable \iff We have a sequence of fields:

$$\mathbb{Q} = K_1 \subseteq K_2 \subseteq \dots \subseteq K_s = K$$

s.t. $\text{Gal}(K_{i+1}/K_i)$ is cyclic and then it means K is generated over \mathbb{Q} by extending by roots of elements of each field (starting with \mathbb{Q}).

Hence: roots of $f(x)$ are expressible using 4 arithmetics operations and extracting roots (of any order) from \mathbb{Q} , i.e. "Solvable by radicals".

Conclusion: Not every polynomial of degree ≥ 5 is solvable by radicals, as for the general polynomial of degree n we get that the Galois group of the s.f. is S_n .

The proof is available at Jacobson - Basic Algebra I

For modern group theory the most important theorem regarding solvable group was proved in 1962:

Theorem 7.4.9 The Feit-Thompson Theorem(1962)

Finite groups of odd order are solvable.



Example 7.4.10 : Any group of order 3974821 is solvable.

Corollary 7.4.11

Every finite nonabelian simple group has even order.

The theorem was a first in many respects:

Apart from its mathematical importance, it had the longest proof of any theorem up to that time (proof of 252 pages)!

The proof used results of Brauer in modular

7.5 Classification of finite simple groups

Question: Is it possible to determine all the finite simple groups (up to isomorphism)?

Motivation: The classification of simple Lie groups, which suggested one could also characterize the structure of finite simple groups of Lie type.

Suggestion of Brauer(1954): If a nonabelian finite simple group had an involution(element of order 2), it would be possible to characterize the structure of all possible centralizers of the involution.

What do we mean by that?

If we have $x \in G$ s.t. $x^2 = -1$, we look at $C_G(x)$. If we know the structure of $C_G(x)$ can only be isomorphic to, say, 10 possibilities, then we can construct the group around the centralizers.

By Feit-Thompson: Every non-abelian simple group has an involution!

Clearly there are infinite number of isomorphism types - for instance:

- $\mathbb{Z}/p\mathbb{Z}$ for any prime p .
- A_n , $n \geq 5$.

There are also many infinite families of matrix group, for instance, if F is a field of order q :

- $\text{PSL}(n, q) = \text{SL}(n, q)/Z(\text{SL}(n, q))$ are simple unless $n = 2$, and $q = 2$ or 3 .

and many more.

It turns out that in addition to the infinite families of the types listed above, there are also examples of special simple groups:

In 1860 Mathieu discovered a simple group not of the above types. And then later found another 4 such groups: $M_{1,1}, M_{1,2}, M_{2,2}, M_{2,3}, M_{2,4}$.

Additional “sporadic” finite simple groups were discovered between 1965 (the Janko groups) and 1974 in an attempt to classify all finite simple groups (these were discovered by chance, by trying to build counter-examples!).

In 1972, Gorenstein suggested that it would be possible to give a complete list of finite simple groups involving the known infinite families plus a finite list of sporadic groups.

In 1976, it was in the final stages of proof, finally announced in 1980.

The statement of the theorem:

Theorem 7.5.1

If G is a finite simple group then it is one of the following:

- $\mathbb{Z}/p\mathbb{Z}$ for a prime p .
- A_n , $n \geq 5$.
- A simple matrix group over a finite field. (these are called groups of Lie type, there is a list of a finite number of types: classical families, exceptional families and twisted families).
- One of 26 sporadic groups.

Significance and implications: The proof was a huge step forward, it was not even believed possible in the early 70s!

It now means that many general theorems can be proved using the classification, by checking cases.

There is also the task of understanding the structure of the known groups, especially the stranger of the sporadic groups.

The proof consists of hundreds of papers - the first being the Feit-Thompson theorem.

In the 1990s Gorenstein, Lyons, and Solomon gradually published a simplified revised version of the proof (in 6 volumes)

7.5.1 The sporadic groups , the Fischer Griess Monster (1982)

In 1973, Fischer and Griess hypothesized the existence of a new gigantic simple group with very special properties.

Griess constructed it (thus proving its existence) in 1980.

John Thompson showed that the uniqueness would follow from a claim that was proved in 1990 by Griess, Meierfrankenfeld and Yoav Segev.