

# Algebraic Background

Ömer Küçüksakallı

Middle East Technical University



September 1, 2016  
ECC 2016 – Summer School

- 1 Rings
- 2 Field Extensions
- 3 Modules and Free Abelian Groups

This lecture is based on the textbooks:

- Stewart, Tall - Algebraic Number Theory and Fermat's Last Theorem
- Marcus - Number Fields

# Rings

- A **ring** is one of the fundamental algebraic structures.
- It consists of a set equipped with **two binary operations** that generalize the arithmetic operations of addition and multiplication.
- We use the notation  $(R, +, \cdot)$  to indicate a ring.
  - $(R, +)$  is an additive group: identity, inverse, associativity, commutativity.
  - Multiplication is associative:  $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
  - Distribution law holds:  $a \cdot (b + c) = a \cdot b + a \cdot c$
- Unless explicitly stated to the contrary, the term ring means a commutative ring with multiplicative identity  $1_R$ .

## Example

The number systems **Z**, **Q**, **R** and **C** are examples of rings under the usual addition and multiplication.

# Two different rings with the same additive structure

- The fundamental difference between an additive group and a ring is the additional structure given by the multiplication.
- For example consider the two classical example of rings:
  - $\mathbf{C}$  with usual addition and multiplication of complex numbers,
  - $\mathbf{R} \times \mathbf{R}$  with componentwise addition and multiplication.
- Note that both rings have the same underlying additive structure.
- How can we justify that these two algebraic objects are different as rings?

# Homomorphisms

- A ring **homomorphism**  $f : R \rightarrow S$  is a map between two rings  $(R, +, \cdot)$  and  $(S, \oplus, \odot)$  which respect the addition and multiplication on both rings. More precisely,
  - $f(1_R) = 1_S$ ,
  - $f(a + b) = f(a) \oplus f(b)$
  - $f(a \cdot b) = f(a) \odot f(b)$for all  $a, b \in R$ .
- Two rings are the “same” if there exists a a bijective ring homomorphism between them.
- Such a map is called an **isomorphism** of rings and such rings are called **isomorphic** rings.

# An example

## Example

The rings  $(\mathbf{C}, +, \cdot)$  and  $(\mathbf{R} \times \mathbf{R}, +, \cdot)$  are not isomorphic.

## Proof.

- Assume there exists an isomorphism  $f : \mathbf{C} \rightarrow \mathbf{R} \times \mathbf{R}$ .
- Set  $i = \sqrt{-1}$ , an element of  $\mathbf{C}$ . Then

$$f(i)^4 = f(i^4) = f(1_{\mathbf{C}}) = 1_{\mathbf{R} \times \mathbf{R}}.$$

- $1_{\mathbf{R} \times \mathbf{R}} = (1, 1)$  and we have  $f(i)^4 = (1, 1)$ .
- There can be no  $f(i) \in \mathbf{R} \times \mathbf{R}$  with this property. A contradiction



- An isomorphism of rings respects the properties of those rings. For example if one ring has no zero divisors then so is the other one.

- Groups have special subsets which are called subgroups.
- Any ring  $R$  has an underlying additive group structure and it has subgroups with respect to this structure.
- We introduce ideals which need special attention. An ideal is a nonempty subset  $I$  of  $R$  such that
  - $I$  is an additive subgroup of  $R$ , and
  - $r \cdot i \in I$  for every  $r \in R$  and  $i \in I$ .

## Example

- Ideals of  $\mathbf{Z}$  are of the form  $a\mathbf{Z} = \{ak : k \in \mathbf{Z}\}$ .
- There are only two ideals of  $\mathbf{Q}$ . Namely  $I_1 = \{0\}$  and  $I_2 = \mathbf{Q}$ .
- $\mathbf{Z}$  is an additive subgroup of  $\mathbf{Q}$  but it is not an ideal of  $\mathbf{Q}$ .



- If  $N$  is a normal subgroup of a group  $G$ , then one can introduce the quotient group  $G/N$  on which there is a natural well-defined group operation. This construction can be generalized to rings!
- The elements of the quotient ring  $R/I$  are cosets

$$r + I = \{r + i : i \in I\}.$$

- The addition and multiplication are defined respectively by
  - $(r + I) \oplus (s + I) = (r + s) + I$ , and
  - $(r + I) \odot (s + I) = (r \cdot s) + I$ .
- The second operation, namely the multiplication, is well-defined because  $r \cdot i \in I$  for every  $r \in R$  and  $i \in I$ .

# The first isomorphism theorem

- Let  $f : R \rightarrow S$  be a homomorphism. The kernel and the image are defined as follows:

$$\begin{aligned}\text{Ker}(f) &= \{r \in R : f(r) = 0_S\}, \\ \text{Im}(f) &= \{f(r) : r \in R\}.\end{aligned}$$

- The kernel is an ideal of  $R$ .
- The image is a subring of  $S$ .
- The first isomorphism theorem states that

$$R/\text{Ker}(f) \cong \text{Im}(f).$$

# Generating ideals

- The ideal generated by a set  $X$  of  $R$  is the smallest ideal of  $R$  containing  $X$ . Such an ideal is denoted by  $\langle X \rangle$ .
- If there exist a finite subset  $X = \{x_1, x_2, \dots, x_n\}$  of  $R$  such that  $I = \langle X \rangle$ , then we say that  $I$  is finitely generated. We write

$$\langle X \rangle = \langle x_1, x_2, \dots, x_n \rangle$$

- If  $I = \langle x \rangle$  for some  $x \in R$ , then we say that  $I$  is the principal ideal generated by  $x$ .

## Example

If  $m, n \in \mathbf{Z}$ , then  $\langle m, n \rangle = \langle \gcd(m, n) \rangle$ .

# Principal ideal domains

- An integral domain is a ring with no zero divisors. A principal ideal domain, or PID, is an integral domain in which every ideal is principal.
- Let  $S$  be a ring with a subring  $R$  and a subset  $X$ . The notation  $R[X]$  indicates the smallest subring of  $S$  containing both  $R$  and  $X$ .

## Example

The following are examples of PIDs.

- $\mathbf{Z}, \mathbf{Z}[\sqrt{-1}], \mathbf{Z}[\sqrt{2}], \mathbf{Z}\left[\frac{\sqrt{-19}+1}{2}\right]$ .
- A ring of the form  $\mathbf{Z}[\sqrt{d}]$  where  $d \in \mathbf{Z}$  is not always a PID. A classical example is  $\mathbf{Z}[\sqrt{-5}]$  with a non-principal ideal  $\langle 2, 1 + \sqrt{-5} \rangle$ .
- Why does not  $\gcd(2, 1 + \sqrt{-5})$  work?

- A field is a ring in which every non-zero element has a multiplicative inverse.
- Let  $\mathbf{F}$  be a field. The polynomial ring  $\mathbf{F}[x]$  is a principal ideal domain. This can be justified by using the Euclidean algorithm.
- The polynomial ring  $\mathbf{Z}[x]$  is not a principal ideal domain. An example of a non-principal ideal is  $I = \langle x, 2 \rangle$ .

# Unique factorization domains

- A unique factorization domain, or UFD, is an integral domain in which every non-zero non-unit element can be written as a product of prime elements (or irreducible elements), uniquely up to order and units.
- Any PID is a UFD. If  $R$  is a UFD, then so is the polynomial ring  $R[x]$ .
- The ring  $\mathbf{Z}[\sqrt{-5}]$  is not UFD because there are distinct factorizations such as

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

- (Alternatively  $\mathbf{Z}[\sqrt{-5}]$  is a Dedekind domain that is not a PID. If  $R$  is a Dedekind domain, then  $\text{PID} \Leftrightarrow \text{UFD}$ .)
- The ring  $\mathbf{Z}[x]$  is an example of a UFD which is not a PID.

# Factorization of elements

- The “factorization” in the ring  $\mathbf{Z}[\zeta_p]$  plays an important role while studying the solutions of the Diophantine equation  $x^p + y^p = z^p$ .
- There are two distinct properties that can be used to serve as a definition:

## Definition

A non-zero non-unit element  $\pi \in R$  is called prime if

$$\pi \mid ab \text{ for some } a, b \in R \implies \pi \mid a \text{ or } \pi \mid b.$$

## Definition

A non-zero non-unit element  $\pi \in R$  is called irreducible if

$$\pi = ab \text{ for some } a, b \in R \implies a \text{ is a unit or } b \text{ is a unit.}$$

- Every prime element is irreducible. However the converse is not true. For example 2 is irreducible in  $\mathbf{Z}[\sqrt{-5}]$  but it is not prime.

- A proper ideal  $P$  of a ring  $R$  is prime if it satisfies

$$ab \in P \text{ for some } a, b \in R \implies a \in P \text{ or } b \in P.$$

- A proper ideal  $M$  of a ring  $R$  is maximal if it is maximal (with respect to set inclusion) amongst all proper ideals.
- $R/I$  is a field if and only if  $I$  is maximal.
- $R/I$  is an integral domain if and only if  $I$  is prime.
- (Maximal  $\implies$  Prime) because (Field  $\implies$  Integral Domain).



# Field Extensions

- Field extensions often arise in a slightly more general context as a monomorphism  $\sigma : K \rightarrow L$  where  $K$  and  $L$  are fields.
- It is customary to identify  $K$  with its image  $\sigma(K)$ , which is a subfield of  $L$ . We denote such an extension by  $L/K$ .
- If  $L/K$  is a field extension then  $L$  has a natural structure as a vector space over  $K$ .
- The dimension of this vector space is called the degree of the extension and written as  $[L : K]$ .
- The degree is multiplicative in towers.

## Theorem

*If  $M \supseteq L \supseteq K$  are fields, then  $[M : K] = [M : L][L : K]$ .*

# Algebraic and transcendental elements

- Given an extension  $L/K$  and an element  $\alpha \in L$ ,
  - if there exists a non-zero polynomial  $P(x) \in K[x]$  such that  $P(\alpha) = 0$ , then we say that  $\alpha$  is algebraic,
  - if not, then we say that  $\alpha$  is transcendental.
- If  $\alpha$  is algebraic over  $K$ , then there exists a unique monic polynomial satisfied by  $\alpha$  whose degree is minimal. We write

$$\min_{\alpha, K} \in K[x].$$

## Example

If  $\alpha = \exp(2\pi i/8)$ , then  $\min_{\alpha, \mathbf{Q}} = x^4 + 1 \in \mathbf{Q}[x]$ .

## Example

If  $\beta = \exp(2\pi i/5) + \exp(-2\pi i/5)$ , then  $\min_{\beta, \mathbf{Q}} = x^2 + x - 1 \in \mathbf{Q}[x]$ .

# Transcendental extensions

- If  $X$  is a subset of  $L$ , we write  $K(X)$  for the smallest subfield of  $L$  containing  $K$  and  $X$ .
- If  $\alpha \in L$  is transcendental over  $K$ , then  $Q(\alpha) \neq 0$  for all non-zero polynomials  $Q \in K[x]$ . In this case,

$$K(\alpha) = \left\{ \frac{P(\alpha)}{Q(\alpha)} : P, Q \neq 0 \in K[x] \right\}.$$

- One can consider an indeterminate  $x$ , then the field of rational functions is

$$K(x) = \left\{ \frac{P}{Q} : P, Q \neq 0 \in K[x] \right\}.$$

- We have  $[K(x) : K] = \infty$ .

## Theorem

If  $\alpha \in L$  is algebraic over  $K$ , then  $[K(\alpha) : K] < \infty$ . In this case,

- $[K(\alpha) : K] = \deg(\min_{\alpha, K})$ , and
- $K(\alpha) = K[\alpha]$ .

## Proof.

- Set  $n = \deg(\min_{\alpha, K})$ . In order to see that  $[K(\alpha) : K] = n$ , we shall show that  $K(\alpha)$  is a vector space over  $K$  with basis  $\{1, \alpha, \dots, \alpha^{n-1}\}$ .
- The inclusion  $K[\alpha] \subseteq K(\alpha)$  is trivial. To see the converse, pick an element  $P(\alpha)/Q(\alpha) \in K(\alpha)$ . We must have  $\gcd(Q, \min_{\alpha, K}) = 1$  in the Euclidean ring  $K[x]$ . Then we use the existence of  $f, g \in K[x]$  such that  $f \cdot Q + g \cdot \min_{\alpha, K} = 1$ .



- If  $K/\mathbf{Q}$  is a finite extension then  $K$  is called a number field.
- A number field is an algebraic extension of  $\mathbf{Q}$ .
- We have something stronger.

## Theorem (Primitive element theorem)

*If  $K$  is a number field, then  $K = \mathbf{Q}(\alpha)$  for some complex number  $\alpha$ .*

- Not all algebraic extensions are simple! (It may not be possible to generate them with a single element.)
- For example;
  - any infinite algebraic extension is not simple,
  - there exists a finite inseparable extension that is not simple.

- Another important family of algebraic field extensions is given by finite fields.
- The field  $\mathbf{F}_p$ : Let  $p$  be a prime element in  $\mathbf{Z}$ . Then  $\mathfrak{p} = \langle p \rangle$  is a prime ideal of  $\mathbf{Z}$ . The quotient ring  $\mathbf{Z}/\mathfrak{p}$  is a finite integral domain. Thus it is a field with  $p$  elements.

## Theorem

*For each  $q$ , a power of a prime  $p \in \mathbf{Z}$ , there exist a unique field  $\mathbf{F}_q$  with precisely  $q$  elements up to isomorphism.*

- The construction of such a field with  $q = p^d$  can be achieved by the quotient ring  $\mathbf{F}_p[x]/\langle f(x) \rangle$  where  $f(x) \in \mathbf{F}_p[x]$  is an irreducible polynomial of degree  $d$ .
- Non-zero elements of  $\mathbf{F}_q$  form a cyclic group of order  $q - 1$  under the multiplication.

# Modules and Free Abelian Groups



- Let  $R$  be a ring. An  $R$ -module consists of an abelian group  $M$  and an operation  $\cdot : R \times M \rightarrow M$  such that for all  $r, s \in R$  and  $x, y \in M$ :
  - ①  $r \cdot (x + y) = r \cdot x + r \cdot y$ ,
  - ②  $(r + s) \cdot x = r \cdot x + s \cdot x$ ,
  - ③  $(rs) \cdot x = r \cdot (s \cdot x)$ ,
  - ④  $1_R \cdot x = x$ .
- If  $R$  is a field, then an  $R$ -module is the same thing as a vector space over the field  $R$ . Thus an  $R$ -module can be considered as a generalization of a vector space.
- Because of the lack of division in  $R$ , many properties of vector spaces may not hold for  $R$ -modules.
- For example, an  $R$ -module may not have a basis.

# Submodules and homomorphisms

- Suppose  $M$  is an  $R$ -module and  $N$  is a subgroup of  $M$ . Then  $N$  is an  $R$ -submodule if,

$$r \in R \text{ and } n \in N \implies r \cdot n \in N.$$

- If  $M$  and  $N$  are  $R$ -modules, then a map  $f : M \rightarrow N$  is an  $R$ -module homomorphism if, for any  $m, n \in M$  and  $r, s \in R$ ,

$$f(r \cdot m + s \cdot n) = r \cdot f(m) + s \cdot f(n).$$

- A bijective module homomorphism is an isomorphism of modules, and the two modules are called isomorphic.
- The isomorphism theorems familiar from vector spaces are also valid for  $R$ -modules.

- **Finitely generated:** An  $R$ -module  $M$  is finitely generated if there exist finitely many elements  $x_1, \dots, x_n \in M$  such that every element of  $M$  is a linear combination of those elements with coefficients from the ring  $R$ .
- **Free:** A free  $R$ -module is a module that has a basis, or equivalently, one that is isomorphic to a direct sum of copies of the ring  $R$ . These are the modules that behave very much like vector spaces.
- **Torsion-Free:** A torsion-free module is a module over a ring such that  $0$  is the only element annihilated by a regular element (non zero-divisor) of the ring.

- Any abelian group  $M$  can be made into a  $\mathbf{Z}$ -module by defining

$$n \cdot m = \underbrace{m + m + \dots + m}_{n \text{ times}}$$

for any  $n \in \mathbf{Z}$  and  $m \in M$ .

## Example

As a  $\mathbf{Z}$ -module,  $\mathbf{Q}$  is

- not finitely generated,
- not free,
- torsion-free,

# Elliptic curves as modules

- Given an abelian group  $A$ , let  $\text{End}(A)$  be the set of endomorphisms  $f : A \rightarrow A$  (i.e. surjective group homomorphisms).
- It is easy to verify that  $(\text{End}(E), +, \circ)$  is a ring with identity (possibly noncommutative). Here the multiplication is given by the composition of functions.
- The abelian group  $A$  is naturally an  $\text{End}(A)$ -module with  $f \cdot a$  defined to be  $f(a)$ .

## Example

Any elliptic curve  $E$  has an abelian group structure. Thus any elliptic curve  $E$  is naturally an  $\text{End}(E)$ -module.

# Free abelian groups

- If  $G$  is finitely generated as a  $\mathbf{Z}$ -module, so that there exist  $g_1, \dots, g_n \in G$  such that every  $g \in G$  is a sum

$$g = m_1g_1 + \dots + m_n g_n \quad (m_i \in \mathbf{Z})$$

then  $G$  is called a finitely generated abelian group.

- Generalizing the notion of linear independence in a vector space, we say that elements  $g_1, \dots, g_n$  in an abelian group  $G$  are linearly independent (over  $\mathbf{Z}$ ) if any equation

$$m_1g_1 + \dots + m_n g_n = 0 \quad (m_i \in \mathbf{Z})$$

implies  $m_1 = m_2 = \dots = m_n = 0$ .

- A linearly independent set which generates  $G$  is called a basis.
- If  $\{g_1, \dots, g_n\}$  is a basis, then every  $g \in G$  has a unique representation  $g = \sum_{i=1}^n m_i g_i$ .

# Change of basis

- An abelian group with a basis of  $n$  elements is called a free abelian group of rank  $n$ .

## Theorem

Let  $G$  be a free abelian group of rank  $n$  with basis  $\{x_1, \dots, x_n\}$ . Suppose that  $[a_{ij}]$  is an  $n \times n$  matrix with integer entries. Then the elements

$$y_i = \sum_{j=1}^n a_{ij}x_j \quad (i = 1, \dots, n)$$

form a basis of  $G$  if and only if  $\det([a_{ij}]) = \pm 1$ .

- For example, a standard basis for  $\mathbf{Z}^2$  is  $e_1 = (1, 0)$  and  $e_2 = (0, 1)$ . If we consider  $y_1 = 3e_1 + 2e_2$  and  $y_2 = 2e_1 + e_2$ , then  $\{y_1, y_2\}$  is a  $\mathbf{Z}$ -basis for  $\mathbf{Z}^2$  because  $\det\left(\begin{bmatrix} 3 & 2 \\ 2 & 1 \end{bmatrix}\right) = -1$ . Note that  $\begin{bmatrix} 3 & 2 \\ 2 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} -1 & 2 \\ 2 & -3 \end{bmatrix}$

- We will need the following facts in order analyze the ring of integers

## Theorem

*Every subgroup of a free abelian group of rank  $n$  is also a free group of rank less than or equal to  $n$ .*

## Theorem

*Let  $G$  be a free abelian group of rank  $n$ , and  $H$  a subgroup of  $G$ . Then  $G/H$  is finite if and only if the ranks of  $G$  and  $H$  are equal. If this is the case and if  $G$  and  $H$  have  $\mathbf{Z}$ -bases  $\{x_1, \dots, x_n\}$  and  $\{y_1, \dots, y_n\}$ , respectively, with  $y_i = \sum_{j=1}^n a_{ij}x_j$ , then*

$$|G/H| = |\det([a_{ij}])|.$$



# The End