Part IB — Groups, Rings and Modules

Definitions

Based on lectures by O. Randal-Williams
Notes taken by Dexter Chua
Lent 2016

These notes are not endorsed by the lecturers, and I have modified them (often significantly) after lectures. They are nowhere near accurate representations of what was actually lectured, and in particular, all errors are almost surely mine.

Groups

Sylow subgroups and Sylow theorems. Applications, groups of small order. [8]

Rings
Definition and examples of rings (commutative, with 1). Ideals, homomorphisms, quotient rings, isomorphism theorems. Prime and maximal ideals. Fields. The characteristic of a field. Field of fractions of an integral domain.

Factorization in rings; units, primes and irreducibles. Unique factorization in principal ideal domains, and in polynomial rings. Gauss’ Lemma and Eisenstein’s irreducibility criterion.

Rings $\mathbb{Z}[\alpha]$ of algebraic integers as subsets of $\mathbb{C}$ and quotients of $\mathbb{Z}[x]$. Examples of Euclidean domains and uniqueness and non-uniqueness of factorization. Factorization in the ring of Gaussian integers; representation of integers as sums of two squares.

Ideals in polynomial rings. Hilbert basis theorem. [10]

Modules
## Contents

0 Introduction .......................... 3

1 Groups .................................. 4
   1.1 Basic concepts .......................... 4
   1.2 Normal subgroups, quotients, homomorphisms, isomorphisms ... 4
   1.3 Actions of permutations .................. 5
   1.4 Conjugacy, centralizers and normalizers .................. 6
   1.5 Finite p-groups .......................... 6
   1.6 Finite abelian groups ..................... 6
   1.7 Sylow theorems ........................... 6

2 Rings ................................... 7
   2.1 Definitions and examples .................. 7
   2.2 Homomorphisms, ideals, quotients and isomorphisms .............. 8
   2.3 Integral domains, field of factions, maximal and prime ideals ... 9
   2.4 Factorization in integral domains ................ 10
   2.5 Factorization in polynomial rings ................ 11
   2.6 Gaussian integers ........................ 11
   2.7 Algebraic integers ........................ 11
   2.8 Noetherian rings .......................... 11

3 Modules ................................. 12
   3.1 Definitions and examples .................. 12
   3.2 Direct sums and free modules ................ 13
   3.3 Matrices over Euclidean domains .............. 13
   3.4 Modules over \(\mathbb{F}[X]\) and normal forms for matrices .......... 14
   3.5 Conjugacy of matrices* ..................... 14
0 Introduction
1 Groups

1.1 Basic concepts

**Definition** (Group). A group is a triple \((G, \cdot, e)\), where \(G\) is a set, \(\cdot : G \times G \to G\) is a function and \(e \in G\) is an element such that

(i) For all \(a, b, c \in G\), we have \((a \cdot b) \cdot c = a \cdot (b \cdot c)\). (associativity)

(ii) For all \(a \in G\), we have \(a \cdot e = e \cdot a = a\). (identity)

(iii) For all \(a \in G\), there exists \(a^{-1} \in G\) such that \(a \cdot a^{-1} = a^{-1} \cdot a = e\). (inverse)

**Definition** (Subgroup). If \((G, \cdot, e)\) is a group and \(H \subseteq G\) is a subset, it is a subgroup if

(i) \(e \in H\),

(ii) \(a, b \in H\) implies \(a \cdot b \in H\),

(iii) \(\cdot : H \times H \to H\) makes \((H, \cdot, e)\) a group.

We write \(H \leq G\) if \(H\) is a subgroup of \(G\).

**Definition** (Abelian group). A group \(G\) is abelian if \(a \cdot b = b \cdot a\) for all \(a, b \in G\).

**Definition** (Coset). If \(H \leq G\) and \(g \in G\), the left coset \(gH\) is the set
\[
gH = \{x \in G : x = g \cdot h \text{ for some } h \in H\}.
\]

**Definition** (Order of group). The order of a group is the number of elements in \(G\), written \(|G|\).

**Definition** (Order of element). The order of an element \(g \in G\) is the smallest positive \(n\) such that \(g^n = e\). If there is no such \(n\), we say \(g\) has infinite order. We write \(\text{ord}(g) = n\).

1.2 Normal subgroups, quotients, homomorphisms, isomorphisms

**Definition** (Normal subgroup). A subgroup \(H \leq G\) is normal if for any \(h \in H\) and \(g \in G\), we have \(g^{-1}hg \in H\). We write \(H \triangleleft G\).

**Definition** (Quotient group). If \(H \triangleleft G\) is a normal subgroup, then the set \(G/H\) of left \(H\)-cosets forms a group with multiplication
\[
(g_1H) \cdot (g_2H) = g_1g_2H.
\]
with identity \(eH = H\). This is known as the quotient group.

**Definition** (Homomorphism). If \((G, \cdot, e_G)\) and \((H, \ast, e_H)\) are groups, a function \(\phi : G \to H\) is a homomorphism if \(\phi(e_G) = e_H\), and for \(g, g' \in G\), we have
\[
\phi(g \cdot g') = \phi(g) \ast \phi(g').
\]
Definition (Kernel). The kernel of a homomorphism \( \phi : G \to H \) is
\[
\ker(\phi) = \{ g \in G : \phi(g) = e \}.
\]

Definition (Image). The image of a homomorphism \( \phi : G \to H \) is
\[
\text{im}(\phi) = \{ h \in H : h = \phi(g) \text{ for some } g \in G \}.
\]

Definition (Isomorphism). An isomorphism is a homomorphism that is also a bijection.

Definition (Isomorphic group). Two groups \( G \) and \( H \) are isomorphic if there is an isomorphism between them. We write \( G \cong H \).

Definition (Simple group). A (non-trivial) group \( G \) is simple if it has no normal subgroups except \( \{e\} \) and \( G \).

1.3 Actions of permutations

Definition (Symmetric group). The symmetric group \( S_n \) is the group of all permutations of \( \{1, \cdots, n\} \), i.e. the set of all bijections of this set with itself.

Definition (Even and odd permutation). A permutation \( \sigma \in S_n \) is even if it can be written as a product of evenly many transpositions; odd otherwise.

Definition (Alternating group). The alternating group \( A_n \leq S_n \) is the subgroup of even permutations, i.e. \( A_n \) is the kernel of sgn.

Definition (Symmetric group of \( X \)). Let \( X \) be a set. We write \( \text{Sym}(X) \) for the group of all permutations of \( X \).

Definition (Permutation group). A group \( G \) is called a permutation group if it is a subgroup of \( \text{Sym}(X) \) for some \( X \), i.e. it is given by some, but not necessarily all, permutations of some set.

We say \( G \) is a permutation group of order \( n \) if in addition \( |X| = n \).

Definition (Group action). An action of a group \((G, \cdot)\) on a set \( X \) is a function
\[
* : G \times X \to X
\]
such that
(i) \( g_1 \cdot (g_2 \cdot x) = (g_1 \cdot g_2) \cdot x \) for all \( g_1, g_2 \in G \) and \( x \in X \).
(ii) \( e \cdot x = x \) for all \( x \in X \).

Definition (Permutation representation). A permutation representation of a group \( G \) is a homomorphism \( G \to \text{Sym}(X) \).

Notation. For an action of \( G \) on \( X \) given by \( \phi : G \to \text{Sym}(X) \), we write \( G^X = \text{im}(\phi) \) and \( G_X = \ker(\phi) \).

Definition (Orbit). If \( G \) acts on a set \( X \), the orbit of \( x \in X \) is
\[
G \cdot x = \{ g \cdot x \in X : g \in G \}.
\]

Definition (Stabilizer). If \( G \) acts on a set \( X \), the stabilizer of \( x \in X \) is
\[
G_x = \{ g \in G : g \cdot x = x \}.
\]
1.4 Conjugacy, centralizers and normalizers

**Definition** (Automorphism group). The automorphism group of $G$ is

$$\text{Aut}(G) = \{ f : G \rightarrow G : f \text{ is a group isomorphism} \}.$$  

This is a group under composition, with the identity map as the identity.

**Definition** (Conjugacy class). The conjugacy class of $g \in G$ is

$$ccl_G(g) = \{ hgh^{-1} : h \in G \},$$

i.e. the orbit of $g \in G$ under the conjugation action.

**Definition** (Centralizer). The centralizer of $g \in G$ is

$$C_G(g) = \{ h \in G : hgh^{-1} = g \},$$

i.e. the stabilizer of $g$ under the conjugation action. This is alternatively the set of all $h \in G$ that commute with $g$.

**Definition** (Center). The center of a group $G$ is

$$Z(G) = \{ h \in G : hgh^{-1} = g \text{ for all } g \in G \} = \bigcap_{g \in G} C_G(g) = \ker(\phi).$$

**Definition** (Normalizer). Let $H \leq G$. The normalizer of $H$ in $G$ is

$$N_G(H) = \{ g \in G : g^{-1}Hg = H \}.$$  

1.5 Finite $p$-groups

**Definition** ($p$-group). A finite group $G$ is a $p$-group if $|G| = p^n$ for some prime number $p$ and $n \geq 1$.

1.6 Finite abelian groups

1.7 Sylow theorems
2 Rings

2.1 Definitions and examples

Definition (Ring). A ring is a quintuple \((R, +, \cdot, 0_R, 1_R)\) where \(0_R, 1_R \in R\), and \(+, \cdot : R \times R \to R\) are binary operations such that

(i) \((R, +, 0_R)\) is an abelian group.

(ii) The operation \(\cdot : R \times R \to R\) satisfies associativity, i.e.

\[ a \cdot (b \cdot c) = (a \cdot b) \cdot c, \]

and identity:

\[ 1_R \cdot r = r \cdot 1_R = r. \]

(iii) Multiplication distributes over addition, i.e.

\[ r_1 \cdot (r_2 + r_3) = (r_1 \cdot r_2) + (r_1 \cdot r_3) \]
\[ (r_1 + r_2) \cdot r_3 = (r_1 \cdot r_3) + (r_2 \cdot r_3). \]

Notation. If \(R\) is a ring and \(r \in R\), we write \(−r\) for the inverse to \(r\) in \((R, +, 0_R)\).

This satisfies \(r + (−r) = 0_R\). We write \(r − s\) to mean \(r + (−s)\) etc.

Definition (Commutative ring). We say a ring \(R\) is commutative if \(a \cdot b = b \cdot a\) for all \(a, b \in R\).

Definition (Subring). Let \((R, +, \cdot, 0_R, 1_R)\) be a ring, and \(S \subseteq R\) be a subset. We say \(S\) is a subring of \(R\) if \(0_R, 1_R \in S\), and the operations \(+, \cdot\) make \(S\) into a ring in its own right. In this case we write \(S \leq R\).

Definition (Unit). An element \(u \in R\) is a unit if there is another element \(v \in R\) such that \(u \cdot v = 1_R\).

Definition (Field). A field is a non-zero ring where every \(u \neq 0_R \in R\) is a unit.

Definition (Product of rings). Let \(R, S\) be rings. Then the product \(R \times S\) is a ring via

\[ (r, s) + (r', s') = (r + r', s + s'), \quad (r, s) \cdot (r', s') = (r \cdot r', s \cdot s'). \]

The zero is \((0_R, 0_S)\) and the one is \((1_R, 1_S)\).

We can (but won’t) check that these indeed are rings.

Definition (Polynomial). Let \(R\) be a ring. Then a polynomial with coefficients in \(R\) is an expression

\[ f = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n, \]

with \(a_i \in R\). The symbols \(X^i\) are formal symbols.

Definition (Degree of polynomial). The degree of a polynomial \(f\) is the largest \(m\) such that \(a_m \neq 0\).

Definition (Monic polynomial). Let \(f\) have degree \(m\). If \(a_m = 1\), then \(f\) is called monic.
**Definition** (Polynomial ring). We write $R[X]$ for the set of all polynomials with coefficients in $R$. The operations are performed in the obvious way, i.e. if $f = a_0 + a_1 X + \cdots + a_n X^n$ and $g = b_0 + b_1 X + \cdots + b_k X^k$ are polynomials, then
\[
    f + g = \sum_{i=0}^{\max\{n,k\}} (a_i + b_i) X^i,
\]
and
\[
    f \cdot g = \sum_{i=0}^{n+k} \left( \sum_{j=0}^{i} a_j b_{i-j} \right) X^i,
\]
We identify $R$ with the constant polynomials, i.e. polynomials $\sum a_i X^i$ with $a_i = 0$ for $i > 0$. In particular, $0_R \in R$ and $1_R \in R$ are the zero and one of $R[X]$.

**Definition** (Power series). We write $R[[X]]$ for the ring of power series on $R$, i.e.
\[
    f = a_0 + a_1 X + a_2 X^2 + \cdots ,
\]
where each $a_i \in R$. This has addition and multiplication the same as for polynomials, but without upper limits.

**Definition** (Laurent polynomials). The Laurent polynomials on $R$ is the set $R[X, X^{-1}]$, i.e. each element is of the form
\[
    f = \sum_{i \in \mathbb{Z}} a_i X^i
\]
where $a_i \in R$ and only finitely many $a_i$ are non-zero. The operations are the obvious ones.

### 2.2 Homomorphisms, ideals, quotients and isomorphisms

**Definition** (Homomorphism of rings). Let $R, S$ be rings. A function $\phi : R \to S$ is a ring homomorphism if it preserves everything we can think of, i.e.

(i) $\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2)$,
(ii) $\phi(0_R) = 0_S$,
(iii) $\phi(r_1 \cdot r_2) = \phi(r_1) \cdot \phi(r_2)$,
(iv) $\phi(1_R) = 1_S$.

**Definition** (Isomorphism of rings). If a homomorphism $\phi : R \to S$ is a bijection, we call it an isomorphism.

**Definition** (Kernel). The kernel of a homomorphism $\phi : R \to S$ is
\[
    \ker(\phi) = \{ r \in R : \phi(r) = 0_S \}.
\]

**Definition** (Image). The image of $\phi : R \to S$ is
\[
    \text{im}(\phi) = \{ s \in S : s = \phi(r) \text{ for some } r \in R \}.
\]
Definition (Ideal). A subset $I \subseteq R$ is an ideal, written $I \triangleleft R$, if

(i) It is an additive subgroup of $(R, +, 0_R)$, i.e. it is closed under addition and
additive inverses. (additive closure)

(ii) If $a \in I$ and $b \in R$, then $a \cdot b \in I$. (strong closure)

We say $I$ is a proper ideal if $I \neq R$.

Definition (Generator of ideal). For an element $a \in R$, we write

$$(a) = aR = \{a \cdot r : r \in R\} \triangleleft R.$$ 

This is the ideal generated by $a$.

In general, let $a_1, a_2, \cdots, a_k \in R$, we write

$$(a_1, a_2, \cdots, a_k) = \{a_1r_1 + \cdots + a_kr_k : r_1, \cdots, r_k \in R\}.$$ 

This is the ideal generated by $a_1, \cdots, a_k$.

Definition (Generator of ideal). For $A \subseteq R$ a subset, the ideal generated by $A$ is

$$(A) = \left\{ \sum_{a \in A} r_a \cdot a : r_a \in R, \text{ only finitely-many non-zero} \right\}.$$ 

Definition (Principal ideal). An ideal $I$ is a principal ideal if $I = (a)$ for some $a \in R$.

Definition (Quotient ring). Let $I \triangleleft R$. The quotient ring $R/I$ consists of the (additive) cosets $r + I$ with the zero and one as $0_R + I$ and $1_R + I$, and operations

$$(r_1 + I) + (r_2 + I) = (r_1 + r_2) + I$$

$$(r_1 + I) \cdot (r_2 + I) = r_1r_2 + I.$$ 

Definition (Characteristic of ring). Let $R$ be a ring, and $\iota : \mathbb{Z} \to R$ be the unique such map. The characteristic of $R$ is the unique non-negative $n$ such that $\ker(\iota) = n\mathbb{Z}$.

2.3 Integral domains, field of fractions, maximal and prime ideals

Definition (Integral domain). A non-zero ring $R$ is an integral domain if for all $a, b \in R$, if $a \cdot b = 0_R$, then $a = 0_R$ or $b = 0_R$.

Definition (Zero divisor). An element $x \in R$ is a zero divisor if $x \neq 0$ and there is a $y \neq 0$ such that $x \cdot y = 0 \in R$.

Notation. Write $R[X, Y]$ for $(R[X])[Y]$, the polynomial ring of $R$ in two variables. In general, write $R[X_1, \cdots, X_n] = (\cdots (R[X_1])[X_2]\cdots)[X_n]$.

Definition (Field of fractions). Let $R$ be an integral domain. A field of fractions $F$ of $R$ is a field with the following properties

(i) $R \subseteq F$
(ii) Every element of $F$ may be written as $a \cdot b^{-1}$ for $a, b \in R$, where $b^{-1}$ means the multiplicative inverse to $b \neq 0$ in $F$.

**Definition (Maximal ideal).** An ideal $I$ of a ring $R$ is maximal if $I \neq R$ and for any ideal $J$ with $I \leq J \leq R$, either $J = I$ or $J = R$.

**Definition (Prime ideal).** An ideal $I$ of a ring $R$ is prime if $I \neq R$ and whenever $a, b \in R$ are such that $a \cdot b \in I$, then $a \in I$ or $b \in I$.

### 2.4 Factorization in integral domains

**Definition (Unit).** An element $a \in R$ is a unit if there is a $b \in R$ such that $ab = 1_R$. Equivalently, if the ideal $(a) = R$.

**Definition (Division).** For elements $a, b \in R$, we say $a$ divides $b$, written $a \mid b$, if there is a $c \in R$ such that $b = ac$. Equivalently, if $(b) \subseteq (a)$.

**Definition (Associates).** We say $a, b \in R$ are associates if $a = bc$ for some unit $c$. Equivalently, if $(a) = (b)$. Equivalently, if $a \mid b$ and $b \mid a$.

**Definition (Irreducible).** We say $a \in R$ is irreducible if $a \neq 0$, $a$ is not a unit, and if $a = xy$, then $x$ or $y$ is a unit.

**Definition (Prime).** We say $a \in R$ is prime if $a$ is non-zero, not a unit, and whenever $a \mid xy$, either $a \mid x$ or $a \mid y$.

**Definition (Euclidean domain).** An integral domain $R$ is a Euclidean domain (ED) if there is a Euclidean function $\phi : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ such that

(i) $\phi(a \cdot b) \geq \phi(b)$ for all $a, b \neq 0$

(ii) If $a, b \in R$, with $b \neq 0$, then there are $q, r \in R$ such that

$$a = b \cdot q + r,$$

and either $r = 0$ or $\phi(r) < \phi(b)$.

**Definition (Principal ideal domain).** A ring $R$ is a principal ideal domain (PID) if it is an integral domain, and every ideal is a principal ideal, i.e. for all $I \triangleleft R$, there is some $a$ such that $I = (a)$.

**Definition (Unique factorization domain).** An integral domain $R$ is a unique factorization domain (UFD) if

(i) Every non-unit may be written as a product of irreducibles;

(ii) If $p_1 p_2 \cdots p_n = q_1 \cdots q_m$ with $p_i, q_j$ irreducibles, then $n = m$, and they can be reordered such that $p_i$ is an associate of $q_i$.

**Definition (Ascending chain condition).** A ring satisfies the ascending chain condition (ACC) if there is no infinite strictly increasing chain of ideals.

**Definition (Noetherian ring).** A ring that satisfies the ascending chain condition is known as a Noetherian ring.

**Definition (Greatest common divisor).** $d$ is a greatest common divisor (gcd) of $a_1, a_2, \cdots, a_n$ if $d \mid a_i$ for all $i$, and if any other $d'$ satisfies $d' \mid a_i$ for all $i$, then $d' \mid d$. 

10
2.5 Factorization in polynomial rings

**Definition** (Content). Let $R$ be a UFD and $f = a_0 + a_1 X + \cdots + a_n X^n \in R[X]$. The content $c(f)$ of $f$ is

$$c(f) = \gcd(a_0, a_1, \ldots, a_n) \in R.$$

**Definition** (Primitive polynomial). A polynomial is primitive if $c(f)$ is a unit, i.e. the $a_i$ are coprime.

2.6 Gaussian integers

**Definition** (Gaussian integers). The Gaussian integers is the subring $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$.

2.7 Algebraic integers

**Definition** (Algebraic integer). An $\alpha \in \mathbb{C}$ is called an algebraic integer if it is a root of a monic polynomial in $\mathbb{Z}[X]$, i.e. there is a monic $f \in \mathbb{Z}[X]$ such that $f(\alpha) = 0$.

**Notation.** For $\alpha$ an algebraic integer, we write $\mathbb{Z}[\alpha] \subseteq \mathbb{C}$ for the smallest subring containing $\alpha$.

**Definition** (Minimal polynomial). Let $\alpha \in \mathbb{C}$ be an algebraic integer. Then the minimal polynomial is a polynomial $f_\alpha$ is the irreducible monic such that $I = \ker(\phi) = (f_\alpha)$.

2.8 Noetherian rings

**Definition** (Noetherian ring). A ring is Noetherian if for any chain of ideals

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots,$$

there is some $N$ such that $I_N = I_{N+1} = I_{N+2} = \cdots$. This condition is known as the ascending chain condition.

**Definition** (Finitely generated ideal). An ideal $I$ is finitely generated if it can be written as $I = (r_1, \cdots, r_n)$ for some $r_1, \cdots, r_n \in R$. 

3 Modules

3.1 Definitions and examples

Definition (Module). Let $R$ be a commutative ring. We say a quadruple $(M, +, 0_M, \cdot)$ is an $R$-module if

(i) $(M, +, 0_M)$ is an abelian group

(ii) The operation $\cdot : R \times M \to M$ satisfies

(a) $(r_1 + r_2) \cdot m = (r_1 \cdot m) + (r_2 \cdot m);
(b) r \cdot (m_1 + m_2) = (r \cdot m_1) + (r \cdot m_2);
(c) r_1 \cdot (r_2 \cdot m) = (r_1 \cdot r_2) \cdot m; and
(d) 1_R \cdot m = m.$

Definition (Submodule). Let $M$ be an $R$-module. A subset $N \subseteq M$ is an $R$-submodule if it is a subgroup of $(M, +, 0_M)$, and if $n \in N$ and $r \in R$, then $rn \in N$. We write $N \leq M$.

Definition (Quotient module). Let $N \leq M$ be an $R$-submodule. The quotient module $M/N$ is the set of $N$-cosets in $(M, +, 0_M)$, with the $R$-action given by

$r \cdot (m + N) = (r \cdot m) + N.$

Definition (R-module homomorphism and isomorphism). A function $f : M \to N$ between $R$-modules is an $R$-module homomorphism if it is a homomorphism of abelian groups, and satisfies

$f(r \cdot m) = r \cdot f(m)$

for all $r \in R$ and $m \in M$.

An isomorphism is a bijective homomorphism, and two $R$-modules are isomorphic if there is an isomorphism between them.

Definition (Annihilator). Let $M$ be an $R$-module, and $m \in M$. The annihilator of $m$ is

$\text{Ann}(m) = \{r \in R : r \cdot m = 0\}.$

For any set $S \subseteq M$, we define

$\text{Ann}(S) = \{r \in R : r \cdot m = 0 \text{ for all } m \in S\} = \bigcap_{m \in S} \text{Ann}(m).$

In particular, for the module $M$ itself, we have

$\text{Ann}(M) = \{r \in R : r \cdot m = 0 \text{ for all } m \in M\} = \bigcap_{m \in M} \text{Ann}(m).$

Definition (Submodule generated by element). Let $M$ be an $R$-module, and $m \in M$. The submodule generated by $m$ is

$Rm = \{r \cdot m \in M : r \in R\}.$

Definition (Finitely generated module). An $R$-module $M$ is finitely generated if there is a finite list of elements $m_1, \ldots, m_k$ such that

$M = Rm_1 + Rm_2 + \cdots + Rm_k = \{r_1m_1 + r_2m_2 + \cdots + r_km_k : r_i \in R\}.$
3.2 Direct sums and free modules

**Definition** (Direct sum of modules). Let $M_1, M_2, \cdots, M_k$ be $R$-modules. The **direct sum** is the $R$-module

$$M_1 \oplus M_2 \oplus \cdots \oplus M_k,$$

which is the set $M_1 \times M_2 \times \cdots \times M_k$, with addition given by

$$(m_1, \cdots, m_k) + (m_1', \cdots, m_k') = (m_1 + m_1', \cdots, m_k + m_k'),$$

and the $R$-action given by

$$r \cdot (m_1, \cdots, m_k) = (rm_1, \cdots, rm_k).$$

**Definition** (Linear independence). Let $m_1, \cdots, m_k \in M$. Then \{m_1, \cdots, m_k\} is **linearly independent** if

$$\sum_{i=1}^{k} r_im_i = 0$$

implies $r_1 = r_2 = \cdots = r_k = 0$.

**Definition** (Freely generate). A subset $S \subseteq M$ generates $M$ **freely** if

(i) $S$ generates $M$

(ii) Any set function $\psi : S \rightarrow N$ to an $R$-module $N$ extends to an $R$-module map $\theta : M \rightarrow N$.

**Definition** (Free module and basis). An $R$-module is **free** if it is freely generated by some subset $S \subseteq M$, and $S$ is called a **basis**.

**Definition** (Relations). If $M$ is a finitely-generated $R$-module, we have shown that there is a surjective $R$-module $\phi : R^k \rightarrow M$. We call $\ker(\phi)$ the **relation module** for those generators.

**Definition** (Finitely presented module). A finitely-generated module is **finitely presented** if we have a surjective homomorphism $\phi : R^k \rightarrow M$ and $\ker \phi$ is finitely generated.

3.3 Matrices over Euclidean domains

**Definition** (Elementary row operations). **Elementary row operations** on an $m \times n$ matrix $A$ with entries in $R$ are operations of the form

(i) Add $c \in R$ times the $i$th row to the $j$th row. This may be done by multiplying by the following matrix on the left: $$\begin{pmatrix} 1 \\ \vdots \\ 1 \\ c \\ \vdots \\ 1 \\ \vdots \\ 1 \end{pmatrix},$$

where $c$ appears in the $i$th column of the $j$th row.
(ii) Swap the $i$th and $j$th rows. This can be done by left-multiplication of the matrix

\[
\begin{pmatrix}
1 & & & & \\
& \ddots & & & \\
& & 1 & 0 & 1 \\
& & 1 & \ddots & 1 \\
& & 1 & 0 & \ddots \\
& & & & 1 \\
\end{pmatrix}
\]

Again, the rows and columns we have messed with are the $i$th and $j$th rows and columns.

(iii) We multiply the $i$th row by a unit $c \in R$. We do this via the following matrix:

\[
\begin{pmatrix}
1 & & & & \\
& \ddots & & & \\
& & 1 & c & 1 \\
& & 1 & \ddots & 1 \\
& & & & 1 \\
\end{pmatrix}
\]

Notice that if $R$ is a field, then we can multiply any row by any non-zero number, since they are all units.

We also have elementary column operations defined in a similar fashion, corresponding to right multiplication of the matrices. Notice all these matrices are invertible.

**Definition** (Equivalent matrices). Two matrices are *equivalent* if we can get from one to the other via a sequence of such elementary row and column operations.

**Definition** (Invariant factors). The $d_k$ obtained in the Smith normal form are called the *invariant factors of $A$*.

**Definition** (Minor). A $k \times k$ minor of a matrix $A$ is the determinant of a $k \times k$ sub-matrix of $A$ (i.e. a matrix formed by removing all but $k$ rows and all but $k$ columns).

**Definition** (Fitting ideal). For a matrix $A$, the $k$th *Fitting ideal* $\text{Fit}_k(A) \triangleleft R$ is the ideal generated by the set of all $k \times k$ minors of $A$.

### 3.4 Modules over $\mathbb{F}[X]$ and normal forms for matrices

### 3.5 Conjugacy of matrices*