# 3201 Commutative Algebra Notes

Based on the 2013 autumn lectures by Dr J López Peña

MATH3201 – Commutative Algebra.

1 October 2013
Dr Javier LÓPEZ-PEÑA
Maths 500.

Administrative Details.

Office Hours: Thu 10am. Room 806. E-mail: j.lopezpena@ucl.ac.uk

Outline of course — Finitely generated modules over Principal Ideal Domains.

Goal: To prove the classification theorem for finitely generated modules over PID.

Weekly coursework.

chapter 1
INTRODUCTION TO RINGS.

1.1 Definitions and Examples.

Definition: A ring is a set $R$ with two operations $+$ (addition) and $\cdot$ (multiplication) satisfying the following properties:

(Sum)

S1: Commutativity $\quad a+b=b+a \quad \forall a,b \in R$

S2: Associativity $\quad (a+b)+c = a+(b+c) \quad \forall a,b,c \in R$

S3: Zero $\quad \exists\, 0 \in R$ s.t. $0+a=a=a+0 \quad \forall a \in R$.

S4: Inverses $\quad \forall a \in R \quad \exists\, -a \in R$ s.t. $a+(-a)=0$.

Remark – S1–S4 imply that $(R,+)$ is an abelian group.

(Multiplication)

P1: Associativity $\quad a(bc)=(ab)c \quad \forall a,b,c \in R$

P2: One $\quad \exists\, 1 \in R$ s.t. $1\cdot a = a = a\cdot 1 \quad \forall a \in R$

Remark – P1, P2 imply that $(R,\cdot)$ is a monoid.

P3: Distributivity $\quad (a+b)c = ac+bc, \quad a(b+c) = ab+ac.$

Note – Condition S3 implies that $R$ must be non-empty. In general, except for the trivial group, $R=\{0\}$, zero differs from one.

Definition: If a ring $R$ satisfies the following property, then $R$ is a commutative ring:

P4: Commutativity $\quad ab=ba \quad \forall a,b \in R$.

Examples of rings –

1. $\mathbb{Q} = \{\frac{a}{b} \mid a,b \in \mathbb{Z},\ b \neq 0\}$ 2. $\mathbb{Z} = \{\dots,-2,-1,0,1,2,\dots\}$ 3. $\mathbb{R}, \mathbb{C}, \mathbb{F}$ field.

4. Polynomial rings. where $R$ is a ring, $R[x] = \{a_0 + a_1 x + \dots + a_n x^n \mid n \in \mathbb{N},\ a_i \in R\}$.

5. Polynomials in several variables: where $R$ is a ring, $x_1,\dots,x_n$ variables. $R[x_1,\dots,x_n]$ are polynomials in $x_1,\dots,x_n$.

6. Power series: where $R$ is a ring, $R[[x]] = \{\sum_{n\in\mathbb{N}} a_n x^n \mid a_n \in R\}$

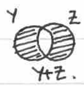
Return to the first example, and consider the ring of reduced fractions (rational numbers) $\mathbb{Q} = \{\frac{a}{b} \mid a,b \in \mathbb{Z},\ b\neq 0,\ \gcd(a,b)=1\}$.

Then we define, for $\frac{a}{b}, \frac{c}{d} \in R$, $\frac{a}{b}+\frac{c}{d} = \frac{ad+bc}{bd}$ and $\frac{a}{b}\cdot\frac{c}{d} = \frac{ac}{bd}$. This motivates a further example

7. $\mathbb{Z}_{(2)} = \{\frac{a}{b} \mid a,b \in \mathbb{Z},\ b \text{ odd},\ \gcd(a,b)=1\}$ is a ring. The same does not apply if $b$ is even, since $\nexists\, 1$ in this set.

8. $M_n(R)$ = $n\times n$ matrices with coefficients in $R$. [non-commutative!]

9. Power set ring. Take any non-empty set $X$. Define $R = P(X) = \{Y \text{ s.t. } Y \subseteq X\}$ with operations $Y+Z = (Y\cup Z)\setminus(Y\cap Z)$




and $YZ = Y\cap Z$. We claim that $P(X)$ is a commutative ring.

Here, the zero element is $\phi$ as $\left.\begin{matrix} Y\cup\phi = Y \\ Y\cap\phi=\phi \end{matrix}\right\} \Rightarrow (Y\cup\phi)\setminus(Y\cap\phi) = Y\setminus\phi = Y$.

The additive inverse of $Y$ is itself: $-Y=Y \quad \because \left.\begin{matrix} Y\cup Y = Y \\ Y\cap Y = Y\end{matrix}\right\} \Rightarrow Y\setminus Y = \phi$.

Also, under $\times$, $1 = X$.

This example demonstrates the generality of rings as structures over abstract domains.

10. Let $V$ be a vector space, $\mathrm{End}(V) = \{f: V\to V \mid f \text{ is a linear map}\}$ is a ring with operations $(f+g)(v) := f(v)+g(v)$, $(f\cdot g)(v) = f(g(v))$ (composition)

Then, $0 = 0_V$, $0(v)=0$ and $1 = \mathrm{Id}_V$, $\mathrm{Id}_V(v) = v \quad \forall v \in V$.

This is not commutative, since $\mathrm{End}(V)$ is simply a matrix ring (by choosing a basis), which is non-commutative (see example 8).

11. Rings of functions. $C(\mathbb{R}) = \{f: \mathbb{R}\to\mathbb{R} \mid f \text{ continuous}\}$ $\quad (f+g)(x) = f(x)+g(x), \quad (f\cdot g)(x) = f(x)\cdot g(x)$

This is a commutative ring. Here, multiplication is defined pointwise. If we take composition as the multiplication, is this still a ring? i.e. $(f\cdot g)(x) = f(g(x))$

- $(f\cdot(gh))(x) \overset{def}{=} f((gh)(x)) = f(g(h(x)))$, $((fg)\cdot h)(x) = (fg)(h(x)) = f(g(h(x))) \Rightarrow$ associativity holds.
- Let $f(x)=x^2$, $g(x)=x$, $h(x)=\sqrt{|x|}$. Then $f\cdot(g+h)(x) = f((g+h)(x)) = (x+\sqrt{|x|})^2 = x^2+x+2x\sqrt{x}$ but $(fg+fh)(x) = f(x)+f(\sqrt{x}) = x^2+x$

Distributivity does not hold $\Rightarrow$ not a ring.

12. Quaternions. $\mathbb{H} = \{a + bi + cj + dk \mid a,b,c,d \in \mathbb{R},\ ij = k = -ji,\ i^2 = j^2 = k^2 = -1\}$

This has an additional dimension than $\mathbb{C}$, but loses commutativity $\Rightarrow$ non-commutative ring.

13. Group rings. Let $R$ be a ring, $G$ be a group. $R[G] = \{\sum_{x\in G} a_x \cdot x \mid a_x \in R$, only finitely many $a_x \neq 0\}$

Commutativity depends on commutativity of group operation in $G$.

We can also define the group ring by functions. Then $R[G] = \{f : G \to R \mid f$ has a finite support$\}$ i.e. $f(x) = 0\ \forall x \in G$ except a finite number.

Then define $(f+g)(x) = f(x) + g(x)$, $(f\cdot g)(x) = (f*g)(x) = \sum_{y\in G} f(y)\, g(y^{-1}x)$, the convolution product.

1.2 Subrings and Ideals.

**Definition** Let $R$ be a ring. Then a subset $S \subseteq R$ is a subring if

1. $1 \in S$  2. $S$ is additively closed (i.e. $S$ is a subgroup of $(R,+)$). This implies that $\cdot\ 0 \in S$ $\cdot\ a,b \in S \Rightarrow a+b \in S$ and $\cdot\ a \in S \Rightarrow -a \in S$.

3. $\forall a,b \in S$, $ab \in S$.

Notation — $S \leq R$ means $S$ is a subring of $R$.

Examples of subrings —

1. $\{0\} \leq R$ for any $R$ is not a subring unless $R$ is itself
2. $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$.
3. $R \leq R[x]$ for any ring $R$.
4. $GL_n(\mathbb{R})$ is not a subring of $M_n(\mathbb{R})$ $\because$ $0 \notin GL_n(\mathbb{R})$. However, we can see that for diagonal or triangular matrices, $D_n(\mathbb{R})$, $\underset{\text{upper}}{U_n(\mathbb{R})}$, $\underset{\text{lower triangular}}{L_n(\mathbb{R})}$ $\leq M_n(\mathbb{R})$.

   $M_2(\mathbb{R})$ is not a subring of $M_3(\mathbb{R})$ because $I_3 \notin M_3(\mathbb{R})$. However, $\left\{\begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & e\end{pmatrix} \middle| a,b,c,d,e \in \mathbb{R}\right\} \leq M_3(\mathbb{R})$.
5. Let $R$ be a ring and $S_1, S_2 \leq R$. Then $S_1 \cap S_2 \leq R$ is a subring.

   More generally, in the infinite case, if $\{S_i\}$ is any non-empty family of subrings of $R$, then $\bigcap S_i \leq R$ is a subring.

   This enables us to talk about "the subring of $R$ generated by a set $X$ of elements", $\bigcap\{S \mid S \leq R$ subring, $X \subseteq S\} \leq R$.

   This is the smallest possible subring of $R$ containing $X$.

**Definition** Let $R$ be a commutative ring, then a subset $I \subseteq R$ is an ideal if it satisfies:

1. Additive closure, i.e. $\cdot\ 0 \in I$, $\cdot\ a,b \in I \Rightarrow a+b \in I$, $\cdot\ a \in I \Rightarrow -a \in I$.
2. Absorbency. $\forall r \in R, \forall a \in I$, $r\cdot a \in I$

} Notation — We write $I \trianglelefteq R$.

Examples of ideals —

1. $\{0\}$ is an ideal of any $R$. This is the zero ideal. Also, $R$ is an ideal of $R$. This is the total ideal.

If $I \trianglelefteq R$ and $I \neq R$, then $I$ is a proper ideal.

3 October 2013
Dr. Javier LÓPEZ-PEÑA
Maths 500.

3. Let $R = \mathbb{Z}$, $(2) = \{2n \mid n \in \mathbb{Z}\}$. Then $(2) \trianglelefteq \mathbb{Z}$ is an ideal. More generally, if $a \in R$, $(a) = \{ra \mid r \in R\} \trianglelefteq R$ is ideal.

   This is called the principal ideal generated by $a$.
4. Let $R$ be a ring, $I, J \trianglelefteq R$ are ideals. Then $I \cap J \trianglelefteq R$ and $I + J = \{i + j \mid i \in I, j \in J\} \trianglelefteq R$.

   $I \cap J$ is the largest ideal contained in $I$ and $J$, while $I+J$ is the smallest ideal containing $I$ and $J$.
5. If $R$ is a ring, $a_1, \dots, a_n \in R$, we define $(a_1, a_2, \dots, a_n) := (a_1) + (a_2) + \dots + (a_n)$. This is called the ideal generated by $a_1, \dots, a_n$

Ideals and quotient rings.

Let $R$ be a (commutative) ring, $I \trianglelefteq R$ ideal. For any $a \in R$ define $a + I := \{a + i \mid i \in I\}$ to be the coset of $a$ modulo $I$. To simplify notation, we denote it as $\bar{a}$.

Question: When are two cosets $a+I$ and $b+I$ the same set?

Since $0 \in I$, $a \in a + I$. If $b \in a+I$, then $\exists i \in I$ s.t. $b = a + i \Rightarrow b - a = i \in I$

In general $\boxed{b + I = a + I \iff b - a \in I}$

Note thus that coset representations are not unique!

3201-02.

Consider the set of cosets $R/I = \{a+I \mid a\in R\} = \{\bar{a} \mid a \in R\}$. We define $\bar{a}+\bar{b} := \overline{a+b}$, $\bar{a}\cdot\bar{b} := \overline{ab}$.

**Proposition** $R/I$ is a ring with the above operations.

Proof – Before checking our properties, we must ensure that operations are well-defined.

Let $\bar{a}=\bar{a'}$, $\bar{b}=\bar{b'}$. Then $\bar{a}+\bar{b}=\bar{a'}+\bar{b'} \Rightarrow \overline{a+b}=\overline{a'+b'}$? We know $a'-a\in I$, $b'-b\in I$. Then $(a'+b')-(a+b) = \underset{I}{\underset{\cap}{(a'-a)}}+\underset{I}{\underset{\cap}{(b'-b)}} \in I$. [ideal is closed under +]

Hence, $\overline{a+b}=\overline{a'+b'}$.

Similarly, we know $\bar{a}\cdot\bar{b}=\overline{ab}$, $\bar{a'}\cdot\bar{b'}=\overline{a'b'}$. Then $a'b'-ab = a'b'-a'b+a'b-ab = \overbrace{a'\underset{\cup}{(b'-b)}}^{I} + \overbrace{\underset{\cup}{(a'-a)}b}^{I \text{ (absorbency)}} \in I$. Thus, $\bar{a}\cdot\bar{b}=\overline{ab}$.

Note – From this part of the proof, absorbency is used. Here, it is clear why multiplicative closure in itself is an insufficient property.

We know that S1–S4 hold in $R/I$: since $(R,+)$ is an abelian group, $I$ is a subgroup of $R$, then $I \trianglelefteq R$ is a normal subgroup.

$\Rightarrow (R/I,+)$ is a group $\Rightarrow$ S1–S4 hold.

Then consider multiplication. If $\bar{a},\bar{b},\bar{c}\in R/I$, then $\bar{a}(\bar{b}\cdot\bar{c}) = \bar{a}\cdot(\overline{bc}) = \overline{a(bc)} = \overline{(ab)c} = \overline{ab}\cdot\bar{c} = (\bar{a}\cdot\bar{b})\cdot\bar{c} \Rightarrow$ associativity holds. [associativity in R]

$\bar{1}\cdot\bar{a} = \overline{1\cdot a} = \bar{a}$. Then since $1\in R$, $\bar{1}\in R/I$ is the unit element [same applies to $\bar{a}\cdot\bar{1}$].

EX → Finally, we need to prove distributivity:

Examples of sets of cosets $R/I$ –

1. $R/R = \{\bar{0}\}$, which is the trivial ring.
2. $R/(0) = R$.
3. Let $R=\mathbb{Z}$, $I(2)$. Then $\mathbb{Z}/(2) = \{\bar{0},\bar{1}\} = \mathbb{F}_2 = \mathbb{Z}_2$.

## 1.3 Ring homomorphisms.

**Definition** Let $R,S$ be rings. A map $f:R\to S$ is a <u>ring homomorphism</u> if

- $f(0)=0$ • $f(a+b)=f(a)+f(b)$ • $f(1)=1$ • $f(ab)=f(a)f(b)$.

If $f$ is injective it is a <u>monomorphism</u>, if $f$ is surjective it is an <u>epimorphism</u>, and if $f$ is bijective it is an <u>isomorphism</u>.

$R$ is isomorphic to $S$ ($R\cong S$) if there exists an isomorphism $f:R\to S$.

8 October 2013
Dr. Javier LÓPEZ PEÑA
Maths 500.

**Definition** If $f:R\to S$ is a ring homomorphism, we define <u>image</u> $\operatorname{Im} f := \{f(r) \mid r\in R\} \subseteq S$, and kernel $\operatorname{Ker} f := \{r\in R \mid f(r)=0\} \subseteq R$.

**Lemma** (1) $\operatorname{Im} f \le S$ is a subring and (2) $\operatorname{Ker} f \trianglelefteq R$ is an ideal.

Proof – (1) We just need to check zero, one, closure under + and ×. (zero) $\exists\, 0_S \in \operatorname{Im} f \because f(0_R)=0_S$ (one) $\exists\, 1_S\in\operatorname{Im} f \because f(1_R)=1_S$.

(closure under +) Let $x,y\in\operatorname{Im} f$. Then $\exists\, a,b\in R$ s.t. $x=f(a), y=f(b) \Rightarrow f(a)+f(b)=f(a+b)=x+y \Rightarrow x+y\in\operatorname{Im} f$.

(closure under ×) Likewise, $xy = f(a)\cdot f(b) = f(ab) \Rightarrow xy\in\operatorname{Im} f$ $\Rightarrow \operatorname{Im} f$ is a subring of $S$// q.e.d.

(2) (additive subgroup) $f(0_R)=0_S \Rightarrow 0_R\in\operatorname{Ker} f$, zero contained. Let $a,b\in\operatorname{Ker} f \Rightarrow f(a)=f(b)=0 \Rightarrow f(a+b)=f(a)+f(b)=0$, closed under addition.

$a\in\operatorname{Ker}(f) \Rightarrow f(-a)=-f(a)=-0=0 \Rightarrow -a\in\operatorname{Ker} f$, closed under inverses. [Alternatively, replace three conditions with $a-b\in\operatorname{Ker} f$].

(absorbency). Let $a\in\operatorname{Ker} f$, $r\in R$. Then $f(ra)=f(r)\cdot f(a)=f(r)\cdot 0=0 \Rightarrow ra\in\operatorname{Ker} f \Rightarrow$ absorbency. Thus $\operatorname{Ker} f\trianglelefteq R$// q.e.d.

**Theorem** (First Isomorphism Theorem).

Let $R,S$ be rings, $f:R\to S$ a ring homomorphism. Then $R/\operatorname{Ker} f \cong \operatorname{Im} f$.

Proof – Consider the map $\varphi: \frac{R}{\operatorname{Ker} f} \to \operatorname{Im} f$; $\overbrace{r+\operatorname{Ker} f}^{\text{cosets}} \longmapsto f(r)$. We must check that this application is well-defined.

(Well-defined) Assume $r+\operatorname{Ker} f = r'+\operatorname{Ker} f$. Then $\varphi(r+\operatorname{Ker} f) \overset{?}{=} \varphi(r'+\operatorname{Ker} f)$. $r'-r\in\operatorname{Ker} f \Rightarrow f(r'-r)=0 \Rightarrow f(r')-f(r)=0$

$\Rightarrow f(r')=f(r) \Rightarrow \varphi(r'+\operatorname{Ker} f)=\varphi(r+\operatorname{Ker} f) \Rightarrow$ well-defined.

(Ring structure) $\varphi(0+\operatorname{Ker} f)=f(0)=0$. $\varphi(1+\operatorname{Ker} f)=f(1)=1$. $a+\operatorname{Ker} f=\bar{a}$, $b+\operatorname{Ker} f=\bar{b}$. Then $\varphi(\bar{a}+\bar{b})=\varphi(\overline{a+b})=f(a+b)=f(a)+f(b)=\varphi(\bar{a})+\varphi(\bar{b})$.

$\varphi(\bar{a}\cdot\bar{b})=\varphi(\overline{ab})=f(ab)=f(a)f(b)=\varphi(\bar{a})\varphi(\bar{b})$. $\Rightarrow \varphi$ is a ring homomorphism.

(Isomorphism) $\varphi(\bar{a})=f(a)$, $\varphi(\bar{b})=f(b) \Rightarrow f(a)=f(b) \Rightarrow f(b-a)=0 \Rightarrow b-a\in\operatorname{Ker} f \Rightarrow \bar{a}=\bar{b} \Rightarrow \varphi$ injective.

Let $y\in\operatorname{Im} f$, $\exists\, r\in R$ s.t. $y=f(r)=\varphi(r+\operatorname{Ker} f) \Rightarrow y=\varphi(\bar{r}) \Rightarrow \varphi$ surjective.

This yields a bijective homomorphism $\Rightarrow$ isomorphism exists and $R/\operatorname{Ker} f\cong\operatorname{Im} f$// q.e.d.

Examples of ring homomorphisms –

1. Let $R$ be a ring. $\begin{array}{l} \mathrm{id}: R\to R \\ r\mapsto r \end{array} \Rightarrow$ identity map is a ring homomorphism.
2. Let $S\le R$ be a subring. $\iota: S\to R$, $s\mapsto s$. This is an inclusion map, which is a ring homomorphism.

3. $R=\mathbb{Z}=S$. $f:\mathbb{Z}\to\mathbb{Z}$, $n\mapsto 2n$. This is not a ring homomorphism since $f(1)=2\neq 1$.

4. [complex conjugation] $R=\mathbb{C}=S$, $\sigma:\mathbb{C}\to\mathbb{C}$, $z=a+bi\mapsto \bar{z}=a-bi$. This is a ring homomorphism.

5. Let $R$ be any ring, $I\trianglelefteq R$ an ideal. Then $\pi_I: R\to R/I$, $r\mapsto r+I$ is a ring homomorphism.

However, it is only injective if $I$ is the trivial zero ideal (in which it is identity map). Moreover, $\pi_I$ is always surjective.

6. Let $R$ be any ring, $a\in R$. Then consider $\begin{array}{rl} ev_a: R[x] &\longrightarrow R \\ p(x) &\longmapsto p(a)\end{array}$ is the evaluation of polynomial at $a$.

If $p,q$ are polynomials, $ev_a(p+q)=p(a)+q(a)=ev_a(p)+ev_a(q)$, $ev_a(p\cdot q)=ev_a(p)\cdot ev_a(q)$. $ev_a(0)=0$, $ev_a(1)=1 \Rightarrow$ ring homomorphism.

$\operatorname{Ker} ev_a=\{p(x)\in R[x] \mid p(a)=0\}=\{p(x)\in R[x] \mid (x-a)|p\}=\{(x-a)\cdot q \mid q\in R[x]\}$. This is the principal ideal generated by $x-a$, denoted $(x-a)$.

$\operatorname{Im} ev_a = R$ $\because$ $\forall b\in R$, $ev_a(\underbrace{b}_{\text{const polynomial } b})=b$.

By First Isomorphism Theorem, $\frac{R[x]}{(x-a)}\cong R$ indeed.

**Lemma** Let $f:R\to S$, $g:S\to T$ be ring homomorphisms. Then $g\circ f: R\to T$ is also a ring homomorphism.

Proof –
$$\left.\begin{array}{l}(g\circ f)(0_R)=g(f(0_R))=g(0_S)=0_T. \qquad (g\circ f)(1_R)=g(f(1_R))=g(1_S)=1_T.\\ (g\circ f)(a+b)=g(f(a+b))=g(f(a)+f(b))=g(f(a))+g(f(b))=(g\circ f)(a)+(g\circ f)(b).\\ (g\circ f)(ab)=g(f(ab))=g(f(a)f(b))=g(f(a))g(f(b))=(g\circ f)(a)\,(g\circ f)(b)\end{array}\right\}\ g\circ f \text{ is a ring homomorphism}_{//}\ \text{q.e.d.}$$

**Lemma** Let $R$ be a ring, $S\leq R$ a subring, $I\trianglelefteq R$ an ideal. Then

(1) $S+I=\{s+i \mid s\in S, i\in I\}\leq R$ is a subring, (2) $I\trianglelefteq S+I$ is an ideal, and (3) $S\cap I\trianglelefteq S$ is an ideal of $S$.

Proof – (1) $\left.\begin{array}{l}0\in S \text{ subring}\\ 0\in I \text{ subring}\end{array}\right\}$ $0=\underset{S}{0}+\underset{I}{0}\in S+I$. (in general, $\forall s\in S$, $s=s+0\in S+I$). $\left.\begin{array}{l}1\in S\\ 0\in I\end{array}\right\}1\in S+I$.

$x,y\in S+I \Rightarrow \begin{array}{l}\exists s_1,i_1 \text{ s.t. } x=s_1+i_1\\ \exists s_2\in S, i_2\in I \text{ s.t. } y=s_2+i_2\end{array} \Rightarrow x+y=s_1+i_1+s_2+i_2=\underset{S}{(s_1+s_2)}+\underset{I}{(i_1+i_2)}\in S+I$.

$x=s_1+i_1 \Rightarrow -x=-s_1-i_1\in S+I$. $\quad xy=(s_1+i_1)(s_2+i_2)=\overbrace{s_1s_2}^{S}+\overbrace{s_1i_2+i_1s_2+i_1i_2}^{I \text{ by absorbency}}\in S+I$.

(2) NTP: $I\trianglelefteq S+I$ is an ideal. We note that $\forall i\in I$, $0\in S$, $i=0+i\in S+I \Rightarrow I\subseteq S+I$. $I$ is closed for $+$, inverses, contains $0$.

For absorbency, $\forall x\in S+I$, $x\in R$. Since $I$ has absorbency w.r.t. $R$, $\forall i\in I$, $xi\in I \Rightarrow I$ is an ideal of $S+I$.

(3) $\left.\begin{array}{l}0\in S\\ 0\in I\end{array}\right\}0\in S\cap I$. $\quad x,y\in S\cap I \Rightarrow \begin{array}{l}x\in S,\ x\in I\\ y\in S,\ y\in I\end{array} \Rightarrow x-y\in S,\ x-y\in I \Rightarrow x-y\in S\cap I$. Take $x\in S\cap I$, $s\in S \Rightarrow \underset{sx\in S}{\boxed{\begin{array}{l}x\in S\\ s\in S\end{array}}}\ \underset{sx\in I}{\boxed{\begin{array}{l}x\in I\\ s\in S\end{array}}} \Rightarrow sx\in S\cap I$
$\Rightarrow S\cap I$ is an ideal$_{//}$ q.e.d.

(Second Isomorphism Theorem)

**Theorem** Let $R$ be a ring, $S\leq R$ a subring. If $I\trianglelefteq R$ is an ideal, then $\frac{S+I}{I}\cong\frac{S}{S\cap I}$.

Proof – Rather than finding an isomorphism between cosets, we try to define a homomorphism between $\frac{S+I}{S}$ and simply $S$.

We have $\begin{array}{ccccc} S & \xrightarrow{\iota} & S+I & \xrightarrow{\pi_I} & (S+I)/I\\ s & \underset{\text{inclusion}}{\longmapsto} & s+0=s & \longmapsto & \overline{s+i}\end{array}$. Thus, setting $\varphi:\pi_I\circ\iota$, we have a ring isomorphism $\varphi: S\to\frac{S+I}{I}$, $\varphi(s)=s+I$.

By 1st isomorphism theorem, it suffices to show that $\operatorname{Ker}\varphi=S\cap I$, $\operatorname{Im}\varphi=\frac{S+I}{I}$.

Take $x\in\frac{S+I}{I}$, $x=y+I$ for some $y\in S+I \Rightarrow \exists s\in S, i\in I$ s.t. $y=s+i \Rightarrow x=(s+i)+I$. Since $(s+i)-s=i\in I$, then

$s+i$, $s$ generate same coset $\Rightarrow x=(s+i)+I=s+I=\varphi(s)\Rightarrow x\in\operatorname{Im}\varphi$. Since $x$ was an arbitrary element, $\operatorname{Im}\varphi=\frac{S+I}{I}$.

Then, $\operatorname{Ker}\varphi=\{s\in S \mid \varphi(s)=0_{\frac{S+I}{I}}\}=\{s\in S \mid s+I=0+I\}=\{s\in S \mid s\in I\}=S\cap I \Rightarrow$ by 1st isomorphism theorem, $\frac{S+I}{I}\cong\frac{S}{S\cap I}{}_{//}$ q.e.d.

10 October 2013.
Dr. Javier LÓPEZ-PEÑA
Maths 500.

**Theorem** (Third Isomorphism Theorem)

Let $R$ be a ring, $I,J\trianglelefteq R$ be ideals with $I\subseteq J$, then $\frac{J}{I}\trianglelefteq\frac{R}{I}$ is an ideal and moreover, $\frac{(R/I)}{(J/I)}\cong\frac{R}{J}$.

Proof – $\frac{J}{I}=\{j+I \mid j\in J\}$. Let $a+I, b+I\in\frac{J}{I}$. Then $(a+I)-(b+I)=(a-b)+I\in\frac{J}{I}$ $\because$ $a-b\in J$. $\Rightarrow$ closed under $+$, inverses, has $0$.

Let $a\in J$, $a+I\in J/I$, $r+I\in R/I$. Then $(r+I)(a+I)=ra+I\in J/I \Rightarrow$ absorbency is satisfied. Then $\frac{J}{I}$ is an ideal$_{//}$ q.e.d.

Define $\varphi:\frac{R}{I}\to\frac{R}{J}$, $r+I\mapsto r+J$. We need to check if $\varphi$ is well-defined, i.e. $r+I=r'+I \Rightarrow r+J=r'+J$. By rule of equality on cosets,

clearly $r'-r\in I\subseteq J \Rightarrow r'-r\in J \Rightarrow r+J=r'+J$. Then, we establish that $\varphi$ is a ring homomorphism: $\varphi(0+I)=0+J$, $\varphi(1+I)=1+J$.

$\varphi((a+I)+(b+I))=\varphi((a+b)+I)=(a+b)+J=(a+J)+(b+J)=\varphi(a+I)+\varphi(b+I)$. Likewise, we have

$\varphi((a+I)(b+I))=\varphi(ab+I)=ab+J=(a+J)(b+J)=\varphi(a+I)\varphi(b+I) \Rightarrow \varphi$ is a homomorphism$_{//}$ q.e.d.

$\operatorname{Ker}\varphi=\{r+I\in R/I \mid \varphi(r+I)=0+J\}=\{r+I\in R/I \mid r+J=0+J\}=\{r+I\in R/I \mid r\in J\}=J/I$.

Also, $\operatorname{Im}\varphi=\{\varphi(r+I) \mid r+I\in R/I\}=\{r+J \mid r\in R\}=\frac{R}{J}$. Then by 1st isomorphism theorem, $\frac{(R/I)}{\operatorname{Ker}\varphi}\cong\operatorname{Im}\varphi \Rightarrow \frac{(R/I)}{(J/I)}\cong\frac{R}{J}{}_{//}$ q.e.d.

**Corollary** (Correspondence Theorem).

There are 1-1 correspondences $\{\text{subrings of } R/I\}\leftrightarrow\{\text{subrings } S\leq R \text{ s.t. } I\subseteq S\}$ and $\{\text{ideals of } R/I\}\leftrightarrow\{\text{ideals } J\trianglelefteq R \text{ s.t. } I\subseteq J\}$.

Proof. Simply take $J\mapsto J/I$ by applying 3rd isomorphism theorem$_{//}$ q.e.d.

chapter 2

# INTEGRAL DOMAINS: UFDs, PIDs, EDs.

We will deal with domains $R^* = R\setminus\{0\}$ where $R$ is a commutative ring. These are generally non-trivial in our course.

**Definition** $a \in R^*$ is a unit if $\exists b \in R$ s.t. $ab = 1$ (i.e. $a$ has a multiplicative inverse). $b = a^{-1}$ and $U(R)$ is the group of units in $R$.

Remark – $U(R)$ is a multiplicative group.

$a$ is a zero divisor if $\exists b \in R^*$ s.t. $ab = 0$.

**Definition** We say that $R$ is a field if every non-zero element is a unit (i.e. $U(R) = R^*$).

Examples of fields – 1. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$; 2. $\mathbb{Z}/(p)$, $p$ is prime 3. $\mathbb{R}(x) = \{\frac{f(x)}{g(x)} \mid f, g \in \mathbb{R}[x],\ g \neq 0\}$.

**Definition** $R$ is an integral domain (ID) if it has no zero divisors i.e. $ab = 0 \Rightarrow a = 0$ or $b = 0$ or equivalently $a \neq 0, b \neq 0 \Rightarrow ab \neq 0$.

Examples of integral domains –

1. All fields 2. $\mathbb{Z}$ 3. If $R$ is an integral domain, $R[x]$ is an integral domain as well.

**Proposition** (Cancellation law)

Let $R$ be an ID, $a, b, c \in R$ $(a \neq 0)$ s.t. $ab = ac \Rightarrow b = c$.

Proof – $ab = ac \Rightarrow ab - ac = 0 \overset{\text{distributivity}}{\Rightarrow} a(b-c) = 0 \Rightarrow a = 0$ or $b - c = 0 \overset{a\neq 0}{\Rightarrow} b - c = 0 \Rightarrow b = c$ // q.e.d.

**Definition** A ring $R$ is simple if it has no non-trivial ideals (i.e. no ideals apart from $(0)$ and $R$).

**Proposition** A commutative ring $R$ is simple $\Leftrightarrow$ $R$ is a field.

Proof – $(\Rightarrow)$. Let $R$ be a simple ring. Consider $a \in R^*$, then principal ideal generated by $a$ is $(a) \trianglelefteq R$. Clearly $(a) \neq (0)$ $\because a \neq 0$.

Since $R$ is simple, $(a) \neq (0) \Rightarrow (a) = R$ (total ideal) $\Rightarrow 1 \in (a) = R \Rightarrow \exists b \in R$ s.t. $1 = ab \Rightarrow R$ is a field.

$(\Leftarrow)$. Let $R$ be a field. Let $I \trianglelefteq R$ be an ideal. Assume $I \neq (0)$, then $\exists a \in I$ s.t. $a \neq 0$. Since $R$ is a field, $\exists a^{-1} \in R$.

By absorbency of ideal, $a^{-1}a \in I \Rightarrow 1 \in I$. Then $\forall x \in R$, $x = x \cdot 1$ and since $1 \in I$, by absorbency, $x \in I$. $\Rightarrow R \subseteq I \subseteq R \Rightarrow I = R$

Hence $I$ is either $(0)$ or $R$, so $R$ is necessarily simple by definition // q.e.d.

15 October 2013
Dr Javier LÓPEZ-PEÑA
Maths 500.

**Definition** Let $R$ be a ring, $I \triangleleft R$. We say $I$ is a maximal ideal if $I \subseteq J \trianglelefteq R$, then $J = I$ or $R$.

**Proposition** $I \trianglelefteq R$ is maximal $\Leftrightarrow$ $R/I$ is a field.

Proof – $R/I$ is a field $\Leftrightarrow$ $R/I$ is simple $\Leftrightarrow$ the only ideals of $R/I$ are $\{0\}$ and $R/I$. However, by the correspondence theorem $K \triangleleft R/I$. $\Leftrightarrow$ $K = J/I$ for some $J \trianglelefteq R$, $I \subseteq J \Rightarrow \forall K = \frac{J}{I} \trianglelefteq R/I$, then either $\frac{J}{I} = 0 \Rightarrow J = I$ or $\frac{J}{I} = \frac{R}{I} \Leftrightarrow J = R \Leftrightarrow \forall J \trianglelefteq R$ s.t. $I \subseteq J$, either $J = I$ or $J = R$.

$\Leftrightarrow$ $I$ is maximal // q.e.d.

**Definition** Let $R$ be a ring, $I \trianglelefteq R$. We say $I$ is a prime ideal if $ab \in I \Rightarrow a \in I$ or $b \in I$. (equivalently, $a \notin I, b \notin I \Rightarrow ab \notin I$.)

**Proposition** $R$ is a ring, $I \trianglelefteq R$ $(I \neq R)$. Then $I$ is a prime ideal $\Leftrightarrow$ $R/I$ is an integral domain.

Proof – $(\Rightarrow)$ Assume $I$ is prime. Take $\bar{a}, \bar{b} \in R/I$ s.t. $\bar{a} \cdot \bar{b} = 0 \Rightarrow \overline{ab} = \bar{0} \Rightarrow ab \in I \Rightarrow a \in I$ or $b \in I$ (by definition of $I$).

If $a \in I$ then $\bar{a} = \bar{0}$, and if $b \in I$ then $\bar{b} = \bar{0}$. So $\bar{a} \cdot \bar{b} = \bar{0} \Rightarrow \bar{a} = \bar{0}$ or $\bar{b} = \bar{0} \Rightarrow I$ is an integral domain // q.e.d.

$(\Leftarrow)$. Assume $R/I$ is an integral domain. Take $a, b \in R$ s.t. $ab \in I$, then $\overline{ab} = \bar{0}$ is in $R/I \Rightarrow \bar{a} \cdot \bar{b} = \bar{0} \Rightarrow \bar{a} = \bar{0}$ or $\bar{b} = \bar{0}$ as $R/I$ is integral domain.

Then $\bar{a} = 0 \Rightarrow a \in I$ or $\bar{b} = 0 \Rightarrow b \in I$. // q.e.d.

**Corollary** If $I \trianglelefteq R$ is maximal, then $I$ is a prime ideal.

Proof – $I$ is maximal $\Leftrightarrow$ $R/I$ is a field $\Rightarrow$ $R/I$ is an integral domain $\Leftrightarrow$ $I$ is prime // q.e.d.

## 2.2 Ideals and divisibility.

**Definition** If $R$ is a ring, $a, b \in R$, we say that $a$ divides $b$ / $b$ is a multiple of $a$ / $b$ is divisible by $a$ if $\exists c \in R$ s.t. $b = ac$. We write $a \mid b$.

Remark – $a \mid b \Leftrightarrow b \in (a) \Rightarrow b = ac$, $\forall d \in R$, $bd = acd \in (a)$. Then $a \mid b \Leftrightarrow (b) \subseteq (a)$.

**Definition** Let $R$ be a ring, $a, b \in R$. We say that $a$ and $b$ are associates (denoted $a \sim b$) if $\exists u \in U(R)$ s.t. $b = ua$.

**Proposition.** Let $R$ be an ID, $a,b\in R$, then the following hold:

(1) $a\sim b \Leftrightarrow a|b$ and $b|a$ (i.e. $(a)=(b)$). (2) $a\sim 1 \Leftrightarrow a\in U(R)$ [i.e. $\Leftrightarrow (a)=R$].

(3) $a\sim 0 \Leftrightarrow a=0$. (4) "being associates" is an equivalence relation $\begin{cases} a\sim a \\ a\sim b \Rightarrow b\sim a \\ a\sim b,\ b\sim c \Rightarrow a\sim c. \end{cases}$

Proof – (1) $a\sim b \Leftrightarrow \exists u\in U(R)$ s.t. $b=ua \Rightarrow a|b$ but $u\in U(R) \Rightarrow \exists u^{-1}\in U(R)$ s.t. $u\cdot u^{-1}=1$ so $b=ua \Rightarrow u^{-1}b=u^{-1}ua=a \Rightarrow b|a$.

Conversely, $\left.\begin{array}{l} a|b \Rightarrow \exists c\in R \text{ s.t. } b=ac \\ b|a \Rightarrow \exists d\in R \text{ s.t. } a=bd \end{array}\right\} b=b\cdot cd \Rightarrow \underset{\text{case 1:}}{cd=1}$ if $b\neq 0$, or $\underset{\text{case 2:}}{b=0}$. For case 1, $b\neq 0 \Rightarrow cd=1 \Rightarrow c,d\in U(R) \Rightarrow b=ac$ for $c\in U(R) \Rightarrow a\sim b$.

For case 2: if $b=0$, $b|a \Rightarrow a=0$, so $a\sim b$. In both cases, $a\sim b$, q.e.d.

(2) $a\sim 1 \Leftrightarrow \exists u\in U(R)$ s.t. $1=a\cdot u \Leftrightarrow a\in U(R)$, q.e.d. (3) $a=0 \Rightarrow a\cdot u=0\ \forall u\in U(R)$, q.e.d.

(4) $a=a\cdot 1 \Rightarrow a\sim a$. $a\sim b \Rightarrow b=au \Rightarrow a=u^{-1}b \Rightarrow b\sim a$ where $u\in U(R)$, $u^{-1}\in U(R)$.

$\left.\begin{array}{l} a\sim b \Rightarrow b=ua \\ b\sim c \Rightarrow c=vb \end{array}\right\} c=a(uv)$ for $u\in U(R)$, $v\in U(R) \Rightarrow a\sim c$, q.e.d.

## 2.3 Primes and Irreducibles.

**Definition** Let $R$ be an integral domain, $a,b\in R^*\setminus U$. Then $a$ is a <u>proper divisor</u> of $b$ if $\exists c\in R$, $c\notin U(R)$ s.t. $b=ac$.

[Equivalently, $a$ is a proper divisor of $b$ if $a|b$, but $a$ and $b$ are not associate i.e. $(b)\subsetneq(a)\subsetneq R$.]

**Definition** Let $R$ be an integral domain, $a\in R^*\setminus U(R)$. We say that $a$ is <u>irreducible</u> if $a\neq 0$, $a\notin U(R)$ and $a$ has no proper divisors.

[i.e. $b|a \Rightarrow$ either $b\in U(R)$ or $b\sim a$, or $(a)\subseteq(b) \Rightarrow (b)=R$ or $(b)=(a)$].

Note – This condition is very similar to the maximality condition, except we restrict it to the principal ideals. Thus, an element is irreducible $\Leftrightarrow$ $(a)$ is maximal ideal within all principal ideals.

**Ex** Show that if $R=\mathbb{Z}[x]$, $2\in R$ is irreducible but $(2)$ is not maximal.

Ans. 2 is irreducible in $\mathbb{Z}[x]$ $\because$ 2 is irreducible in $\mathbb{Z}$. [Note – $U(\mathbb{Z}[x])=\{\pm 1\}$, and in general, $U(R[x])=U(R)$].

However, $(2)$ is not maximal: $\mathbb{Z}[x]/(2)\cong\mathbb{F}_2[x]$ and this is not a field, as $x\in\mathbb{F}_2[x]$ and $\nexists a\in\mathbb{F}_2[x]$ s.t. $ax=1$. i.e. $x$ has no multiplicative inverse.

In fact, the only unit of $\mathbb{F}_2[x]$ is 1, q.e.d.

Note – $(2)\subseteq(2+x)=\{2f(x)+x\,g(x):\ f,g\in\mathbb{Z}[x]\}=\{$every polynomial in $\mathbb{Z}[x]$ with even constant term$\}$. This proves too that $(2)$ is not maximal, from the definition.

**Proposition** Let $R$ be an integral domain, $a\in R^*\setminus U(R)$. Then the following are equivalent:

(1) $a$ is irreducible, (2) If $a=bc$ for some $b,c\in R$, then either $b\in U(R)$ or $c\in U(R)$ (3) $a=bc$ for some $b,c\in R \Rightarrow$ either $b\sim a$ or $c\sim a$.

**Proposition** $R$ is an integral domain $\Rightarrow$ prime elements are also irreducible.

Proof – Assume $a=bc$, then $b|a$, $c|a$. On the other hand, $a|bc \Rightarrow$ either $a|b$ or $a|c$. Then we have:

- $b|a$ and $a|b \Rightarrow a\sim b$ • $c|a$ and $a|c \Rightarrow a\sim c$. Thus, $a$ is irreducible, q.e.d.

## 2.4 Principal Ideal Domains.

Consider $(4)\subseteq\mathbb{Z}$, $(6)\subseteq\mathbb{Z}$. Then $(4)+(6)=\{4h+6k\mid h,k\in\mathbb{Z}\}=(2)$, where $\gcd(4,6)=2$.

Recall from earlier example that in $(2)+(x)$, we had $(2+x)\neq(1)$, where $1\neq\gcd(2,x)$.

17 October 2013
Dr Javier LÓPEZ-PEÑA.
40 hrs 500

**Definition** $R$ is a commutative ring. We say that $R$ is a <u>principal ideal domain</u> if $R$ is an ideal domain and $\forall I\trianglelefteq R$, $\exists a\in R$ s.t. $I=(a)$

Remark – $(a)=(b) \Leftrightarrow a\sim b$. If $R$ is a PID, $I=(a) \Rightarrow a$ is unique up to associates.

Examples of Principal Ideal Domains –

1. $\mathbb{F}$ is a field, which is simple $\Rightarrow I\trianglelefteq\mathbb{F} \Rightarrow \left.\text{either } I=\mathbb{F}=(1) \text{ or } I=0=(0)\right\} \Rightarrow \mathbb{F}$ is a PID.
2. $\mathbb{Z}$. Using group theory, we provide a hand-waving proof (for now): $I\trianglelefteq\mathbb{Z} \Rightarrow I$ is an additive subgroup of $\mathbb{Z} \Rightarrow \mathbb{Z}$ cyclic as an additive group $\Rightarrow I$ cyclic $\Rightarrow I=(n)$ for some $n\in\mathbb{Z} \Rightarrow$ PID.
3. Let $\mathbb{F}$ be a field, then $\mathbb{F}[x]$ is a PID.

**Proposition** If $R$ is a PID, every irreducible element is prime.

Proof – $a$ irreducible $\Leftrightarrow$ $(a)$ maximal among principal ideals. But every ideal is principal $\Rightarrow$ $(a)$ maximal. More explicitly, take $I$ s.t. $(a)\subseteq I$.

$R$ is a PID $\Rightarrow \exists b\in R$ s.t. $I=(b) \Rightarrow (a)\subseteq(b) \Rightarrow a\in(b) \Rightarrow \exists c\in R$ s.t. $a=bc$. However, $a$ is irreducible $\Rightarrow$ either $b$ is a unit or $b\sim a$.

If $b$ is a unit, $(b)=R$. Whereas if $b\sim a$, $(b)=(a)$. Thus, $I=R$ or $(a) \Rightarrow$ by definition, $(a)$ is maximal.

$(a)$ is maximal $\Rightarrow$ $(a)$ is a prime ideal $\Leftrightarrow$ $a$ is prime, q.e.d.

**Corollary** If $R$ is a principal ideal domain, $I \trianglelefteq R$ is a prime ideal $\Rightarrow$ $I$ is maximal.

## 2.5 Euclidean Domains.

These are very specialised types of rings, $ED \subseteq PID \subseteq ID$, in which we can intuit some kind of Euclidean division for the group.

In $\mathbb{Z}$, $a,b \in \mathbb{Z}$. Then $b \neq 0 \Rightarrow \exists q,r$ s.t. $a = bq + r$ with either $|r| < |b|$ or $r = 0$. This is not necessarily unique, as it depends strictly on positivity.

For instance, $9 = 4 \cdot 2 + 1 = 4 \cdot (3) + (-3) \Rightarrow$ not unique, but satisfies our earlier conditions.

We extend this notion to other rings. For instance, in $\mathbb{F}[x]$, our conditions become $\deg(r(x)) < \deg(b(x))$ or $r = 0$ (which has no degree).

This means that we need to find a function that translates elements in $R$ to a comparable number (i.e. that is well-ordered).

**Definition** An <u>Euclidean domain</u> is an integral domain $R$ endowed with a map $N : R^* \to \mathbb{N}$, the <u>Euclidean norm</u>, that satisfies

ED1: If $a, b \in R^*$ and $a | b$, then $N(a) \leq N(b)$, and

ED2: $\forall a, b \in R^*$, $\exists q, r \in R$ s.t. $a = bq + r$ and either $r = 0$ or $N(r) < N(b)$.

Examples of EDs —

1. $\mathbb{Z}$, where $N(a) = |a|$ under usual division
2. $\mathbb{F}[x]$, $N(f(x)) = \deg(f(x))$ under polynomial division. (not its root!)
3. Gaussian integers: $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$. $N(a+bi) = a^2 + b^2$. If $z = a + bi$, $N(z) = z\bar{z}$.
   $\mathbb{Z}[i] \subseteq \mathbb{C}$ field, ID $\Rightarrow$ $\mathbb{Z}[i]$ is an ID.

Claim — $(\mathbb{Z}[i], N)$ is an ED. ED1: Take $z | w$ in $\mathbb{Z}[i]$. $w = zt$ for some $t \in \mathbb{Z}[i] \Rightarrow N(w) = N(zt) = zt \cdot \overline{(zt)} = z \cdot t \cdot \bar{z} \cdot \bar{t} = z\bar{z} \cdot t\bar{t} = N(z)N(t)$

We know $\forall (R,N)$ ED, $\forall a \in R$, $1 | a \Rightarrow N(1) \leq N(a)$. Let $t = c + di$, $c, d \in \mathbb{Z}$. Then $w \neq 0 \Rightarrow t \neq 0 \Rightarrow$ either $c$ or $d \neq 0 \Rightarrow c^2 + d^2 > 0 \Rightarrow c^2 + d^2 \geq 1$.

i.e. $N(t) \geq 1$, so $N(w) = N(z) \cdot N(t) \geq N(z)$. For ED2: Take $z, w \in \mathbb{Z}[i]$, $w \neq 0$. We know that $\mathbb{Z}[i] \subseteq \mathbb{Q}(i)$ ($\mathbb{C}$ with $\mathbb{Q}$ coefficients), which is a field. Then we can take

$w^{-1} \in \mathbb{Q}(i)$. $z \cdot w^{-1} \in \mathbb{Q}(i) \Rightarrow zw^{-1} = a + bi$, $a, b \in \mathbb{Q}$. Take $u, v$ s.t. $|u - a| \leq \frac{1}{2}$, $|v - b| \leq \frac{1}{2}$. Then $q = u + vi \in \mathbb{Z}[i]$. Then we define

$s = (a-u) + (b-v)i \in \mathbb{Q}(i)$. Then $r = sw \in \mathbb{Q}(i)$. However, we have $q \cdot w + r = q \cdot w + s \cdot w = (q + s) \cdot w = (a + bi) \cdot w = zw^{-1} \cdot w = z \in \mathbb{Z}[i]$.

Then $r = z - qw \in \mathbb{Z}[i]$. Then $N(r) = N(sw) = sw\overline{(sw)} = s\bar{s}w\bar{w} = N(s)N(w)$. Using same definition, $N(s) = (a-u)^2 + (b-v)^2 \leq \frac{1}{4} + \frac{1}{4} \leq \frac{1}{2} < 1$.

Thus $N(r) = N(s)N(w) < N(w)$ // q.e.d.

22 October 2013
Dr. Javier LÓPEZ-PEÑA
Maths 500.

Clearly then, $\forall a \in R^*$, $N(a) \geq N(1)$.

**Proposition** If $R$ is an integral domain, $N : R^* \to \mathbb{N}$ is a map satisfying ED2 $\Rightarrow$ $R$ is a principal ideal domain. [In particular, $R$ is an ED $\Rightarrow$ $R$ is a PID.].

Proof — Take $I \trianglelefteq R$. If $I = 0$, $I = (0)$. If $I = R$, $I = (1)$. Assume $I \neq 0$, $I \neq R$. Then $I$ contains at least one non-zero element.

Consider the set $\{N(a) \mid a \in I, a \neq 0\} \subseteq \mathbb{N}$. By Archimedean principle of natural numbers, every non-empty subset of $\mathbb{N}$ contains a minimal element.

$\Rightarrow \exists a \in I$ s.t. $N(a)$ is the smallest (among elements of $I$). Claim: $I = (a)$. Pick any element $b \in I$. Then by ED2, $b = aq + r$, where • $r \neq 0$ or • $N(r) < N(a)$.

$r = \underset{\in I}{b} - \underset{\in I}{a}q \Rightarrow aq \in I \Rightarrow r \in I$, so $N(r) < N(a)$ is impossible by minimality of $N(a)$. Thus $r = 0 \Rightarrow b = aq \Rightarrow b$ is a multiple of $a \Rightarrow b \in (a) \Rightarrow I = (a)$ // q.e.d.

**Corollary** $\mathbb{Z}$ is a PID, $\mathbb{F}[x]$ is a PID. (but $\mathbb{Z}[x]$ is not!), and $\mathbb{Z}[i]$ is a PID.

Proof — All three a IDs satisfying ED2.

**Proposition** Let $(R, N)$ be an ED. Take $a \in R^*$, then $a \in U(R) \iff N(a) = N(1)$.

Proof — ($\Rightarrow$). Assume $a \in U(R)$. Then $N(1) \leq N(a)$. $1 = a \cdot a^{-1} \Rightarrow a | 1 \overset{ED1}{\Rightarrow} N(a) \leq N(1) \Rightarrow N(a) = N(1)$ // q.e.d.

($\Leftarrow$). $a \in R$, $N(a) = N(1)$. We can write $1 = a \cdot q + r$ where either $r = 0$ or $N(r) < N(a)$. If $N(r) < N(a) = N(1)$, this is a contradiction as $N(1)$ is minimal

$\therefore r = 0 \Rightarrow 1 = a \cdot q \Rightarrow a \in U(R)$.

Examples —

1. $U(\mathbb{Z}) = \{n \in \mathbb{Z} \mid N(n) = N(1)\} = \{n \in \mathbb{Z} \mid |n| = 1\} = \{1, -1\}$.
2. $U(\mathbb{F}[x]) = \{f \in \mathbb{F}[x] \mid N(f) = N(1)\} = \{f \in \mathbb{F}[x] \mid \deg f = \deg(1) = 0\} = \mathbb{F}^*$ (i.e. constants except zero polynomial).
3. $U(\mathbb{Z}[i]) = \{a + bi \in \mathbb{Z}[i] \mid N(a+bi) = N(1)\} = \{a + bi \in \mathbb{Z}[i] \mid a^2 + b^2 = 1\} = \{a + bi \in \mathbb{Z}[i] \mid a = 1, b = 0$ or $a = 0, b = 1\} = \{1, i, -1, -i\}$.
4. Non-example: Let $R = \mathbb{Z}[\sqrt{2}]$, $N(a + b\sqrt{2}) = |a^2 - 2b^2|$. $(R,N)$ is an ED, but $U(\mathbb{Z}[\sqrt{2}]) = \{a + b\sqrt{2} \mid |a^2 - 2b^2| = 1\} = \{a + b\sqrt{2} \mid a^2 - 2b^2 = \pm 1\}$

   Solving this will require the use of Pell's equations.

## 2.6 Unique Factorisation Domains.

**Definition** Let $R$ be an integral domain. Then $R$ is a unique factorisation domain (UFD) if every non-zero, non-unit element $a$ of $R$ ($a \in R^* \setminus U(R)$) can be written as a product $a = p_1 \cdots p_r$ where $p_i$ are irreducible, and moreover such a factorisation is unique up to reordering of $p_i$ terms and up to associates (multiplication by units).

**Proposition** If $R$ is an integral domain, the following are equivalent:

(1) $R$ is a UFD, (2) Every $a \in R^* \setminus U(R)$ admits a factorisation into prime elements, (3) Every $a \in R^* \setminus U(R)$ admits a factorisation into irreducibles, and every irreducible is prime.

Proof – (1)$\Rightarrow$(3): Assume $R$ is a UFD. Existence of factorisation comes from definition of UFD. Only NTP: every irreducible is prime. Let $a \in R^* \setminus U(R)$, a irreducible. Assume $a | bc$. (If $bc = 0$, $b = 0 \Rightarrow a|b$ or $c = 0 \Rightarrow a|c$). Suppose $bc \neq 0$. $a|bc \Rightarrow \exists d \in R$ s.t. $ad = bc$. If $b \in U(R)$, $\exists b^{-1} \in R$ s.t. $adb^{-1} = c \Rightarrow a|c$. Likewise if $c \in U(R)$, $adc^{-1} = b \Rightarrow a|b$. So we eliminate cases and are left with $b, c \in R^* \setminus U(R)$. Then $R$ is a UFD $\Rightarrow$ $b = b_1 \cdots b_s$, $c = c_1 \cdots c_t$ for unique $b_i, c_j$ irreducible. Assume also that $d \in R^* \setminus U(R)$, eliminating zero and unit cases similarly. Then $d = d_1 \cdots d_r$ for irreducible $d_k$. Then $ad = bc \Rightarrow ad_1 \cdots d_r = b_1 \cdots b_s c_1 \cdots c_t$. $\Rightarrow$ two factorisations of same element in $R$. Since $R$ is UFD, $b_1 \cdots b_s c_1 \cdots c_t$ is a reordering (up to associates) of $ad_1 \cdots d_r$. So $\exists i$ s.t. $a \sim b_i$ or $\exists j$ s.t. $a \sim c_j \Rightarrow a|b_i|b$ or $a|c_j|c$
$\Rightarrow a|bc$ implies $a|b$ or $a|c \Rightarrow a$ is prime// q.e.d.

(3)$\Rightarrow$(2): Trivial, from definition of (3).

(2)$\Rightarrow$(1): Take $a \in R^* \setminus U(R)$. Then by (2), $a = p_1 \cdots p_r$ with $p_i$ prime. Hence, a factorisation into primes exists. Also, $p_i$ prime $\Rightarrow p_i$ irreducible $\Rightarrow a$ has factorisation into irreducibles. Then NTP: uniqueness. Assume $a = p_1 \cdots p_r = q_1 \cdots q_s$ with $q_i$ irreducible. We prove uniqueness (i.e. $r = s$, and $p_i \sim q_i$ after relabelling) by induction on $r$:

Take $r = 1$. Then $p_1 = q_1 \cdots q_s$ with $\{q_i\}$ irreducible. Then $s = 1$, $p_1 = q_1 \Rightarrow p_1 \sim q_1$.

Assume claim holds for $r-1$, any $s$. Then consider $p_1 \cdots p_{r-1} p_r = q_1 \cdots q_s$. $\Rightarrow p_r | q_1 \cdots q_s$. $p_r$ is prime $\Rightarrow \exists q_j$ s.t. $p_r | q_j$. Reordering, WLOG, $p_r | q_s$. $\Rightarrow q_s = p_r \cdot u$, $q_s$ is irreducible. $p_r$ is not a unit, so $u$ is a unit and $p_r \sim q_s$.

Then $p_1 \cdots p_r = q_1 \cdots q_s = q_1 \cdots q_{s-1} u p_r \Rightarrow$ by cancellation property, $p_1 \cdots p_{r-1} = q_1 \cdots (q_{s-1} u)$. By inductive hypothesis, we have $r-1 = s-1 \Rightarrow r = s$, and $p_1 \sim q_1, \ldots, p_{r-1} \sim q_{r-1}$ $\Rightarrow$ decomposition is unique $\Rightarrow$ $R$ is a UFD.

We aim to show eventually that PID $\Rightarrow$ UFD. To prove this, it is sufficient to show the existence of factorisations. We will first introduce some abstract theory.

## 2.7 Chain conditions.

We can factorise things by an iterative process. However, how do we know that the process ends? For integers, quotients decrease and are bounded below. But for general $R$?

**Definition** If $R$ is an integral domain, we say that $R$ satisfies the ascending chain condition (ACC) for principal ideals if for every chain of (principal ideals),
$I_1 \subseteq I_2 \cdots \subseteq I_n \subseteq I_{n+1}$, $\exists N \in \mathbb{N}$ s.t. $\forall n \geq N$, $I_n = I_N$.

Consider $(a_1) \subseteq (a_2) \subseteq \cdots \subseteq (a_n) \subseteq (a_{n+1}) \subseteq \cdots$. We know that $a|b \Leftrightarrow (b) \subseteq (a)$, so this means that there is a finite chain of divisors as they get smaller down the chain.

**Proposition** (Case of Zorn's lemma).
Let $R$ be a ring satisfying ACC for (principal) ideals. Then if $\mathcal{S}$ is any non-empty family of (principal) ideals $\Rightarrow \exists I \in \mathcal{S}$ which is maximal in $\mathcal{S}$.
(i.e. $\forall J \in \mathcal{S}$ s.t. $I \subseteq J$, then $I = J$).

Proof – Let $\mathcal{S} \neq \emptyset$ be a family of ideals. Assume $\mathcal{S}$ does not admit a maximal element. Pick $I_1 \in \mathcal{S}$, so $I_1$ is not a maximal element.
$\Rightarrow \exists I_2 \in \mathcal{S}$ s.t. $I_1 \subsetneq I_2$, but $I_2$ is not maximal either. $\Rightarrow \exists I_3 \in \mathcal{S}$, $I_2 \subsetneq I_3 \Rightarrow \cdots \Rightarrow \exists I_{n+1} \in \mathcal{S}$ s.t. $I_n \subsetneq I_{n+1}$.
Thus, we have a chain $I_1 \subsetneq I_2 \subsetneq \cdots \subsetneq I_n \subsetneq I_{n+1} \subsetneq \cdots$ is a contradiction with ACC as inclusions are strict, so $\nexists N \in \mathbb{N}$ s.t. $\forall n \geq N$, $I_n = I_N$// q.e.d.

Example –
Let $R$ be a UFD. Then if $a \in R^* \setminus U(R)$, $(a) \subseteq (b) \Rightarrow b|a$. By unique factorisation, $a = p_1 \cdots p_r$, $b|a \Rightarrow \exists i_1, \ldots, i_s$ $1 \leq i_1 < \cdots < i_s \leq r$ s.t. $b \sim p_{i_1} \cdots p_{i_s}$. $a$ can only have finitely many divisors (up to units) $\Rightarrow$ only finitely many principal ideals $(b)$ s.t. $(a) \subseteq (b)$.
Thus, $(a_1) \subseteq (a_2) \subseteq \cdots \subseteq (a_n) \subseteq (a_{n+1}) \subseteq \cdots$ stabilises as all $(a_i)$ must belong to finite set $\Rightarrow R$ satisfies ACC// q.e.d.

24 October 2013
Dr. Javier LÓPEZ-PEÑA
Maths 500.

**Proposition** If $R$ satisfies ACC on principal ideals, then every element $a \in R^* \setminus U(R)$ admits a factorisation as a product of irreducibles.

Proof – Define $\mathcal{S} = \{(a) \mid a \in R^* \setminus R(U)$ and cannot be written as a product of irreducibles$\}$. NTP: $\mathcal{S} = \emptyset$. Proof by contradiction: assume $\mathcal{S} \neq \emptyset$. Then there are elements with no factorisation. By lemma, $\exists (a) \in \mathcal{S}$ which is maximal. $a \in R^* \setminus R(U)$ and $a$ is not a product of irreducibles
$\Rightarrow a$ cannot be irreducible, because $a = a$. $\Rightarrow \exists b, c \in R$ s.t. $a = bc$. Then $b, c$ are proper divisors (i.e. not units, not associates of $a$).
Then $b|a \Rightarrow (a) \subseteq (b)$. Since $a \not\sim b$, the principal ideals generated are not the same, so $(a) \subsetneq (b)$. Since $b$ is not a unit, $(b)$ is larger than $(a)$.
$\Rightarrow (b) \notin \mathcal{S} \Rightarrow$ since $b \in R^* \setminus U(R)$, $b$ can be written as a product of irreducibles, $b = b_1 \cdots b_r$. Likewise, $c|a \Rightarrow (a) \subsetneq (c) \Rightarrow c = c_1 \cdots c_s$ ($c_i$ irreducibles).
Clearly then $a = b_1 \cdots b_r c_1 \cdots c_s$, a product of irreducibles, so $(a) \notin \mathcal{S} \Rightarrow \mathcal{S} = \emptyset$// q.e.d.

3201-08.

**Proposition** Every PID satisfies ACC.

Proof – consider an ascending chain of ideals $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$ Consider $I = \bigcup_{n\geq 1} I_n$, which is an infinite union. We claim $I \trianglelefteq R$ is an ideal.

$\cdot\, 0 \in I \because 0 \in I_1 \subseteq I$ $\quad\cdot$ Let $a, b \in I$, $\exists n$ s.t. $a \in I_n$, $\exists m$ s.t. $b \in I_m$. If $m \geq n$, $I_n \subseteq I_m$, so $a \in I_m$ [otherwise $n \geq m$ so $b \in I_n$].

$\Rightarrow \exists\, n \in \mathbb{N}$ s.t. $a, b \in I_n \Rightarrow a - b \in I_n \subseteq I$. $\quad\cdot$ Let $a \in I, r \in R$, then $\exists n \in \mathbb{N}$ s.t. $a \in I_n \Rightarrow r \cdot a \in I_n \subseteq I$. Thus, $I \trianglelefteq R$ is an ideal.

Since $R$ is a PID, each ideal is principal $\Rightarrow I$ is principal. Then $\exists a \in R$ s.t. $I = (a)$. $a \in I = \bigcup_{n\geq 1} I_n \Rightarrow \exists N \in \mathbb{N}$ s.t. $a \in I_N \Rightarrow a \in (I_N)$.

$\forall\, n \geq N$, $I_N \subseteq I_n \subseteq I = (a)$. However, $(a) \in (I_N) \Rightarrow (a) \subseteq I_N \Rightarrow I_n = (a) = I_N$, q.e.d.

**Corollary** ED $\Rightarrow$ PID $\Rightarrow$ UFD.

2.8 The rings $\mathbb{Z}[\sqrt{m}]$

Here, consider $m \in \mathbb{Z}$ which is not a square. Then $\mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ (or $\mathbb{R}$ if $m > 0$). Then $\mathbb{Z}[\sqrt{m}]$ is a subring of an ID, so $\mathbb{Z}[\sqrt{m}]$ is an ID.

In fact, $\mathbb{Z}[\sqrt{m}] \cong \dfrac{\mathbb{Z}[x]}{(x^2 - m)}$ by the 1st isomorphism theorem.

Define $N : \mathbb{Z}[\sqrt{m}]^* \longrightarrow \mathbb{N}$ by $N(a + b\sqrt{m}) = |(a + b\sqrt{m})(a - b\sqrt{m})| = |a^2 - mb^2|$ [compare to where $m = 1$, which gives the norm on $\mathbb{Z}[i]$. Absolute values are required to keep it in $\mathbb{N}$].

**Proposition** The map $N$ has the following properties:

(1) $N(\alpha\beta) = N(\alpha)N(\beta)$ $\quad$ (2) $\alpha \in U(\mathbb{Z}[\sqrt{m}]) \Leftrightarrow N(\alpha) = 1$. $\quad$ (3) $\alpha \sim \beta \Leftrightarrow \beta \mid \alpha$ and $N(\beta) = N(\alpha)$.

Proof – omitted, same as computations for $\mathbb{Z}[i]$.

We can characterise the different types of $\mathbb{Z}[\sqrt{m}]$: if $m = -1$, $U(\mathbb{Z}[\sqrt{-1}]) = \{1, -1, i, -i\}$, if $m \leq -2$, $U(\mathbb{Z}\sqrt{m}) = \{1, -1\}$ ($a^2 + |m|b^2 = 1$), if $m \geq 2$, $U(\mathbb{Z}[\sqrt{m}]) = \{a + b\sqrt{m} \mid \underbrace{a^2 - mb^2 = \pm 1}_{\text{Pell's equation, in general has infinitely many solutions.}}\}$

i.e. there are either 2, 4 or infinitely many units.

29 October 2013.
Dr. Javier LÓPEZ-PEÑA.
Maths 500.

Proposition. $\mathbb{Z}[\sqrt{m}]$ satisfies ACC on principal ideals. (In particular, every non-zero non-unit element decomposes as a product of irreducibles).

Proof – Take an ACC of principal ideals, $(a_1) \subseteq (a_2) \subseteq \cdots \subseteq (a_n) \subseteq \cdots$, $a_2 \mid a_1$, $a_3 \mid a_2$, $\ldots$, $a_{n+1} \mid a_n$. $\Rightarrow a_{n+1} \mid a_n \mid \cdots \mid a_3 \mid a_2 \mid a_1$.

Then $N(a_{n+1}) \mid N(a_n) \mid \cdots \mid N(a_2) \mid N(a_1) \Rightarrow N(a_1) \geq N(a_2) \geq \cdots \geq N(a_n) \geq N(a_{n+1}) \geq \cdots \Rightarrow \exists k \in \mathbb{N}$ s.t. $N(a_n) = N(a_k)$ $\forall n \geq k$.

$n \geq k \Rightarrow (a_k) \subseteq (a_n) \Rightarrow a_n \mid a_k \Rightarrow a_n \sim a_k$ by property 3 $\Rightarrow (a_n) = (a_k)$ $\forall n \geq k$, q.e.d.

Examples of $\mathbb{Z}[\sqrt{m}]$:

1. $\mathbb{Z}[\sqrt{-5}]$. Then $6 \in \mathbb{Z}[\sqrt{-5}]$, $6 = 2\cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. Claim that $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ are irreducible in $\mathbb{Z}[\sqrt{-5}]$. If $\alpha \mid \beta$, $N(\alpha) \mid N(\beta)$. Then by contradiction, assume $2 = \alpha\beta$ in $\mathbb{Z}[\sqrt{-5}]$, then $N(2) = N(\alpha\beta) \Rightarrow 4 = N(\alpha)N(\beta)$. WLOG, $N(\alpha) = 1, 2$ or $4$. $N(\alpha) = 1 \Rightarrow \alpha$ is a unit. $N(\alpha) = 4 \Rightarrow \beta$ is a unit, and $\alpha \sim 2$.
Thus $\alpha$ is a proper divisor of $2 \Rightarrow N(\alpha) = 2$. $\alpha = x + y\sqrt{-m} \Rightarrow N(\alpha) = |x^2 - my^2| = |x^2 + 5y^2| = 2$. $x^2 + 5y^2 = 2$ in integers $\underset{\text{if } y \neq 0,\ 5y^2 \geq 5 > 2.\ \text{Thus}}{\Rightarrow} y = 0$, and $x$ has no solution.
$\Rightarrow \nexists\, \alpha \in \mathbb{Z}[\sqrt{-5}]$ s.t. $N(\alpha) = 2 \Rightarrow 2$ is irreducible. Likewise, 3 is irreducible $\because \nexists\, (x, y) \in \mathbb{Z}^2$ s.t. $x^2 + 5y^2 = 3$.
$N(1 \pm \sqrt{-5}) = |1 + 5| = 6$. $\alpha \mid (1 \pm \sqrt{-5}) \Rightarrow N(\alpha) = \{1, 2, 3, 6\}$. Thus, $1 \pm \sqrt{-5}$ is irreducible. Then $2\cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ are two different factorisations of the same element $6 \in \mathbb{Z}[\sqrt{-5}]$. Thus, $\mathbb{Z}[\sqrt{-5}]$ is not a UFD. Moreover, $2 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ but does not divide either of $1 \pm \sqrt{-5}$ because $N(2) \nmid N(1 \pm \sqrt{-5})$.
2. $\mathbb{Z}[\sqrt{-7}]$. Then $8 = 2\cdot 2\cdot 2 = (1 + \sqrt{-7})(1 - \sqrt{-7})$. Then $2$, $1 \pm \sqrt{-7}$ are irreducibles. $\Rightarrow$ number of irreducibles in factorisations does not need to be unique.

2.9 GCD and factorisations.

**Definition** Let $R$ be a UFD, $a, b \in R$. Then $d$ is a (not "the"!) greatest common divisor of $a$ and $b$ if (1) $d \mid a$, $d \mid b$ and (2) $e \mid a, e \mid b \Rightarrow e \mid d$. (norms here may not be defined if not ED!)

[Alternatively: (1) $(a) \subseteq (d)$, $(b) \subseteq (d)$ and (2) $\left.\begin{matrix}(a) \subseteq (e)\\(b) \subseteq (e)\end{matrix}\right\}$ $(d) \subseteq (e)$ ].

If $d, d'$ are gcds of $a, b$, $(d) \subseteq (d') \subseteq (d)$ and thus, $(d) = (d')$ and $d \sim d'$. i.e. if gcds exist, they are unique up to associates.

**Proposition** gcd has the following properties:

(1) If $a = 0$, $\gcd(a, b) = b$. $\quad$ (2) If $a \in U(R)$, $\gcd(a, b) = 1$ [or $a$] $\quad$ (3) If $a = u p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, $b = v p_1^{\beta_1} \cdots p_r^{\beta_r}$ where $\alpha_i, \beta_i \geq 0$, $u, v \in U(R)$, $p_i$ are distinct primes $\Rightarrow d = \prod p_i^{\gamma_i}$, $\gamma_i = \min(\alpha_i, \beta_i)$ is the gcd of $(a, b)$.

(4) If $R$ is a PID, $a, b \in R$. Then $(a) + (b)$ must be principal (PID) and $(a) + (b) = (d)$ for some $d \in R$. $d$ is $\gcd(a, b)$ and moreover, $d \in (d) = (a) + (b)$. Then $\exists\, h, k$ s.t. $d = ah + bk \Rightarrow$ (Bézout's Identity) $\quad$ (5) If $(R, N)$ is an ED $\Rightarrow$ gcd can be calculated by Euclidean algorithm.

Proof – omitted (or already partly given).

Proposition If $R$ is a UFD, $\gcd(ra_1, \ldots, ra_n) = r\gcd(a_1, \ldots, a_n)$. In particular, if $d = \gcd(a_1, \ldots, a_n)$, $\gcd\left(\frac{a_1}{d}, \ldots, \frac{a_n}{d}\right) = 1$.

Proof – omitted.

## 2.10 Field of fractions.

We know that given a field $\mathbb{F}$, $R \leq \mathbb{F}$ is a subring $\Rightarrow$ $R$ is an integral domain. Can we construct a field out of any integral domain $R$? Yes.

This is analogous to constructing $\mathbb{Q}$ from $\mathbb{Z}$. This is outlined in the method below:

Let $R$ be an integral domain, consider the set $\{(a,b) \mid a,b \in R,\ b \neq 0\} = R \times R^*$. Define the relation $(a,b) \sim (c,d) \Leftrightarrow ad = bc$. Claim: $\sim$ is an equivalence relation.

i.e. satisfies ① reflexivity ✓ $(a,b) \sim (a,b)$, ② symmetry ✓ $(a,b) \sim (c,d) \Rightarrow (c,d) \sim (a,b)$, ③ transitivity ✓. $(a,b) \sim (c,d),\ (c,d) \sim (e,f) \Rightarrow ad = bc,\ cf = de \Rightarrow adf = bcf = bde \overset{d \neq 0}{\Rightarrow} af = be \Rightarrow (a,b) \sim (e,f)$

Then we obtain equiv classes $\overline{(a,b)} = \{(c,d) \in R \times R^* \text{ s.t. } (c,d) \sim (a,b)\}$. Notation: we write $\frac{a}{b} := \overline{(a,b)}$. Take $Q = \{\frac{a}{b} \mid a,b \in R,\ b \neq 0\}$. Then we define the operations

$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$, $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$. Claim: 1. $+, \times$ are well-defined 2. With $+, \times$, $Q$ is a field. i.e. $\frac{a}{b} \in Q,\ a \neq 0 \Rightarrow (\frac{a}{b})^{-1} = (\frac{b}{a})$.

$\boxed{\text{Theorem}}$ (Field of fractions).

Let $R$ be an integral domain, then $\exists Q$ field such that • $R \leq Q$ and • $\forall q \in Q,\ \exists a,b \in R,\ b \neq 0$ s.t. $q = ab^{-1}$.

Moreover, $Q$ is unique up to field isomorphism.

Note: consider general construction $R \times S$, if $S \subseteq R$ st. $\begin{cases} 1 \in S \\ s,t \in S \Rightarrow st \in S \end{cases}$. The ring $S^{-1}R = \{\frac{a}{s} \mid a \in R,\ s \in S\}$ is called the localisation of $R$ (away from $S$).

Consider $R$ as a UFD. We seek to establish that polynomial ring $R[x]$ is also a UFD. For instance, is $\mathbb{Z}[x]$ a UFD?

Main idea:
$$\begin{array}{ccc} R \text{ UFD} & \longrightarrow & Q \text{ field of fractions} \\ | & & \wr \\ R[x] \text{ PID} & \longleftrightarrow & Q[x] \text{ PID? } (\Rightarrow \text{UFD}). \end{array}$$

## 2.11 Polynomial rings over domains.

$\boxed{\text{Definition}}$ Let $R$ be a UFD, $Q$ is a field of fractions of $R$ (written $Q = Q(R)$), $f(x) \in R[x]$. We say that $f$ is primitive if $\gcd(a_0, \dots, a_n) = 1$. i.e. $\nexists p \in R$ prime s.t. $p \mid a_i\ \forall i = 0, \dots, n$.

Examples – • $f(x)$ is monic $\Rightarrow$ $f(x)$ is primitive • $3 + 4x + 2x^2 \in \mathbb{Z}[x]$ is primitive • $2 + 10x + 16x^2 + 4x^3$ is not primitive (in $\mathbb{Z}[x]$).

• $f(x)$ is irreducible $\Rightarrow$ $f(x)$ is primitive

$\boxed{\text{Lemma}}$ Let $R$ be a UFD, $Q = Q(R)$. Then $f(x) \in Q[x] \Rightarrow \exists \lambda \in Q$ and $\tilde{f} \in R[x]$ primitive such that $f = \lambda \cdot \tilde{f}$. Moreover, $\lambda, \tilde{f}$ are unique up to multiplication by units of $R$.

Notation: $\lambda = c(f)$ is called the content of $f$, $\tilde{f}$ is called the primitive part of $f$.

Proof – $f \in Q[x]$, $f = \frac{a_0}{b_0} + \frac{a_1}{b_1}x + \dots + \frac{a_n}{b_n}x^n$, $a_i, b_i \in R$. $b = b_0 \cdots b_n$, $a_i' = \frac{a_i b}{b_i} = b_0 \cdots b_{i-1} a_i b_{i+1} \cdots a_n \in R$. Let $d = \gcd(a_0', \dots, a_n')$, $c_i = \frac{a_i'}{d} \in R$. 31 October 2013. Dr. Javier LÓPEZ-PEÑA. Maths 500

Then $f = \underbrace{\frac{1}{b}}_{\in Q^*}(\underbrace{a_0' + a_1'x + \dots + a_n'x^n}_{\in R[x]}) = \frac{d}{b}(c_0 + c_1x + \dots + c_nx^n)$. $\gcd(c_0, \dots, c_n) = \gcd(\frac{a_0'}{d}, \dots, \frac{a_n'}{d}) = \frac{1}{d}\gcd(a_0', \dots, a_n') = \frac{d}{d} = 1$.

$\Rightarrow c_0 + c_1x + \dots + c_nx^n$ is primitive. Assume $f = \lambda\tilde{f} = \mu\tilde{g}$ $\lambda, \mu \in Q^*$. $\tilde{f}, \tilde{g} \in R[x]$ primitive. $\tilde{f} = a_0 + \dots + a_nx^n$, $\tilde{g} = b_0 + \dots + b_nx^n$, $\lambda = \frac{a}{b}$, $\mu = \frac{c}{d}$.

$\frac{a}{b}(a_0 + \dots + a_nx^n) = \frac{c}{d}(b_0 + \dots + b_nx^n) \Rightarrow ad\,a_0 + ad\,a_1x + \dots + ad\,a_nx^n = bc\,b_0 + \dots + bc\,b_nx^n \Rightarrow \begin{cases} ad\,a_0 = bc\,b_0 \\ \vdots \\ ad\,a_n = bc\,b_n \end{cases}$ $ad\,a_i = bc\,b_i\ \forall i = 0, \dots, n$.

Primitive $\Rightarrow \gcd(a_0, \dots, a_n) = 1$, $\gcd(b_0, \dots, b_n) = 1$. $ad = ad \cdot 1 = ad \cdot \gcd(a_0, \dots, a_n) = \gcd(ad\,a_0, \dots, ad\,a_n) = \gcd(bc\,b_0, \dots, bc\,b_n) = bc \cdot \gcd(b_0, \dots, b_n) = bc \cdot 1 = bc$.

[$ad = bc \Leftrightarrow \frac{a}{b} = \frac{c}{d}$, gcd defined up to a unit] $ad \sim bc$ (in $R$) $\Rightarrow \exists u \in U(R)$ s.t. $bc = uad \Rightarrow \frac{c}{d} = u \cdot \frac{a}{b}$, $\mu = u\lambda$. $\frac{a}{b}a_i = \frac{c}{d}b_i \Rightarrow \lambda a_i = \mu b_i = u\lambda b_i \Rightarrow a_i = ub_i\ \forall i = 0, \dots, n$

$\Rightarrow \tilde{f} = u\tilde{g} \Rightarrow \tilde{g} = u^{-1}\tilde{f}$ // q.e.d.

$\boxed{\text{Proposition}}$ Consider $f \in Q[x]$. Then the following properties apply:

(i) $\lambda \in Q^* \Rightarrow c(\lambda f) = \lambda \cdot c(f)$, $\widetilde{(\lambda f)} = \tilde{f}$ (ii) $f \in R[x] \Leftrightarrow c(f) \in R$ (iii) $f$ primitive $\Leftrightarrow c(f) = 1$ (up to units of $R$).

(iv) $f, g$ primitive and $f \sim g$ in $Q[x] \Leftrightarrow f \sim g$ in $R[x]$.

Proof – (i) $\lambda f = \lambda \cdot (c(f) \cdot \tilde{f}) = \underbrace{\lambda c(f)}_{\in Q^*} \cdot \underbrace{\tilde{f}}_{\in R[x] \text{ primitive}}$. $c(\lambda f)\widetilde{(\lambda f)} = \lambda f \Rightarrow c(\lambda f) = \lambda \cdot c(f)$, $\widetilde{(\lambda f)} = \tilde{f}$ up to units of $R$ // q.e.d.

(ii) $\left.\begin{array}{l} c(f) \in R \\ \tilde{f} \in R[x] \end{array}\right\}$ $c(f) \cdot \tilde{f} \in R[x] \Rightarrow f \in R[x]$. $f = a_0 + \dots + a_nx^n$ $a_i \in R$, $d = \gcd(a_0, \dots, a_n)$ primitive $\gcd(\frac{a_0}{d}, \dots, \frac{a_n}{d}) = 1 \Rightarrow f = d \cdot (\underbrace{\frac{a_0}{d}}_{\in R} + \dots + \underbrace{\frac{a_n}{d}}_{\in R}x^n) = c(f) \cdot \tilde{f} \Rightarrow c(f) = d \in R$ // q.e.d.

(iii) Same proof – $1 = \gcd(a_0, \dots, a_n) \Rightarrow f = 1 \cdot f = c(f) \cdot \tilde{f} \Rightarrow c(f) = 1$ // q.e.d.

(iv) $f, g$ primitive $\Rightarrow c(f) = c(g) = 1$. Assume $f \sim g$ in $Q[x] \Rightarrow \exists \lambda \in U(Q[x])$ ($U(Q) = Q^*$) s.t. $g = \lambda f$. $g = \tilde{g}$. $c(g) = 1 = c(\lambda f) = \lambda \cdot c(f) = \lambda$.

$\Rightarrow \lambda = 1$ up to units of $R$, i.e. $\lambda \in U(R)$. $g = \lambda f \Rightarrow g \sim f$ in $R[x]$ // q.e.d.

$\boxed{\text{Theorem}}$ (Gauss's Lemma)

Let $R$ be a UFD, $Q = Q(R)$. Then $f, g \in R[x]^*$ is primitive $\Rightarrow fg$ is primitive.

Proof – Same as last year (see MATH7202).

$\boxed{\text{Proposition}}$ $f, g \in Q[x]^* \Rightarrow \begin{cases} c(fg) = c(f)c(g) \\ \widetilde{fg} = \tilde{f} \cdot \tilde{g}. \end{cases}$

Proof – $fg = c(f) \cdot \tilde{f}\, c(g)\, \tilde{g} = c(f)c(g) \cdot \underbrace{\tilde{f} \cdot \tilde{g}}_{\text{primitive}} = c(fg) \cdot \widetilde{fg} \Rightarrow c(fg) = c(f)c(g)$, $\widetilde{fg} = \tilde{f} \cdot \tilde{g}$ // q.e.d.

**Proposition** Let $f \in R[x]^*$. (i) If $\deg f = 0$, $f$ irreducible in $R[x] \Leftrightarrow f$ irreducible in $R$. (b) If $\deg f \geq 1$, $f$ irreducible in $R[x] \Leftrightarrow \begin{cases} f \text{ is primitive, and} \\ f \text{ is irreducible in } Q[x]. \end{cases}$

Proof – (i) Assume $f = gh$ in $R[x]$. $\deg f = 0 \Rightarrow \deg g = \deg h = 0 \Rightarrow g, h \in R \Rightarrow f = gh$ in $R$ // q.e.d.

(ii) $f$ irreducible in $R[x] \Rightarrow f$ is primitive. Let $f = gh$ in $Q[x]$. $\left.\begin{array}{l} c(f)\cdot\tilde{f} = c(gh)\cdot(\widetilde{gh}) \\ 1\cdot\tilde{f} = c(g)c(h)\cdot\tilde{g}\cdot\tilde{h} \end{array}\right\} \Rightarrow \tilde{f} = \widetilde{gh}$ in $R[x]$, which contradicts irreducibility of $f$ in $R[x]$ // q.e.d.

12 November 2013.
Dr. Javier LÓPEZ-PEÑA
Maths 500.

**Theorem** $R$ is a UFD $\Rightarrow R[x]$ is a UFD.

Proof – Take $f \in R[x]$ non-zero, non-unit. If $\deg f = 0 \Rightarrow f \in R$ because $f$ is constant. $R$ is a UFD $\Rightarrow \exists$ irreducible (in $R$) $p_1, \dots, p_s \in R$ s.t. $f = p_1 \cdots p_s$.
$\Rightarrow$ each $p_i$ is irreducible in $R \Rightarrow p_i$ is irreducible in $R[x]$ by proposition ~~q.e.d~~. Then consider $\deg f \geq 1$, we look at $f$ as an element of $Q[x]$ $\because R \leq Q$, $R[x] \leq Q[x]$.
$Q$ is a field $\Rightarrow Q[x]$ is a PID. $\Rightarrow$ In particular, $Q[x]$ is a UFD. So $\exists f_1, \dots, f_s \in Q[x]$ irreducible (in $Q[x]$) s.t. $f = f_1 \cdots f_s$. For each $i$, we write $f_i = c(f_i)\cdot\tilde{f}_i$
$\tilde{f}_i \in R[x]$, $\tilde{f}_i$ are primitive. $c(f_i) \in Q^* = \mathcal{U}(Q[x])$. Then since $c(f_i)$ is a unit in $Q[x]$, $\left.\begin{array}{l} f_i \sim \tilde{f}_i \text{ in } Q[x], \ f_i \text{ irreducible in } Q[x] \end{array}\right\} \Rightarrow \tilde{f}_i$ irreducible in $Q[x]$.
Since $\tilde{f}_i$ is also primitive, each $f_i$ is irreducible in $R[x] \Rightarrow$ factorisations exist $\forall f \in R[x]$ as $f = f_1 \cdots f_s = \overbrace{c(f_1)c(f_2)\cdots c(f_s)}^{\in Q} \cdot \underbrace{\tilde{f}_1 \cdots \tilde{f}_s}_{\text{primitive, by Gauss's lemma}}$. Such a decomposition is unique, thus $c(f) = c(f_1)\cdots c(f_s)$ and $\tilde{f} = \tilde{f}_1 \cdots \tilde{f}_s \Rightarrow$ we know $c(f) \in R$ because $f \in R[x]$, so $c = c(f_1)\cdots c(f_s) \in R$. $c \in R \Rightarrow c = p_1 \cdots p_k$ for some $p_i \in R$ irreducible as $R$ is a UFD $\Rightarrow p_i$ are irreducibles in $R[x] \Rightarrow f = p_1 \cdots p_k \tilde{f}_1 \cdots \tilde{f}_s$ is a factorisation into irreducibles in $R[x]$. This proves existence, now it remains to prove uniqueness.
Assume $f = \overbrace{p_1 \cdots p_k}^{\in R} \overbrace{f_1 \cdots f_s}^{\in R[x]}$, $\deg(f_i) \geq 1$. $= \overbrace{q_1 \cdots q_{k'}}^{\in R} \overbrace{g_1 \cdots g_{s'}}^{\in R[x]}$, $\deg(g_j) \geq 1$. Here, assume $p_i, q_i, f_j, g_j$ are irreducible $\forall i, j$. $f_i$ irreducible $\Rightarrow f_i$ primitive
$\Rightarrow f_1 \cdots f_s$ is primitive. Likewise $g_1 \cdots g_s$ is primitive. However, decompositions to content/primitives are unique up to units, so up to units, we get that:
$\begin{cases} p_1 \cdots p_k = q_1 \cdots q_{k'} & \text{for content} \\ f_1 \cdots f_s = g_1 \cdots g_{s'} & \text{for primitives.} \end{cases}$ $p_1 \cdots p_k = q_1 \cdots q_{k'} \in R$ which is a UFD, so $\Rightarrow k = k'$ and $p_i \sim q_i$ in $R$ (after reordering). Then we have
$f_1 \cdots f_s = g_1 \cdots g_{s'}$ in $R[x] \Rightarrow$ equality holds in $Q[x]$. Each $\{f_i$ is irreducible in $R[x] \Rightarrow$ primitive$\}$ $f_i$ is irreducible in $Q[x]$. Similarly, $g_i$ irreducible in $Q[x]$.
$\Rightarrow$ since $Q[x]$ is a UFD, $s = s'$, $f_i \sim g_i$ in $Q[x]$ (after reordering). Using proposition, $\left.\begin{array}{l} f_i \sim g_i \text{ in } Q[x] \\ f_i, g_i \text{ primitive} \end{array}\right\} f_i \sim g_i$ in $R[x] \Rightarrow R[x]$ is a UFD // q.e.d.

# Chapter 3
# MODULES.

**Definition** Let $R$ be a commutative ring with 1. A <u>module over $R$</u> (or $R$-module) is an abelian group $(M, +)$ together with a map $R \times M \to M$. $(r, m) \to r\cdot m$. satisfying the following properties:

M1. $\underbrace{(r+s)}_{\text{addition in ring}} m = r\cdot m \underbrace{+}_{\text{addition in module}} s\cdot m$

M2. $r(m+n) = rm + rn$ — both here are additions in module. [Distributivity].

M3. $\underbrace{(rs)}_{\text{product in ring}} m = r(sm)$ — products in module. [pseudoassociativity]

M4. $1\cdot m = m$ [modularity].

The map $R \times M \to M$ is called the <u>module action</u> of $R$ on $M$.

Examples –

1. $R = \mathbb{F}$ field. Then $\mathbb{F}$-modules $\equiv$ vector spaces over $\mathbb{F}$.
2. $R = \mathbb{Z}$, take $(G, +)$ an abelian group. Define $\begin{array}{l} \mathbb{Z} \times G \to G \\ (n, g) \mapsto n\cdot g \end{array}$ defined $:= \begin{cases} \overbrace{g + \dots + g}^{n \text{ times}} & \text{if } n > 0 \\ 0_G & \text{if } n = 0_{\mathbb{Z}} \\ \underbrace{(-g) + \dots + (-g)}_{-n \text{ times}} & \text{if } n < 0. \end{cases}$
With this action, $(G, +)$ becomes a $\mathbb{Z}$-module. $\Rightarrow \mathbb{Z}$-modules $\equiv$ abelian groups.
3. Let $R$ be a ring. $M = R$. $R \times \overset{R}{\overset{\shortparallel}{M}} \to \overset{R}{\overset{\shortparallel}{M}}$ $(r, m) \mapsto r\cdot m$ is taken to be the usual product of $R$. $\Rightarrow$ With this action, $R$ is a module over itself. This is the <u>left regular action</u> of $R$ on itself, which we denote as ${}_R R$. [Notation: we write ${}_R M$ to say $M$ is an $R$-module].
4. $\varphi: R \to S$ is a ring homomorphism and let ${}_S M$ be an $S$-module. Define $\begin{array}{l} R \times M \to M \\ (r, m) \mapsto \varphi(r) m \end{array}$. With this action, $M$ is also an $R$-module. In particular, if $R \leq S$ is a subring, we can restrict $M$ ($S$-module) to being a module over the subring $R$ if $\varphi$ is the inclusion homomorphism.
5. Modules over $\mathbb{F}[x]$. We know $\mathbb{F} \leq \mathbb{F}[x]$, so every $\mathbb{F}[x]$-module is also an $\mathbb{F}$-module $\Rightarrow \mathbb{F}[x]$-module is a vector space. Take vector space $V$ over $\mathbb{F}$, and assume we have a modular structure $\begin{array}{l} \mathbb{F}[x] \times V \to V \\ (f, v) \to f\cdot v \end{array}$. If $f = a_0 + a_1 x + \dots + a_n x^n$, then we have $(a_0 + a_1 x + \dots + a_n x^n)\cdot v = a_0\cdot v + (a_1 x)\cdot v + \dots + (a_n x^n)\cdot v$ by M1.
So we only need to know $(a_k x^k)\cdot v = a_k\cdot(x^k v)$ by pseudoassociativity $= a_k \cdot \big(\overbrace{x(x(\cdots (xv))\cdots)}^{k \text{ times}}\big)$ i.e. we have reasoned that the module structure is uniquely determined by the product $\overset{\alpha}{\widetilde{x\cdot v}}$. Define $\alpha: V \to V$, $v \mapsto x\cdot v$. Then $\left.\begin{array}{l} \alpha(v_1 + v_2) = x\cdot(v_1 + v_2) = xv_1 + xv_2 = \alpha(v_1) + \alpha(v_2) \\ \alpha(\lambda v) = x(\lambda v) = (x\lambda)\cdot v = (\lambda x)\cdot v = \lambda(xv) = \lambda\alpha(v) \end{array}\right\}$ $\alpha$ is a linear map that determines action.
So if $V$ is an $\mathbb{F}[x]$-module, then $\exists$ linear map $\alpha: V \to V$ that determines module action. i.e. $\mathbb{F}[x]$-module $\rightsquigarrow (V, \alpha)$ $\begin{array}{l} V \text{ is a v.s.} \\ \alpha: V \to V \text{ is a linear endomorphism.} \end{array}$
Conversely, if $V$ is a vector space, $\alpha: V \to V$ is a linear map, define $\begin{array}{l} \mathbb{F}[x] \times V \to V \\ (a_0 + \dots + a_n x^n, v) \mapsto (a_0 + \dots + a_n x^n)\cdot v = a_0\cdot v + a_1\alpha(v) + a_2\cdot\alpha^2(v) + \dots + a_n\alpha^n(v) = [f(\alpha)](v). \end{array}$
This is a module action that gives an $\mathbb{F}[x]$-module structure on $V$ (determined by $\alpha$). Then $\boxed{\mathbb{F}[x]\text{-mod} \equiv (V, \alpha) \ \begin{array}{l} V \text{ is a v.s. over } \mathbb{F} \\ \alpha: V \to V \text{ endomorphism} \end{array}}$
6. $R$ ring, $M$ is an $R$-module with action $r\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} = \begin{pmatrix} ra_{11} & \cdots & ra_{1n} \\ \vdots & & \vdots \\ ra_{n1} & \cdots & ra_{nn} \end{pmatrix}$.

**Definition** Let $M$ be an $R$-module, a <u>submodule of $M$</u> is a subgroup $P \leq (M, +)$ s.t. $\forall r \in R$, $\forall m \in P$, $r\cdot m \in P$. [equivalently, $P$ is a submodule if $\forall r, s \in R$, $\forall m, n \in P$, $rm + sn \in P$.]

Examples –

1. $R = \mathbb{F}$ is a field, $M = V$ vector spaces over $\mathbb{F}$. Submodules of $M \equiv$ subspaces of $V$
2. $R = \mathbb{Z}$, $M = G$ abelian group. Submodules of $M$ = subgroups of $G$.

This illustrates that modules are just a further level of abstraction and generality. However, we lose specificity to unique contexts (e.g. we cannot perform row reduction).

3. $M = {}_R R$. Then submodules of $M \equiv$ ideals of $R$.
4. Let $M$ be an $R$-module. Then $\overset{\{0\}}{\overset{\shortparallel}{0}} \leq M$ is a submodule, [trivial submodule] and $M \leq M$ is a submodule. [total submodule]

5. $R=\mathbb{F}[x]$, $M$ is a $R$-module, then $M=(V,\alpha)\begin{cases}V \text{ v.s.}\\ \alpha: V\to V \text{ endomorphism}\end{cases}$. Let $P\leq M$ be a submodule. $\Rightarrow P\leq (M,+)$ is a subgroup.

Take $\lambda\in\mathbb{F}$, $v\in P$. Then $\lambda\cdot v\in P$ for all arbitrary $\lambda$ [equivalently, $\lambda,\mu\in\mathbb{F}$, $\forall u,v\in P$, then $\lambda u+\mu v\in P$]. $\Rightarrow$ $P$ is closed under linear combinations

$\Rightarrow$ $P$ is a subspace of $V$. $\forall v\in P$, $x\cdot v\in P$. $\Rightarrow \alpha(v)\in P$, thus $\alpha: P\to P$ and $\alpha(P)\subseteq P$ $\Rightarrow$ $P$ is an $\alpha$-invariant subspace.

Converse is also true, giving us a correspondence: $\{\text{submodules of } M\}\equiv\{\alpha\text{-invariant subspaces of } V\}$.

14 November 2013
Dr. Javier LÓPEZ-PEÑA
Maths 500.

**Proposition** Let $R$ be a ring, $M$ an $R$-module. If $A,B\leq M$ are submodules, then

- $A\cap B\leq M$ is a submodule [actually if $\{P_\alpha\}$ are submodules, then $\bigcap_\alpha P_\alpha\leq M$.]
- $A+B=\{a+b\mid a\in A, b\in B\}\leq M$.

Proof – Omitted. Left as an exercise.

## 3.2 Cyclic modules and finitely generated modules.

If $R$ is a ring, $M$ an $R$-module, and $x\in M$. Then we can construct a submodule $Rx=\{rx\mid r\in R\}\leq M$.

**Definition** If $\exists x\in M$ s.t. $M=Rx$, we say that $M$ is a cyclic module (generated by $x$). If $\exists\, x_1,\dots,x_n$ s.t. $M=Rx_1+\dots+Rx_n$, we say that $M$ is finitely generated and $\{x_1,\dots,x_n\}$ is a generating set of $M$.

Remark – $Rx_1+\dots+Rx_n=\{r_1x_1+\dots+r_nx_n\mid r_i\in R\}$ (set of linear combinations of generating set.

Examples –

1. $0=R\cdot 0$ is cyclic   2. ${}_RR=R\cdot 1$ is cyclic, generated by 1.   3. If $R=\mathbb{Z}$, $M=G$ are abelian groups. Cyclic submodules of $M\equiv$ cyclic subgroups of $G$.

4. If $R=\mathbb{F}$, $M=V$ are vector spaces. Cyclic submodules of $V\equiv$ 1-dimensional subspaces.

**Definition** $R$ ring, $M$ $R$-module, $P\leq M$ submodule. $M/P=\{\bar m\mid m\in M\}$, where $\bar m=m+P=\{m+p\mid p\in P\}$.

Note – Recall that $\bar m=\bar n\Leftrightarrow m-n\in P$, so we can define $\begin{array}{l}R\times M/P\longrightarrow M/P\\ (r,\bar m)\longmapsto r\bar m:=\overline{rm}\end{array}$. We check that this is well-defined: $\bar m=\bar n\Rightarrow m-n\in P\overset{P\text{ submodule}}{\Rightarrow} r(m-n)\in P\Rightarrow rm-rn\in P$

$\Rightarrow\overline{rm}=\overline{rn}$, so the action of $R$ on $M/P$ is well-defined. Also, $M/P$ is itself an $R$-module.

**Proposition** If $M=Rx_1+\dots+Rx_n$ is finitely generated over $R$, $P\leq M$, then $M/P$ is also finitely generated and moreover, it is generated by $\{\bar x_1,\dots,\bar x_n\}$.

Proof – Take $\bar m\in M/P$, $m\in M\Rightarrow\exists\, r_i\in R$ s.t. $m=r_1x_1+\dots+r_nx_n\Rightarrow\bar m=\overline{r_1x_1+\dots+r_nx_n}=\overline{r_1x_1}+\dots+\overline{r_nx_n}=\sum_{i=1}^n r_i\bar x_i\Rightarrow\bar m$ is a linear combination of $\{\bar x_1,\dots,\bar x_n\}$, q.e.d.

**Corollary** If $M$ is cyclic, $P\leq M\Rightarrow M/P$ is cyclic. In particular, $\forall R$ rings, $I\trianglelefteq R$, ${}_RR/I$ is cyclic, generated by $\bar 1=1+I$.

Remark – In general, it is not true that a submodule of a cyclic module must be cyclic e.g. Take $M={}_RR$ for $R$ not a PID.

## 3.3 Module Homomorphisms.

**Definition** $R$ ring, $M,N$ be $R$-modules. $\alpha: M\to N$, then $\alpha$ is an $R$-module homomorphism (or $R$-linear map) if 1. $\alpha(0)=0$, $\alpha(m+n)=\alpha(m)+\alpha(n)$ $\forall m,n\in M$ 2. $\alpha(rm)=r\cdot\alpha(m)$ $\forall r\in R$ $\forall m\in M$.

[or, combining them, $\forall r,s\in R$ $\forall m,n\in M$, $\alpha(rm+sn)=r\alpha(m)+s\alpha(n)$.].

Examples –

1. $\forall R$ rings, $\forall M,N$ $R$-modules, $\begin{array}{l}0: M\longrightarrow N\\ m\mapsto 0\end{array}$ is the zero homomorphism   Implication – there are always maps between modules, even if they do not exist for rings.

2. $M$ is an $R$-module, $\begin{array}{l}\mathrm{id}: M\to M\\ m\mapsto m\end{array}$ is the identity homomorphism. If $P\leq M$ is a submodule, $\begin{array}{l}i: P\to M\\ p\mapsto p\end{array}$ is the inclusion homomorphism.

3. $M$ is an $R$-module, $P\leq M$. $\begin{array}{l}\pi_P: M\to M/P\\ m\mapsto\bar m\end{array}$ (canonical projection) is a module homomorphism.

4. $R=\mathbb{F}$, $M,N$ are vector spaces $V,W$. $\alpha: V\to W$ is a module homomorphism $\Leftrightarrow$ $\alpha$ is a linear map.   5. $R=\mathbb{Z}$, $M,N=$ abelian groups $G,H$. $\alpha: G\to H$ is a mod. hom $\Leftrightarrow$ $\alpha$ is a group hom

Notation – Let $R$ be a ring, $M,N$ $R$-modules. Then $\mathrm{Hom}_R(M,N)=\{\alpha: M\to N\mid\alpha\text{ is a module homomorphism}\}$. Then $\mathrm{Hom}_R(M,M)$ is also an $R$-module.

If $\alpha: M\to N$ is injective it is a monomorphism, if it is surjective it is an epimorphism, if it is bijective it is an isomorphism.

19 November 2013.
Dr. Javier LÓPEZ-PEÑA
Maths 500.

**Definition** Let $\alpha: M\to N$ be a module homomorphism, then $\mathrm{Ker}\,\alpha=\{m\in M\mid\alpha(m)=0\}$, $\mathrm{Im}\,\alpha=\{\alpha(m)\mid m\in M\}$.

Properties – $\cdot\,\mathrm{Ker}\,\alpha\leq M$   $\cdot\,\mathrm{Im}\,\alpha\leq M$   $\cdot\,\alpha$ injective $\Leftrightarrow$ $\mathrm{Ker}\,\alpha=0$   $\cdot\,\alpha$ surjective $\Leftrightarrow$ $\mathrm{Im}\,\alpha=N$.

**Theorem** (1st Isomorphism Theorem for modules).

Let $R$ be a ring, $M,N$ $R$-modules, $\alpha: M\to N$ a module homomorphism. $\Rightarrow\dfrac{M}{\mathrm{Ker}\,\alpha}\cong\mathrm{Im}\,\alpha$.

Proof – $\psi:\dfrac{M}{\mathrm{Ker}\,\alpha}\to\mathrm{Im}\,\alpha$, $m+\mathrm{Ker}\,\alpha\mapsto\psi(m+\mathrm{Ker}\,\alpha)=\alpha(m)$. Need to check: $\psi$ is well-defined and injective: $m+\mathrm{Ker}\,\alpha=n+\mathrm{Ker}\,\alpha$, $m-n\in\mathrm{Ker}\,\alpha\Leftrightarrow\alpha(m-n)=0\Leftrightarrow\alpha(m)=\alpha(n)$

$\psi$ is surjective: take $y\in\mathrm{Im}\,\alpha$, $\exists\, m\in M$ s.t. $y=\alpha(m)=\psi(m+\mathrm{Ker}\,\alpha)\Rightarrow y\in\mathrm{Im}\,\psi$, surjective. $\psi$ is a mod homomorphism: $\psi(r\bar m+s\bar n)=$

$= \psi(\overline{rm}+\overline{sn}) = \psi(\overline{rm+sn}) = \alpha(rm+sn) = r\alpha(m)+s\alpha(n) = r\psi(\overline{m})+s\psi(\overline{n})$ // q.e.d.

**Theorem** (classification of cyclic modules) — applies specifically for commutative rings.

Let $R$ be a ring (commutative, with 1). Let $M$ be an $R$-module, $\boxed{M \text{ cyclic} \Leftrightarrow \exists I \trianglelefteq R \text{ s.t. } M \cong \frac{R}{I}}$. Moreover, the ideal $I$ is unique.

Proof – ($\Leftarrow$) $\left.\begin{array}{l} {}_RR = R\cdot 1 \text{ cyclic}, \\ I \trianglelefteq R \text{ ideal} \end{array}\right\} \Rightarrow R/I$ cyclic (as every quotient is finitely generated by 1 since ${}_RR$ cyclic.) // q.e.d.

($\Rightarrow$) Let $M$ be a cyclic module. Then $\exists x \in M$ s.t. $M = Rx$. Define a map $\alpha: {}_RR \to R\cdot x = M$, $r \mapsto r\cdot x$. $\alpha(r+s) = (r+s)x = rx+sx = \alpha(r)+\alpha(s)$

$\alpha(rs) = (rs)x \overset{\text{pseudoassoc.}}{=} r(sx) = r\cdot\alpha(s) \Rightarrow \alpha$ is a module homomorphism. (note – NOT a ring homomorphism!) By First Isomorphism Theorem,

$\frac{R}{\operatorname{Ker}\alpha} \cong \operatorname{Im}\alpha$. $\forall m \in M$, $\exists r \in R$ s.t. $m = rx. \Rightarrow m = \alpha(r) \Rightarrow \operatorname{Im}\alpha = M. \Rightarrow M \cong \frac{R}{I}$ where $I = \operatorname{Ker}\alpha$. We know that $\operatorname{Ker}\alpha$ is an ideal as it is a submodule of ${}_RR$, thus, $I = \operatorname{Ker}\alpha \trianglelefteq R$ ideal. // q.e.d.

(uniqueness). Assume $\frac{R}{I} \cong \frac{R}{J}$ (as $R$-modules). $\Rightarrow \exists\ \beta: \frac{R}{I} \to \frac{R}{J}$ $R$-module isomorphism. $\Rightarrow \beta$ is surjective $\Rightarrow \exists r+I \in \frac{R}{I}$ s.t. $\beta(r+I) = \underbrace{1+J}_{\text{unit in } \frac{R}{J}}$.

$\forall i \in I$, $ir \in I$ by absorbency, $ir+I = 0+I$. Then $\beta(ir+I) = \beta(0+I) = 0+J$. On the other hand, $\beta(ir+I) = \beta(i(r+I)) = i\,\beta(r+I) = i(1+J) = i+J$.

Then $0+J = i+J \Rightarrow i \in J$. Since $\forall i \in I$, $i \in J$, $I \subseteq J$. Apply the same reasoning to the inverse isomorphism $\beta^{-1}: \frac{R}{J} \to \frac{R}{I}$, then $J \subseteq I$. Thus $I = J$ // q.e.d.

**Definition** Let $R$ be a ring, $M$ $R$-module, $X \subseteq M$ subset. We define the <u>annihilator</u> of $X$, $\operatorname{ann}(X) = \{r \in R \mid r\cdot x = 0\ \forall x \in X\}$.

Remark – If $M$ cyclic, $M = \frac{R}{I}$. $\Rightarrow I = \operatorname{ann}(X)$ where $M = Rx$.

**Proposition** $\operatorname{ann}(X) = \bigcap_{x \in X} \operatorname{ann}(x)$, in particular $\operatorname{ann}(X) \trianglelefteq R$ ideal.

**Theorem** (2nd Isomorphism Theorem).

Let $R$ be a ring, $M$ $R$-mod, $A, B \leq M$ submodules $\Rightarrow \frac{A+B}{A} \cong \frac{B}{A \cap B}$.

**Theorem** (3rd Isomorphism Theorem).

Let $M$ be a $R$-module, $P \leq M$ submodule, $Q \leq M$ submodule s.t. $P \subseteq Q \Rightarrow \frac{M/P}{Q/P} \cong \frac{M}{Q}$.

**Theorem** (Correspondence Theorem).

$\left\{\begin{array}{c}\text{submodules} \\ \text{of } M/P\end{array}\right\} \overset{1:1}{\longleftrightarrow} \left\{\begin{array}{c}\text{submodules of } Q \leq M \\ \text{s.t. } P \subseteq Q\end{array}\right\}$.

Proofs – all omitted; easily analogous to proofs for rings. Moreover, all are simple consequences of the 1st isomorphism theorem.

## 3.4 Direct sums of modules.

**Definition** Let $R$ be a ring, $M_1, \dots, M_n$ $R$-modules. Define $M = \{(m_1, \dots, m_n) \mid m_i \in M_i\}$. with operations $(m_1, \dots, m_n) + (m_1', \dots, m_n') = (m_1+m_1', \dots, m_n+m_n')$, $0 = (0_{M_1}, \dots, 0_{M_n})$,

$r\cdot(m_1, \dots, m_n) = (rm_1, \dots, rm_n)$. With these operations, $M$ is an $R$-module, called the <u>(external) direct sum</u> $M_1 \oplus \dots \oplus M_n$.

Define $M_i' = \{(0, \dots, 0, m_i, 0, \dots, 0) \mid m_i \in M_i\} \leq M$ submodule. Then $M_i \cong M_i'$, so we can identify $M_i$ with $M_i'$ and therefore think of $M_i$ as a submodule of $M$.

Question: Let $M$ be an $R$-module, $A, B \leq M$ submodules. What conditions do we need to guarantee that $A \oplus B \cong M$?

If $M_1, \dots, M_n \leq M$ and $M_1 \oplus \dots \oplus M_n \cong M$, we say that $M$ is the <u>internal direct sum</u> of $M_1, \dots, M_n$.

Aside: Why linear independence does not work for modules: consider $R = \mathbb{Z}$. Then if $M$ is a $\mathbb{Z}$-module, if linear independence *did* work, then for $m_1, \dots, m_n \in M$, $\sum \underset{\in \mathbb{Z}}{\lambda_i} m_i = 0 \Rightarrow \lambda_i = 0$

Problem – consider $M = \mathbb{Z}_{30}$ (abelian group). $m = \overline{5}$, then $\{m\}$ is not "LI" because $6\cdot\overline{5} = \overline{0}$ and $6 \neq 0$. Moreover, $\underset{\in \mathbb{Z}}{30}\cdot m = \overline{0}$ $\forall m \in M$.

**Definition** Let $R$ be a ring, $M$ an $R$-module, $M_1, \dots, M_n \leq M$ submodules. We say that $\{M_i\}_{i=1}^n$ is an <u>independent set of submodules</u> if whenever we have $m_1 + \dots + m_n = 0$ with $m_i \in M_i$, then each $m_i = 0$.

If $M = M_1 \oplus \dots \oplus M_n$. Identify $M_i \cong M_i' = \{(0, 0, \dots, 0, m_i, 0, \dots, 0) \mid m_i \in M_i\}$. Suppose $m_1 \in M_1, \dots, m_n \in M_n$. Then $m_1 + \dots + m_n = (m_1, m_2, \dots, m_n)$ when identified with $M_i'$.

Then if $m_1 + \dots + m_n = 0$, $(m_1, \dots, m_n) = 0 \Rightarrow m_i = 0\ \forall i. \Rightarrow \{M_i\}$ is an independent set of modules.

**Proposition** Let $M$ be an $R$-module, $M_1, \dots, M_n \leq M$ are submodules, the following are equivalent.

(1) $\{M_i\}$ independent set of submodules. (2) $\forall m \in M_1 + \dots + M_n$ $\exists$ unique $m_i \in M_i$ s.t. $m = m_1 + \dots + m_n$

(3) $\forall i = 1, \dots, n$, $M_i \cap \hat{M} = \{0\}$ where $\hat{M}_i = M_1 + \dots + M_{i-1} + M_{i+1} + \dots + M_n$.

Proof – (1)$\Rightarrow$(2): Take $m \in M_1 + \dots + M_n$, assume $m = m_1 + \dots + m_n = m_1' + \dots + m_n' \Rightarrow \underset{\in M_1}{(m_1 - m_1')} + \underset{\in M_2}{(m_2 - m_2')} + \dots + \underset{\in M_n}{(m_n - m_n')} = 0$. Since $\{M_i\}$ form an independent set of submodules, $m_i - m_i' = 0\ \forall i = 1, \dots, n \Rightarrow m_i = m_i'\ \forall i \Rightarrow$ composition is unique.

(2)$\Rightarrow$(3): Take $m \in M_i \cap \hat{M}_i$, where $\hat{M}_i = M_1 + \dots + M_{i-1} + M_{i+1} + \dots + M_n$. Then $m \in \hat{M}_i \Rightarrow \exists m_1, m_2, \dots, m_{i-1}, m_{i+1}, \dots, m_n$ s.t. $m = m_1 + \dots + m_{i-1} + m_{i+1} + \dots + m_n$

However also $m \in M_i \Rightarrow m = m_i \in M_i$. Then $m_i = m_1 + \dots + m_{i-1} + \underset{\in M_i}{0} + m_{i+1} + \dots + m_n \Rightarrow \underset{\in M_1}{0} + \dots + \underset{\in M_{i-1}}{0} + m_i + \underset{\in M_{i+1}}{0} + \dots + \underset{\in M_n}{0} = m_1 + \dots + m_{i-1} + 0 + m_{i+1} + \dots + m_n$

$\Rightarrow m_1 = m_2 = \dots = m_{i-1} = m_{i+1} = \dots = m_n = 0$, $m_i = 0 \Rightarrow m = 0 \Rightarrow M_i \cap \hat{M}_i = \{0\}$.

(3)$\Rightarrow$(1): Let $m_i \in M_i$ s.t. $m_1 + \dots + m_n = 0$. Then $\underset{\in M_i}{m_i} = -\underset{\in M_1}{m_1} - \underset{\in M_2}{m_2} - \dots - \underset{\in M_{i-1}}{m_{i-1}} - \underset{\in M_{i+1}}{m_{i+1}} - \dots - \underset{\in M_n}{m_n} \in M_1 + \dots + M_{i-1} + M_{i+1} + \dots + M_n = \hat{M}_i \Rightarrow \forall i$, $m_i \in M_i \cap \hat{M}_i \Rightarrow m_i = 0$

$\Rightarrow \{M_i\}$ is independent // q.e.d.

Example – Let $M$ be an $R$-module, $A, B \leq M$. $A, B$ independent $\Leftrightarrow A \cap B = 0$.

**Theorem** The following are equivalent:

(1) $M \cong M_1 \oplus \cdots \oplus M_n$ (2) $M = M_1 + \cdots + M_n$ and $\{M_i\}$ are an independent set of submodules.

Proof – (1) $\Rightarrow$ (2): We have already shown that $M = \oplus M_i \Rightarrow \{M_i\}$ is an independent set. $m \in M = \oplus M_i \Rightarrow m = (m_1, \dots, m_n)$. Then we have: 21 November 2013. Dr. Javier LÓPEZ-PEÑA. Maths 500.

$m = (m_1, 0, \dots, 0) + (0, m_2, 0, \dots, 0) \overset{+\cdots+}{+} (0, \dots, 0, m_n) = m_1 + m_2 + \cdots + m_n \Rightarrow M = \sum M_i$ // q.e.d.

(2) $\Rightarrow$ (1): $\forall m \in M$ $\exists$ unique $m_i \in M_i$ s.t. $m = m_1 + \cdots + m_n$, since $M = M_1 + \cdots + M_n$ and each $\{M_i\}$ is part of an independent set. Define $\alpha: M \to \bigoplus_{i=1}^{n} M_i$, by $m \mapsto \alpha(m) = (m_1, \dots, m_n)$. We check that $\alpha$ is a module homomorphism since $\alpha(rm + sn) = r\alpha(m) + s\alpha(n)$. $\alpha$ is surjective (trivial). Then we compute $\mathrm{Ker}(\alpha)$. Let $m \in \mathrm{Ker}(\alpha)$, $m = m_1 + \cdots + m_n$ for unique $m_i \in M_i$. $\alpha(m) = (0, \dots, 0) = (m_1, \dots, m_n) \Rightarrow m_i = 0 \Rightarrow m = 0 \Rightarrow \ker \alpha = 0 \Rightarrow \alpha$ is injective.

Thus, $\alpha$ is a module isomorphism $\Rightarrow M \cong \oplus M_i$ // q.e.d.

Example – Let $M$ be an $R$-module, $A, B \leq M$. Then $\boxed{M \cong A \oplus B \Leftrightarrow M = A + B \text{ and } A \cap B = 0.}$ In this case, $A$ and $B$ are called <u>direct summands</u> of $M$, and $B$ is called <u>a complement</u> of $A$ in $M$. (Complements of modules are not unique and not necessarily isomorphic to each other).

Remark – In modules, $A \oplus B \cong A \oplus C$ does not in general imply $B \cong C$.

If $M \cong A \oplus B$, $\frac{M}{A} \cong \frac{A+B}{A} \cong \frac{B}{A \cap B}$ (2nd isomorphism theorem) $\cong \frac{B}{0} \cong B$. Similarly, $\frac{M}{B} \cong A$.

Notation: If $M \cong M_1 \oplus M_2 \oplus \cdots \oplus M_n$ where $M_1 \cong M_2 \cong \cdots \cong M_n \cong N$; then we write $M = N^n$. In particular, we write $R^n \cong R \oplus R \oplus \cdots \oplus R$.

## 3.5 Quotients of Direct Sums.

**Lemma** Let $R$ be a ring, $M_1, \dots, M_t$, $N_1, \dots, N_t$ $R$-modules, $\alpha_i: M_i \to N_i$ a module homomorphism. Define $\alpha: \oplus M_i \longrightarrow \oplus N_i$, $(m_1, \dots, m_t) \to (\alpha_1(m_1), \alpha_2(m_2), \dots, \alpha_t(m_t))$.

Then $\alpha$ is a module homomorphism, and $\mathrm{Ker}(\alpha) \cong \bigoplus_{i=1}^{t} \mathrm{Ker}(\alpha_i)$, $\mathrm{Im}(\alpha) = \bigoplus_{i=1}^{t} \mathrm{Im}(\alpha_i)$.

Proof – Easy, left as an exercise.

**Corollary** Let $R$ be a ring, $M_1, \dots, M_t$ $R$-modules, $P_i \leq M_i$. Then $P_1 \oplus \cdots \oplus P_t \leq M_1 \oplus \cdots \oplus M_t$ and $\frac{M_1 \oplus \cdots \oplus M_t}{P_1 \oplus \cdots \oplus P_t} \cong \frac{M_1}{P_1} \oplus \cdots \oplus \frac{M_t}{P_t}$.

Proof – Use the First Isomorphism Theorem; map using canonical projections – $\pi_{P_i}: M_i \to M_i/P_i$, $m_i \mapsto m_i + P_i$. These are module homomorphisms $\forall i = 1, 2, \dots, t$. Then, by lemma, $\pi: \oplus M_i \to \oplus \frac{M_i}{P_i}$ is a module homomorphism, with $(m_1, \dots, m_t) \mapsto (m_1 + P_1, \dots, m_t + P_t)$. Then $\mathrm{Im}(\pi) = \bigoplus_{i=1}^{t} \mathrm{Im}\, \pi_{P_i} = \bigoplus_{i=1}^{t} \frac{M_i}{P_i}$ by surjectivity of canonical proj. Thus, $\pi$ is surjective. Then $\mathrm{Ker}(\pi) = \bigoplus_{i=1}^{t} \mathrm{Ker}(\pi_{P_i}) \cong \bigoplus_{i=1}^{t} P_i$. Then by 1st isomorphism theorem, $\frac{\oplus M_i}{\oplus P_i} \cong \oplus \frac{M_i}{P_i}$ // q.e.d.

**Lemma** Let $M, N$ be $R$-modules, $\alpha: M \to N$ an injective module homomorphism. Then $P \leq M$ submodule $\Rightarrow \frac{M}{P} \cong \frac{\alpha(M)}{\alpha(P)}$.

Proof – Consider $\bar{\alpha}: M \to \frac{\alpha(M)}{\alpha(P)}$, $m \mapsto \alpha(m) + \alpha(P)$. Note that $\bar{\alpha}: M \to \alpha(M) = \mathrm{Im}\,\alpha \xrightarrow{\pi_{\alpha(P)}} (\mathrm{Im}\,\alpha) \to \frac{\alpha(M)}{\alpha(P)}$. Thus, $\bar{\alpha} = \underset{\text{(hom)}}{\pi_{\alpha(P)}} \circ \underset{\text{(hom)}}{\alpha}$ is a module homomorphism.

$\ker \bar{\alpha} = \{m \in M \mid \bar{\alpha}(m) = 0\} = \{m \in M \mid \alpha(m) \in \alpha(P)\} \Rightarrow$ clearly, $P \subseteq \mathrm{Ker}\,\bar{\alpha}$. Moreover, $\alpha(m) \in \alpha(P) \Rightarrow \exists p \in P$ s.t. $\alpha(m) = \alpha(p)$. By injectivity of $\alpha$, $\alpha(m) = \alpha(p) \Rightarrow m = p \Rightarrow m \in P \Rightarrow \mathrm{Ker}\,\bar{\alpha} = P$. For surjectivity, let $y \in \frac{\alpha(M)}{\alpha(P)}$, then $y = \alpha(m) + \alpha(P)$ for some $m \in M \Rightarrow y = \bar{\alpha}(m) \Rightarrow y \in \mathrm{Im}\,\bar{\alpha} \Rightarrow \mathrm{Im}\,\bar{\alpha} = \frac{\alpha(M)}{\alpha(P)}$. By 1st isomorphism theorem, $\frac{M}{P} \cong \frac{\alpha(M)}{\alpha(P)}$ // q.e.d.

**Corollary** Let $R$ be a PID, $a, b \in R^* \Rightarrow \frac{Ra}{Rab} \cong \frac{R}{Rb}$. 26 November 2013. Dr. Javier LÓPEZ-PEÑA. Maths 500.

Proof – Take $\alpha: R \to Ra$, $r \mapsto \alpha(r) = r \cdot a$. Then $\alpha$ is injective because $R$ is an integral domain, $a \neq 0 \Rightarrow \mathrm{Ker}\,\alpha = \{0\}$. Then take $P = Rb \leq R$.

By the lemma, $\frac{R}{Rb} \cong \frac{\alpha(R)}{\alpha(Rb)} \cong \frac{Ra}{Rab}$ // q.e.d.

## 3.6 Free Modules.

**Definition** Let $R$ be a ring, $M$ a (finitely generated) $R$-module. We say that $M$ is <u>free</u> if $M \cong \overbrace{{}_R R \oplus \cdots \oplus {}_R R}^{n \text{ copies}} = R^n$.

**Definition** Let $M$ be an $R$-module, $e_1, \dots, e_n \in M$, we say that $\{e_1, \dots, e_n\}$ is a <u>basis</u> of $M$ if $\forall m \in M$, $\exists$ unique $r_1, \dots, r_n \in R$ st. $m = r_1 e_1 + \cdots + r_n e_n$.

**Proposition** Let $M$ be an $R$-module. Then the following are equivalent:

(1) $M$ is a free module (i.e. $M \cong R^n$) (2) $M$ has a basis.

Proof – (1) $\Rightarrow$ (2): $M = R^n = R \oplus \cdots \oplus R$. Let $e_i = (0, \dots, 0, \overset{i}{1}, 0, \dots, 0) \in M$. $\forall m \in M$, $m = (r_1, \dots, r_n) = r_1 e_1 + \cdots + r_n e_n$ and $r_i$ are unique. Thus $M$ has a basis // q.e.d.

(2) $\Rightarrow$ (1): Assume that we have a basis of $M \Rightarrow \forall m \in M$ $\exists$ unique $r_1, \dots, r_n \in R$ s.t. $m = r_1 e_1 + \cdots + r_n e_n$. Define map $\varphi: M \longrightarrow R^n$, $m = \sum r_i e_i \mapsto (r_1, \dots, r_n)$.

Suppose $m = \sum r_i e_i$, $m' = \sum s_i e_i$, then $m + m' = \sum (r_i + s_i) e_i$. Thus $\varphi(m + m') = (r_1 + s_1, \dots, r_n + s_n) = (r_1, \dots, r_n) + (s_1, \dots, s_n) = \varphi(m) + \varphi(m')$.

Similarly, $rm = r \sum r_i e_i = \sum r r_i e_i$. Then $\varphi(rm) = (rr_1, \dots, rr_n) = r(r_1, \dots, r_n) = r\varphi(m) \Rightarrow \varphi$ is a module homomorphism. $\mathrm{Ker}\,\varphi = \{\sum 0 e_i\} = \{0\}$ by uniqueness. $\Rightarrow \varphi$ is injective. $\mathrm{Im}\,\varphi = R^n \Rightarrow \varphi$ is surjective. Thus, $\varphi$ is an isomorphism $\Rightarrow M \cong R^n$ // q.e.d.

**Proposition** Let $F = R^n$ be a free $R$-module, $\{e_1, \dots, e_n\}$ be a basis. Let $M$ be an $R$-module, $m_1, \dots, m_n \in M$ be any elements of $M$. Then $\exists$ unique $\varphi: F \to M$ module homomorphism s.t. $\varphi(e_i) = m_i$.

Proof – Assume $\varphi: F \to M$ is a module homomorphism s.t. $\varphi(e_i) = m_i$. Then $\forall x \in F$, $\exists$ unique $r_1, \dots, r_n \in R$ s.t. $x = \sum r_i e_i$. Then $\varphi(x) = \varphi(\sum r_i e_i) = \sum \varphi(r_i e_i) = \sum r_i \varphi(e_i) = \sum r_i m_i$.
$\Rightarrow \varphi$ is unique. Define $\varphi: F \longrightarrow M$, $\sum r_i e_i \mapsto \varphi(\sum r_i e_i) = \sum r_i m_i$. Take $x = \sum r_i e_i$, $y = \sum s_i e_i$, $r, s \in R$. $\varphi(rx+sy) = \varphi(\sum (rr_i + ss_i) e_i) = \sum (rr_i + ss_i) m_i = r \sum r_i m_i + s \sum s_i m_i$
$= r\varphi(x) + s\varphi(y)$. Thus, $\varphi$ is a module homomorphism // q.e.d.

**Proposition** Let $R$ be a ring, $M$ be a finitely generated $R$-module $\Rightarrow \exists F$ free module, $P \leq F$ s.t. $M \cong \frac{F}{P}$.

Proof – $M$ is finitely generated $\Rightarrow \exists m_1, \dots, m_n \in M$ s.t. $M = Rm_1 + \dots + Rm_n$ (uniqueness not necessary). Take $F = R^n$ with usual basis $e_1, \dots, e_n \Rightarrow \exists$ unique $\varphi: F \to M$ module homomorphism s.t. $\varphi(e_i) = m_i$. Note that $\forall i = 1, \dots, n$, $m_i \in \operatorname{Im}\varphi \Rightarrow \operatorname{Im}\varphi = M$. Then by 1st isomorphism theorem, $\frac{F}{\operatorname{Ker}\varphi} \cong M$ (take $P = \operatorname{Ker}\varphi \leq M$), then $M \cong \frac{F}{P}$ // q.e.d.

**Theorem** Let $R$ be a PID. If the free modules $R^m$ and $R^n$ are isomorphic, then $m = n$. (In particular, any two bases of the same free module have the same number of elements.)

Remark – This is not true if $R$ is not a commutative ring. Also, there is a more complicated, general proof – but here we restrict it to the simple case, for IDs).

Proof – As $R$ is an ID, $\exists Q = Q(R)$ field of fractions of $R$. Assume $\varphi: R^m \to R^n$ is a module isomorphism. We want an isomorphism between $Q^m, Q^n$. Claim: If we have a basis $\{e_1, \dots, e_m\}$ of $R^m$, then $\{e_1, \dots, e_m\}$ is also a basis for $Q^m$. Consider $\psi: Q^m \to Q^n$, $x = \sum_{i=1}^m \lambda_i e_i \mapsto \psi(x) = \sum_{i=1}^m \lambda_i \varphi(e_i)$ for unique $\lambda_i \in Q$. Then $\psi$ is a module homomorphism (same proof as before). Assume $x \in \operatorname{Ker}\psi$, $x = \sum \lambda_i e_i$. $\psi(x) = \sum \lambda_i \varphi(e_i) = 0$. $\lambda_i = \frac{a_i}{b_i}$ for $a_i, b_i \in R$, $b_i \neq 0$. Then $\psi(x) = \sum \frac{a_i}{b_i} \varphi(e_i)$. Take $b = b_1 \cdots b_m$, then, $\hat{b}_i = \frac{b}{b_i} = b_1 \cdots b_{i-1} b_{i+1} \cdots b_m$
$\Rightarrow \psi(x) = \sum \frac{a_i \hat{b}_i}{b} \varphi(e_i) = \frac{1}{b} \sum \overbrace{(a_i \hat{b}_i)}^{\in R} \cdot \varphi(e_i) = \frac{1}{b} \sum \varphi(a_i \hat{b}_i e_i) = \frac{1}{b} \varphi(\sum a_i \hat{b}_i e_i) \Rightarrow \frac{1}{b} \varphi(\sum a_i \hat{b}_i e_i) = 0$. $b \neq 0 \Rightarrow \varphi(\overbrace{\sum a_i \hat{b}_i e_i}^{\in R^m}) = 0$. Since $\varphi$ is an isomorphism on $R^m$, $\sum a_i \hat{b}_i e_i = 0$. Since this is an element on a free module, expression w.r.t. basis is unique, so $a_i \hat{b}_i = 0$. $\hat{b}_i \neq 0$, so $a_i = 0$ as $R$ is an ID. $\Rightarrow a_1 = \dots = a_m = 0 \Rightarrow \lambda_i = 0 \ \forall i$
$\Rightarrow x = 0 \Rightarrow \operatorname{Ker}\psi = \{0\}$. $\psi$ is injective. For surjectivity, $y \in Q^n \Rightarrow y = (\mu_1, \dots, \mu_n)$, $\mu_j \in Q$. $\varphi: R^m \to R^n$ is surjective (isomorphism), so $\forall j = 1, \dots, n$, $\exists x_j \in R^m$ s.t. $\varphi(x_j) = f_j$ where $\{f_1, \dots, f_n\}$ is a basis for $R^n$. Take $x = \sum \mu_j x_j$. $\psi(x) = \sum \mu_j \psi(x_j) = \sum \mu_j f_j = y \Rightarrow \psi$ is surjective. Thus $\psi: Q^m \to Q^n$ is an isomorphism.
Since $Q$ is a field $\overset{\text{basis theorem}}{\Longrightarrow} m = n$ // q.e.d.

Note – In more general proof, for any ring s.t. $\exists I \trianglelefteq R$ maximal, same strategy but map is $\bar{\varphi}: (\frac{R}{I})^m \to (\frac{R}{I})^n$.

The bottom line which is important is this: $\boxed{R^m \cong R^n \Leftrightarrow m = n}$.

**Definition** If $M \cong R^n$, we say that $M$ has rank $n$. (Written $\operatorname{rk}(M) = n$).

Chapter 4
# FREE MODULES, FINITELY GENERATED MODULES AND MATRICES OVER PIDs.

Consider for instance the Dihedral group $D_8 = \langle x, y \mid x^4 = y^2 = 1, \ yx = x^3 y \rangle$. What exactly does notation like this mean? With generators and relations, we want to formalise our understanding – if $M$ is a finitely generated module with generators $e_1, \dots, e_n$ and some relations $f_j$, we write $M = \langle e_i \mid f_i = 0 \rangle$. If all $f_i = 0$, we can just think of $f_i$ as elements. (analogous to $x^4 = 1, y^2 = 1, yx^2y = 1$)
Then if $G = \langle x, y \rangle$, $H = \langle x^4, y^2, yx^2y \rangle$, then $D_8 = \frac{G}{H}$.

**Definition** Let $R$ be a ring, $M$ be a finitely generated $R$-module. We say that $M$ is <u>finitely presented</u> if $\exists F = R^n$ free $R$-module and $P \leq F$ finitely generated s.t. $M \cong \frac{F}{P}$.

**Proposition** Let $R$ be a ring, $M$ an $R$-module, $P \leq M$. If $P$ is finitely generated, $M/P$ is finitely generated, then $M$ is also finitely generated.

[Alternatively, in the SES $0 \to P \to M \to \frac{M}{P} \to 0$, if $P, \frac{M}{P}$ are f.g., so is $M$].

Proof – Let $\{y_1, \dots, y_t\}$ be a finite set of generators for $P$, let $\{\bar{x}_1, \dots, \bar{x}_s\}$ be a finite set of generators for $\frac{X}{P}$. Claim: $\{x_1, \dots, x_s, y_1, \dots, y_t\}$ is a generating set for $M$.
$m \in M$, $\bar{m} \in M/P \Rightarrow \exists r_1, \dots, r_s \in R$ s.t. $\bar{m} = r_1 \bar{x}_1 + \dots + r_s \bar{x}_s = \overline{r_1 x_1 + \dots + r_s x_s} \Rightarrow m - (\sum r_i x_i) \in P$. Let $m - (\sum r_i x_i) = p$. Since $P$ is finitely generated,
$\exists l_1, \dots, l_t$ s.t. $p = l_1 y_1 + \dots + l_t y_t \Rightarrow m = p + \sum r_i x_i = \sum_{i=1}^t l_i y_i + \sum_{i=1}^s r_i x_i \Rightarrow m$ is a linear combination of $\{x_1, \dots, x_s, y_1, \dots, y_t\}$ // q.e.d.

28 November 2013
Dr. Javier LÓPEZ-PEÑA
Maths 500

**Proposition** Let $R$ be a PID, $F \cong R^n$ be a free module, $P \leq F$ a submodule. Then $P$ is finitely generated.

Proof – By induction on $n = \operatorname{rank} F$. $n = 1 \Rightarrow F = {}_R R$. $P \leq F \Rightarrow P \trianglelefteq R$, $R$ PID $\Rightarrow P = (a)$ finitely generated. Assume every submodule of $R^n$ is finitely generated. Assume every submodule of $R^n$ is finitely generated. Let $F = R^{n+1}$, $P \leq F$. Consider $\alpha: F \longrightarrow R$, $(r_1, \dots, r_{n+1}) \mapsto r_{n+1}$. $\operatorname{Ker}\alpha = \{(r_1, \dots, r_n, 0) \mid r_i \in R\} \cong \underset{\wedge}{\overset{= F_n}{R^n}}$, which is a free module of rank $n$. Then consider now $\beta = \alpha|_P : P \to R$ defined by $p \mapsto \alpha(p)$ [this is a restriction]. Then $\operatorname{Ker}\beta = F_n \cap P \leq F_n$ submodule $\Rightarrow F_n \cap P$ is finitely generated. Then by the 1st isomorphism theorem, $\frac{P}{F_n \cap P} \cong \operatorname{Im}\beta \leq R$ submodule. Then since $\operatorname{Im}\beta$ is an ideal and $R$ is a PID, $\operatorname{Im}\beta$ is finitely generated. Apply proposition, then $F_n \cap P$, $\frac{P}{F_n \cap P}$ f.g. $\Rightarrow P$ is f.g. // q.e.d.

Remark – Same proof works for $R$ Noetherian ring (satisfies ACC for all ideals).

**Corollary** Let $R$ be a PID, $M$ be a finitely generated $R$-module. Then $M$ is finitely presented.

Non-Example – Let $R = \mathbb{F}[x_1, x_2, x_3, \dots]$, and $I = \{\text{polynomials with constant term} = 0\} = (x_1, x_2, \dots)$. $R$ is finitely generated as an $R$-module ($R = R \cdot 1$), but then we see that $I \leq_R R$ is not finitely generated. Also, $M = \frac{R}{I} \cong \mathbb{F}$, which is finitely generated. $R = R \cdot 1$ is free. But $M$ is not finitely presented.

Let $R$ be a PID, $M$ be a finitely generated $R$-module. $\Rightarrow M = \frac{F}{P}$ for $F = R^n$ free, $P \leq F$ f.g. Let $\{e_1, \dots, e_n\}$ be a basis of $F$, $\{f_1, \dots, f_n\}$ be a generating set of $P$.

$\Rightarrow f_j = \sum_{i=1}^{n} a_{ij} e_i$ for some $a_{ij} \in R$. We can construct a matrix $A = (a_{ij}) \in M_{n\times m}(R)$. This matrix is called a presentation matrix for the module $M$.

This matrix is not unique – many matrices come from the same module.

4.2 MATRICES OVER PIDS AND FREE MODULES.

Notation – Let $R$ be a ring, $M_n(R)$ be the set of $n\times n$ matrices over $R$. We write $GL_n(R) = U(M_n(R))$. $\det(A) = \sum_{\sigma\in S_n} (\operatorname{sgn}\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)}$ – this definition works for commutative rings.

Most properties of det still hold. Exception: if $A \in M_n(\mathbb{F}) \Rightarrow A$ invertible $\Leftrightarrow \det A \neq 0$. and $A^{-1} = \frac{1}{\det A} \operatorname{adj}(A)^T$. We have an issue with $\frac{1}{\det A}$ for arbitrary rings.

**Theorem** Let $R$ be a commutative ring. $A \in M_n(R) \Rightarrow A \operatorname{adj}(A)^T = \det(A)\cdot I_n$. In particular, $A \in GL_n(R) \Leftrightarrow \det(A) \in U(R)$.

3 December 2013.
Dr. Javier LÓPEZ-PEÑA.
Maths 500.

Let $M = R^m$ with basis $\{e_1, \dots, e_m\} = e$. $x \in M \Rightarrow x = r_1 e_1 + \dots + r_m e_m$, $[x]_e = \begin{pmatrix} r_1 \\ \vdots \\ r_m \end{pmatrix} \in M_{m\times 1}(R)$, the coordinates of $x$ w.r.t. basis $e$. $N = R^n$ with basis $\{f_1, \dots, f_n\} = f$,

$\alpha: M \to N$, then $\alpha(e_j) = \sum_{i=1}^{n} a_{ij} f_i \rightsquigarrow [a_{ij}] \in M_{n\times m}(R)$ is a representation of the module homomorphism.

Same properties from linear algebra still hold – • $[\alpha(m)]_f = [\alpha]^e_f [m]_e$. • $\alpha: M\to N$, $\beta: N \to P$, $M = R^m, N = R^n, P = R^p$. Then $[\beta\circ\alpha]^e_g = [\beta]^f_g [\alpha]^e_f$. • If $\dim M = \dim N$, $\alpha$ isomorphism $\Leftrightarrow [\alpha]^e_f \in GL_m(R)$.

Let $M = R^m$, $e = \{e_1, \dots, e_m\}$ and $e' = \{e'_1, \dots, e'_m\}$ bases, then $e'_j = \sum_{i=1}^{m} p_{ij} e_i$, then $P = [p_{ij}] = [\mathrm{Id}_M]^{e'}_e$. $P$ is called the transition matrix from $e'$ to $e$, and $[\mathrm{Id}_M]^{e'}_e \in GL_m(R)$.

$M \xrightarrow{\alpha} N$ (basis $e$, basis $f$), $\alpha$ is given by $[\alpha]^e_f$. Or,
$$\begin{array}{ccc} M & \xrightarrow{\alpha} & N \\ {\scriptstyle \mathrm{Id}_M}\uparrow & & \downarrow{\scriptstyle \mathrm{Id}_N} \\ M & \xrightarrow{\alpha} & N \end{array}$$
(basis $e'$, basis $f'$) $\Rightarrow$ we get the rule: $[\alpha]^{e'}_{f'} = [\mathrm{Id}_N]^f_{f'} [\alpha]^e_f [\mathrm{Id}_M]^{e'}_e$. There is something "odd" about fixing a basis – since this should apply for all bases! Then we get the relation as follows – $[\alpha]^{e'}_{f'} = X[\alpha]^e_f Y$, $X \in GL_n(R)$, $Y \in GL_m(R)$. Any such $X, Y$ produces a new basis.

**Definition** Let $A, B \in M_{n\times m}(R)$. $A, B$ are said to be equivalent if $\exists X \in GL_n(R)$, $Y \in GL_m(R)$ s.t. $B = XAY$. We write $A \sim B$.

Remark – This is a weaker condition than similarity, which requires $Y = X^{-1}$.

Let $M = F/P$ be a finitely presented module, $F = R^n$ a free module with basis $\{e_1, \dots, e_n\}$, $P \leq F$ finitely generated submodule with generators $\{f_1, \dots, f_m\}$, $A = [a_{ij}]$ presentation matrix with $f_j = \sum a_{ij} e_i$. Take $G = R^m$ free module with basis $\{g_1, \dots, g_m\}$. $\exists$ unique module homomorphism $\alpha: G \to F$ s.t. $\alpha(g_j) = f_j = \sum_{i=1}^{n} a_{ij} e_i$. Then $[\alpha]^g_e = A$, which is exactly the same as the presentation matrix earlier obtained. Then $\operatorname{Im}\alpha = P \leq F$, which is independent of basis/coordinate system chosen. Then if $g' = \{g'_1, \dots, g'_m\}$ is a new basis of $G$, we have $\{\alpha(g'_1), \dots, \alpha(g'_m)\}$ generating $P$; i.e. it is a new generating set for $P$ module. Conversely, if $e' = \{e'_1, \dots, e'_n\}$ is a new basis for $F$, $A' = [\alpha]^{g'}_{e'}$ is also a presentation matrix for $M$.

**Theorem** Let $A$ be a presentation matrix for $M = F/P$, $B \sim A$ i.e. $B = XAY$, $X \in GL_n(R)$, $Y \in GL_m(R)$ $\Rightarrow$ $B$ is also a presentation matrix for $M$.

4.3 ELEMENTARY MATRICES AND OPERATIONS.

We standardise the following notation: 1. Swap two rows/columns $\binom{R_i \leftrightarrow R_j}{C_i \leftrightarrow C_j}$. 2. Multiply row/column by $u \in U(R)$ units. $(uR_i/uR_j)$. 3. Add to a row/column a multiple of another $\binom{R_i + \lambda R_j}{C_i + \lambda C_j}$, $\lambda \in R$

Each has a corresponding elementary matrix. Row reduction corresponds to left-multiplying invertible matrices, which are products of these elementary matrices...... But! These apply only to Euclidean domains! There will be some invertible matrices that cannot be obtained.

Chapter 5
SMITH NORMAL FORM.

**Theorem** (Smith Normal Form)

Let $R$ be a PID, $A \in M_{m\times n}(R) \Rightarrow A$ is equivalent to a diagonal matrix $D = \operatorname{diag}(d_1, \dots, d_r)$ where $r = \min(m,n)$ and $d_1 | d_2 | \cdots | d_r$. Moreover, the elements $d_i$ are unique up to associates.

Examples –

1. Consider $\begin{pmatrix} 0 & 6 \\ 3 & 8 \\ 9 & 18 \end{pmatrix} \in M_{3\times 2}(\mathbb{Z})$. $R = \mathbb{Z}$, which is not a field. However, it is a Euclidean domain so we can perform elementary operations. $\begin{pmatrix} 0 & 6 \\ 3 & 8 \\ 9 & 18 \end{pmatrix} \xleftrightarrow{R_2 \leftrightarrow R_1} \begin{pmatrix} 3 & 8 \\ 0 & 6 \\ 9 & 18 \end{pmatrix} \xleftrightarrow{R_3 - 3R_1} \begin{pmatrix} 3 & 8 \\ 0 & 6 \\ 0 & -6 \end{pmatrix}$
$\xleftrightarrow{R_3 + R_2} \begin{pmatrix} \boxed{3 \; 8} \\ 0 \; 6 \\ 0 \; 0 \end{pmatrix} \xleftrightarrow{R_1 - R_2} \begin{pmatrix} 3 & 2 \\ 0 & 6 \\ 0 & 0 \end{pmatrix} \xleftrightarrow{C_2 - C_1} \begin{pmatrix} 3 & -1 \\ 0 & 6 \\ 0 & 0 \end{pmatrix} \xleftrightarrow{C_1 + 2C_1} \begin{pmatrix} 1 & -1 \\ 12 & 6 \\ 0 & 0 \end{pmatrix} \xleftrightarrow{R_2 - 12R_1} \begin{pmatrix} 1 & -1 \\ 0 & -6 \\ 0 & 0 \end{pmatrix} \xleftrightarrow{C_2 + C_1} \begin{pmatrix} 1 & 0 \\ 0 & -6 \\ 0 & 0 \end{pmatrix} \xleftrightarrow{-C_2} \begin{pmatrix} 1 & 0 \\ 0 & 6 \\ 0 & 0 \end{pmatrix}$ // Note that $8 = 2\cdot 3 + 2 \Rightarrow 2 = 8 - 2\cdot 3$

2. Consider $\begin{pmatrix} 6 & 6 & 15 \\ 2 & 2 & 4 \\ -4 & -6 & 7 \end{pmatrix} \xleftrightarrow{R_2 \leftrightarrow R_1} \begin{pmatrix} 2 & 2 & 4 \\ 6 & 6 & 15 \\ -4 & -6 & 7 \end{pmatrix} \xrightarrow{R_2 - 3R_1} \begin{pmatrix} 2 & 2 & 4 \\ 0 & 0 & 3 \\ -4 & -6 & -7 \end{pmatrix} \xleftrightarrow{R_3 + 2R_1} \begin{pmatrix} 2 & 2 & 4 \\ 0 & 0 & 3 \\ 0 & -2 & 15 \end{pmatrix} \xrightarrow{C_2 - C_1} \begin{pmatrix} 2 & 0 & 4 \\ 0 & 0 & 3 \\ 0 & -2 & 15 \end{pmatrix} \xrightarrow{C_3 - 2C_1} \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & 3 \\ 0 & -2 & 15 \end{pmatrix}$ Do not progress into submatrix yet...
$\xleftrightarrow{R_3 - 5R_1} \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & 3 \\ 0 & -2 & 0 \end{pmatrix} \xleftrightarrow{R_2 \leftrightarrow R_3} \begin{pmatrix} 2 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & 3 \end{pmatrix} \xleftrightarrow{R_1 + R_3} \begin{pmatrix} 2 & 0 & 3 \\ 0 & -2 & 0 \\ 0 & 0 & 3 \end{pmatrix} \xleftrightarrow{C_3 - C_1} \begin{pmatrix} 2 & 0 & 1 \\ 0 & -2 & 0 \\ 0 & 0 & 3 \end{pmatrix} \xleftrightarrow{C_1 \leftrightarrow C_3} \begin{pmatrix} 1 & 0 & 2 \\ 0 & -2 & 0 \\ 3 & 0 & 0 \end{pmatrix} \xrightarrow{R_3 - 3R_1} \begin{pmatrix} 1 & 0 & 2 \\ 0 & -2 & 0 \\ 0 & 0 & -6 \end{pmatrix}$ 2 does not divide! $\xleftrightarrow{C_3 - 2C_1} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & -6 \end{pmatrix}$ // is SNF.

Proof – (Existence) Case 1: ED with norm $N$. Algorithmic proof – Goal: To reduce $A$ to matrix of form $\left(\begin{array}{c|c} d_1 & 0 \\ \hline 0 & A' \end{array}\right)$ and repeat, with $d_1$ divides all entries of $A'$. Iterate until end. To get to this goal, note the following – trivialities first, $A = 0$, $A$ is already in SNF. Assume $A \neq 0$. Pick $a_{ij} \in A$ s.t. $N(a_{ij})$ is minimal. Do $R_1 \leftrightarrow R_i$, $C_1 \leftrightarrow C_j$. Then the element in position (1,1) has minimum norm. Steps to reach SNF are the following: $\boxed{\text{I}}$ Assume $\exists a_{1j}$ in the first row s.t. $a_{11} \nmid a_{1j}$. Then by Euclidean division, $a_{1j} = a_{11}\cdot q + r$, then $N(r) < N(a_{11})$. Perform $C_j - qC_1$. $a_{1j}$ becomes $r$. Perform $C_1 \leftrightarrow C_j$, then we get $r$ in position (1,1). Start over.

$\boxed{\text{II}}$ Assume $\exists a_{i1}$ in first column s.t. $a_{11} \nmid a_{i1}$. Write $a_{i1} = q\cdot a_{i1} + r$, $N(r) < N(a_{11})$. Apply $R_i - qR_1$, getting $r$ in position (1,1). Apply $R_i \leftrightarrow R_1$ (getting $r$ in position (1,1)). Start over from $\boxed{\text{I}}$. Eventually, we get that $a_{11} | a_{i1}, a_{1j}$ $\forall i = 1, \dots, m$, $j = 1, \dots, n$. Then $\boxed{\text{III}}$ apply $C_j - \frac{a_{1j}}{a_{11}} C_1$ $\forall j$, $R_i - \frac{a_{i1}}{a_{11}} R_i$ $\forall i$.

At the end of step $\boxed{\text{III}}$, we have $\left(\begin{array}{c|c} a_{11} & 0 \cdots 0 \\ \hline 0 & \\ \vdots & A' \\ 0 & \end{array}\right)$. $\boxed{\text{IV}}$ suppose $\exists\, a_{ij}$ s.t. $a_{11} \nmid a_{ij}$. Apply $R_1 + R_i$, start over from step $\boxed{\text{I}}$. Then finally at step $\boxed{\text{V}}$, we have $\left(\begin{array}{c|c} d_1 & 0 \\ \hline 0 & A' \end{array}\right)$

with $d_1 | a_{ij}$ $\forall\, a_{ij}$ in $A'$. Then ignore first row/column, repeat process for $A'_1$ which is a smaller matrix. Repeat for $\boxed{\text{I}}$. By reduction of norm $\in \mathbb{N}$, which has the well-ordering property, algorithm eventually terminates.

5 December 2013
Dr. Javier LÓPEZ-PEÑA
Maths 500.

In our next case, consider $R$ PID but not ED. We define a <u>length map</u> for $R$ UFD by $\lambda: R^* \to \mathbb{N}$, $a \mapsto \lambda(a) = \begin{cases} 0 & \text{if } a \in U(R) \\ r & \text{if } a = p_1 \cdots p_r \text{ with } p_i \text{ irreducibles} \end{cases}$

(i.e. number of primes in factorisation, counted with multiplicity). This has the following properties: 1. $a, b \in R^*$, $\lambda(ab) = \lambda(a) + \lambda(b)$ 2. if $a|b$, then $\lambda(a) \leq \lambda(b)$ 3. $a \sim b \iff a|b$ and $\lambda(a) = \lambda(b)$

[this gives us a theoretical approach to the proof – but practically, factorising elements into primes is possibly difficult!]. For $R$ PID but not ED, replace $N$ by $\lambda$.

$\boxed{\text{I}}'$ If $\exists\, a_{1,j}$ s.t. $a_{11} \nmid a_{1j}$. WLOG assume $j=2$ $(a_{11} \nmid a_{12})$. Let $d = \gcd(a_{11}, a_{12})$. By Bézout's identity, $\exists\, x_1, x_2 \in R$ s.t. $d = x_1 a_{11} + x_2 a_{12}$. Then we have $\begin{matrix} d|a_1 \\ d|a_2 \end{matrix} \Rightarrow \begin{matrix} a_{11} = dy_1 \\ a_{12} = dy_2 \end{matrix} \Rightarrow d = dx_1y_1 + dx_2y_2$. By cancellation law, $1 = x_1y_1 + x_2y_2$. Consider $Y = \left(\begin{array}{cc|c} x_1 & -y_2 & \\ x_2 & y_1 & 0 \\ \hline & 0 & I_{m-2} \end{array}\right) \in M_m(R)$. $\det Y = x_1y_1 + x_2y_2 = 1 \in U(R) \Rightarrow$ $Y \in GL_m(R)$. Right multiply $A$ with $Y$ to get $AY = \begin{pmatrix} a_{11} & a_{12} & \cdots \\ a_{21} & a_{22} & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix} \left(\begin{array}{cc|c} x_1 & -y_2 & \\ x_2 & y_1 & 0 \\ \hline & 0 & I_m \end{array}\right) = \begin{pmatrix} x_1a_{11} + x_2a_{12} & \cdots \\ \vdots & \ddots \end{pmatrix} = \begin{pmatrix} d & \cdots \\ \vdots & \ddots \end{pmatrix}$. $d|a_{11} \Rightarrow \lambda(d) \leq \lambda(a_{11})$. Moreover, $d \nsim a_{11}$ $\because$ $d|a_{12}$ but $a_{11} \nmid a_{12}$. Thus, $\lambda(d) < \lambda(a_{11})$ strictly. $\boxed{\text{II}}'$. Same as I$'$ but assume $a_{11} \nmid a_{21}$ (transpose step). $d = a_{11}x_1 + a_{22}x_2$, $x_1y_1 + x_2y_2 = 1$. Then let $X = \left(\begin{array}{cc|c} x_1 & x_2 & \\ -y_2 & y_1 & 0 \\ \hline & 0 & I_{m-2} \end{array}\right)$. Replace $A$ by $XA$ and start over from step $\boxed{\text{I}}'$. then apply steps $\boxed{\text{III}}$, $\boxed{\text{IV}}$ and $\boxed{\text{V}}$ from case 1.

Uniqueness (up to associates): we define the following – for each $i = 1, \ldots, r = \min\{m, n\}$ define the <u>$i^{th}$ fitting ideal</u> $J_i(A)$ = ideal of $R$ generated by all the $i \times i$ minors of $A$. i.e. $J_1(A)$ = ideal generated by entries of $A$, $J_2(A)$ = ideals generated by $\det\begin{pmatrix} a_{i_1j_1} & a_{i_1j_2} \\ a_{i_2j_1} & a_{i_2j_2} \end{pmatrix}$. Proposition: If $A = D(d_1, \ldots, d_r)$ s.t. $d_1 | d_2 | \cdots | d_r$ ($A$ is already in SNF), then $J_i(A) = (d_1 \cdots d_i)$. Proposition: let $A, B \in M_{m \times n}(R)$ where $R$ ID. Then if $A \sim B$, $J_i(A) = J_i(B)$. [$A \sim B$ i.e. $\exists\, X \in GL_m(R)$, $Y \in GL_n(R)$ s.t. $B = XAY$]. Idea of proof for this statement – start with $A$, take $X \in GL_m(R)$, $Y \in GL_n(R)$, then NTP $J_i(A) = J_i(XA) = J_i(AY)$. We use the Binet-Cauchy Theorem: $\det(AB) = \det(A)\det(B)$ and $\det([AB]_{IJ}) = \sum_{K = \{k_1, \ldots, k_r\}} \det A_{IK} \det B_{KJ}$. where $[AB]_{IJ}$ is the minor given by $I = \{i_1, \ldots, i_r\}$, $J = \{j_1, \ldots, j_r\}$. Then $\forall x \in J_i(XA) \Rightarrow x \in J_i(A)$. $\Rightarrow J_i(XA) \subseteq J_i(A)$. Since $X^{-1}$ exists, we do reverse inclusion to get $J_i(A) \subseteq J_i(XA)$.

Suppose $\overset{A}{\overset{\shortparallel}{D(d_1, \ldots, d_r)}} \sim \overset{B}{\overset{\shortparallel}{D(e_1, \ldots, e_r)}}$, with $d_1|d_2|\cdots|d_r$, $e_1|e_2|\cdots|e_r$. $\Rightarrow J_1(A) = J_1(B)$ i.e. $(d_1) = (e_1) \Rightarrow d_1 \sim e_1$. Likewise, we have $J_2(A) = J_2(B) \Rightarrow (d_1d_2) = (e_1e_2) \Rightarrow d_1d_2 \sim e_1e_2$. $d_1 = ue_1$, $u \in U(R)$ $\Rightarrow ue_1d_2 \sim e_1e_2 \overset{\because e_1 \neq 0}{\Rightarrow} ud_2 \sim e_2 \Rightarrow d_2 \sim e_2$. continuing on, $d_i \sim e_i$ .... and $d_r \sim e_r$. $\Rightarrow$ $d_i \sim e_i$ $\forall i = 1, \ldots, r$ $\Rightarrow$ elements are unique up to associates. Suppose instead if $e_1 = 0$, $d_1 = 0$, $d_2 = d_3 = \cdots = 0$, so we have a terminating condition for the algorithm // q.e.d.

10 December 2013.
Dr. Javier LÓPEZ-PEÑA.
Maths 500.

chapter 6

## FINITELY GENERATED MODULES OVER PIDs.

### 6.1 submodules of free modules are free.

$\boxed{\text{Proposition}}$ if $R$ is a PID, $F \cong R^n$ free $R$-module. $P \leq F \Rightarrow \exists\, \{e_1, \ldots, e_n\}$ is a basis of $F$, $\exists\, d_1, \ldots, d_m \in R$ s.t. $\{d_1e_1, \ldots, d_me_m\}$ is a basis of $P$.

[In particular, $P$ is free and $rk(P) \leq rk(F)$.]

Proof – $P$ is finitely generated, so it has generators $(\{f_1, \ldots, f_s\})$ ($s$ elements). Let $G = R^s$ free module of rank $s$, $\alpha: G \to F$ $(\alpha(g_j) = f_j)$ s.t. $\operatorname{Im} \alpha = P$. Let $A$ be a matrix representing $\alpha$ for some bases of $G, F$. $\Rightarrow \exists\, e = \{e_1, \ldots, e_n\}$ basis of $F$ and $g = \{g_1, \ldots, g_s\}$ basis of $G$ s.t. $[\alpha]^g_e = D(d_1, \ldots, d_r)$, $d_1|\cdots|d_r$ is in SNF, by a change in basis of $F$ and $G$. Regardless of basis choice, $\operatorname{Im} \alpha = P$. Then $\alpha(g_j) = \begin{cases} d_je_j & j \leq r \\ 0 & j > r \end{cases}$ $\left(\begin{array}{c|c|c|c} \ddots & 0 & 0 & \cdots 0 \end{array}\right)$. Then $P$ is generated by $\{\alpha(g_1), \ldots, \alpha(g_s)\}$ $= \{d_1e_1, \ldots, d_re_r\}$, so $P = \sum_{i=1} Rd_ie_i$ ($P$ is a sum of these cyclic modules). calculate: $Rd_je_j \cap \sum_{k \neq j} Rd_ke_k$. Then $Rd_je_j \subseteq Re_j$, $\sum_{k \neq j} Rd_ke_k \subseteq \sum_{k \neq j} Re_k$. then $Rd_je_j \cap \sum_{k \neq j} Rd_ke_k \subseteq Re_j \cap \left(\sum_{k \neq j} Re_k\right) = \{0\}$, since $F = Re_1 \oplus \cdots \oplus Re_n$ for basis $\{e_1, \ldots, e_n\}$. Thus, $P = \bigoplus_{j=1}^{r} Rd_je_j$ is a direct sum. Furthermore, if $d_k = 0$, $Rd_ke_k = 0$. so we just remove all $d_k$ s.t. $d_k = 0$. Stop at last nonzero $d_j$, then $P = \bigoplus_{j=1}^{m} Rd_je_j$. Every element in $P$ can be expressed as a linear combination of $\{d_1e_1, \ldots, d_me_m\}$, we then check uniqueness. Assume $a_1d_1e_1 + \cdots + a_md_me_m = b_1d_1e_1 + \cdots + b_md_me_m \Rightarrow \sum_{i=1}^{m} (a_id_i)e_i = \sum_{i=1}^{m} (b_id_i)e_i$ by pseudoassociativity. Since $\{e_1, \ldots, e_m\}$ basis, $a_id_i = b_id_i$ for $i = 1, \ldots, m$. Since $d_1, \ldots, d_m \neq 0$, apply cancellation law $\Rightarrow$ $a_i = b_i$ $\forall i$ $\Rightarrow$ expression as linear comb. is unique $\Rightarrow$ $\{d_1e_1, \ldots, d_me_m\}$ is basis of $P$. In particular, $P$ is free, and $rk(P) = m \leq n = rk(F)$ // q.e.d.

### 6.2 The main theorem

$\boxed{\text{Theorem}}$ - (Classification of finitely generated modules over a PID).

Let $R$ be a PID, $M$ a f.g. $R$-module. $\Rightarrow \exists\, s \in \mathbb{N}$, $\exists\, d_1, \ldots, d_r \in R^* \setminus U(R)$ s.t. $d_1|d_2|\cdots|d_r$ and $\boxed{M = \left(\bigoplus_{i=1}^{r} \frac{R}{(d_i)}\right) \oplus R^s}$.

Proof – $\left.\begin{matrix} R \text{ PID} \\ M \text{ f.g.} \end{matrix}\right\}$ $M$ is finitely presented i.e. $\exists\, F = R^n$ free, $P \leq F$ f.g. submodule s.t. $M \cong F/P$. $\Rightarrow \exists\, \{e_1, \ldots, e_n\}$ basis of $F$, $d_1, \ldots, d_m \in R^*$ s.t. $\{d_1e_1, \ldots, d_me_m\}$ basis of $P$. $F = Re_1 \oplus \cdots \oplus Re_n$, $P = Rd_1e_1 \oplus \cdots \oplus Rd_me_m = Rd_1e_1 \oplus \cdots \oplus Rd_me_m \oplus R \cdot 0\, e_{m+1} \oplus \cdots \oplus R \cdot 0\, e_n$. Then $M \cong \frac{F}{P} \cong \frac{Re_1 \oplus \cdots \oplus Re_m \oplus Re_{m+1} \oplus \cdots \oplus Re_n}{Rd_1e_1 \oplus \cdots \oplus Rd_me_m \oplus R \cdot 0 e_{m+1} \oplus \cdots \oplus R \cdot 0 e_n}$ $\cong \frac{Re_1}{Rd_1e_1} \oplus \cdots \oplus \frac{Re_m}{Rd_me_m} \oplus \underbrace{\frac{Re_{m+1}}{R \cdot 0 \cdot e_m}}_{Re_{m+1} \cong R} \oplus \cdots \oplus \underbrace{\frac{Re_n}{R \cdot 0 \cdot e_n}}_{Re_n \cong R} \cong \frac{R}{(d_1)} \oplus \cdots \oplus \frac{R}{(d_m)} \oplus R \oplus \cdots \oplus R \cong \left(\bigoplus_{i=1}^{r} \frac{R}{(d_i)}\right) \oplus R^s$. If $d_i \in U(R)$, $(d_i) = R$ s.t. $\frac{R}{(d_i)} = 0$. Due to SNF,

if $\alpha: M \to N$ injective
$P \leq M \Rightarrow \frac{M}{P} \cong \frac{\alpha(M)}{\alpha(P)}$

All units in the $d_i$ terms appear in the beginning. After removing the units from front, we get for $r \le m$, $M \cong \bigoplus_{i=1}^{r} \frac{R}{(d_i)} \oplus R^s$ // q.e.d.

Remark – First term (quotient) is for abelian groups, second (free part) is for vector spaces. This is the most complete form.

We then want to show that this decomposition is "unique"

## 6.3 Torsion modules and torsion-free modules.

**Definition** Let $R$ be an ID, $M$ $R$-module, $m \in M$. We say $m$ is a <u>torsion element</u> if $\mathrm{ann}(m) \neq 0$ (i.e. $\exists r \in R^*$ s.t. $rm = 0$. Define $T(M) = \{m \in M \mid \mathrm{ann}(m) \neq 0\} \le M$, which is a submodule. Then $T(M)$ is called the <u>torsion submodule</u> of $M$. If $T(M) = 0$, $M$ is <u>torsion free</u> and if $T(M) = M$, $M$ is a <u>torsion module</u>.

Examples –

1. $M = R^n$ free $\Rightarrow$ $M$ is torsion free $[T(M) = 0]$.
2. If $R = \mathbb{Z}$, $M = {}_{\mathbb{Z}}\mathbb{Q}$. Then ${}_{\mathbb{Z}}\mathbb{Q}$ is torsion free [note however that ${}_{\mathbb{Z}}\mathbb{Q}$ is not free!]
3. $R$ ID, $I \trianglelefteq R$ ideal with $I \neq 0$, $M = \frac{R}{I}$. $\forall m \in M$, $\mathrm{ann}(m) \supseteq I \neq 0 \Rightarrow T(M) = M$.
4. If $R$ PID, $M = \frac{R}{(d_1)} \oplus \cdots \oplus \frac{R}{(d_r)}$ with $d_1 | \cdots | d_r$, $\forall m \in M$, $d_r \cdot m = 0 \Rightarrow M = T(M)$. [actually $\mathrm{ann}(M) = (d_r)$].

**Proposition** Let $R$ be a PID, $M \cong \bigoplus_{i=1}^{r} \frac{R}{(d_i)} \oplus R^s$ f.g. $R$-module. Then $T(M) \cong \bigoplus_{i=1}^{r} \frac{R}{(d_i)}$ and $\frac{M}{T(M)} \cong R_s$.

Proof – Write $A = \bigoplus_{i=1}^{r} \frac{R}{(d_i)}$, $B = R^s$, $M = A \oplus B$. $m \in M$, then $m = (a, b)$ for $a \in A$, $b \in B$. If $r \in R^*$ s.t. $rm = 0$, $(ra, rb) = 0 \Rightarrow \begin{matrix} ra = 0 \\ rb = 0 \end{matrix}$ for $b \in R^s$ free. Since $R^s$ is free, it is torsion free, so $b = 0$. Then $m = (a, 0) \Rightarrow m \in A \Rightarrow T(M) \subseteq \bigoplus_{i=1}^{r} \frac{R}{(d_i)}$. For reverse inclusion, if $m \in \bigoplus_{i=1}^{r} \frac{R}{(d_i)} \Rightarrow d_i \cdot m = 0 \Rightarrow m \in T(M) \Rightarrow$ $T(M) = \bigoplus_{i=1}^{r} \frac{R}{(d_i)}$ // q.e.d. Then since $\left.\begin{matrix} M = A \oplus B \\ \frac{M}{A} \cong B \end{matrix}\right\}$ $\frac{M}{T(M)} \cong \frac{(\oplus \frac{R}{(d_i)}) \oplus R^s}{\oplus \frac{R}{(d_i)}} \cong R^s$ // q.e.d.

**Proposition** If $\left(\bigoplus_{i=1}^{r} \frac{R}{(d_i)}\right) \oplus R^s \cong \left(\bigoplus_{j=1}^{r'} \frac{R}{(d'_j)}\right) \oplus R^{s'} = M$, then $s = s'$ and $\bigoplus_{i=1}^{r} \frac{R}{(d_i)} \cong \bigoplus_{j=1}^{r'} \frac{R}{(d'_j)}$.

Proof – $\bigoplus_{i=1}^{r} \frac{R}{(d_i)} \cong T(M) \cong \bigoplus_{j=1}^{r'} \frac{R}{(d'_j)}$. Similarly $R^s \cong \frac{M}{T(M)} \cong R^{s'} \Rightarrow s = s'$ by uniqueness of dimension // q.e.d.

**Proposition** (important!) If $M$ is a finitely generated module over $R$ PID, then (1) $M$ is torsion free $\Leftrightarrow$ $M$ is free. (2) $M$ is torsion $\Leftrightarrow$ $M \cong \bigoplus_{i=1}^{r} \frac{R}{(d_i)}$, $d_i \in R^* \setminus U(R)$, $d_1 | \cdots | d_r$.

Proof – (1) $M$ torsion free $\Leftrightarrow$ $T(M) = 0$. Then $M \cong \bigoplus_{i=1}^{r} \frac{R}{(d_i)} \oplus R^s \cong T(M) \oplus R^s \cong 0 \oplus R^s \cong R^s$. $\Leftrightarrow$ $M$ is free // q.e.d.

(2) $M$ torsion $\Leftrightarrow$ $M = T(M)$ $\Leftrightarrow$ $M \cong \bigoplus_{i=1}^{r} \frac{R}{(d_i)}$ // q.e.d.

## 6.4 Invariant factors and elementary divisors.

We have already proven that free parts are isomorphic. So now we consider modules that are torsion to evaluate their "uniqueness". As a motivating example, notice that we have:

$\mathbb{Z}_6 = \frac{\mathbb{Z}}{(6)} \cong \mathbb{Z}/(2) \oplus \mathbb{Z}/(3) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3$, this is the Chinese Remainder Theorem. However, we note that 2, 3 do not satisfy our divisibility condition!

**Proposition** (Chinese Remainder theorem for Rings). For $R$ commutative ring, $a, b \in R$ s.t. $\underbrace{(a) + (b) = R}_{\text{"coprime"}} \Rightarrow (a) \cap (b) = (ab)$ and $\frac{R}{(ab)} \cong \frac{R}{(a)} + \frac{R}{(b)}$.

Proof – Left as exercise.

**Corollary** If $R$ is a PID, $d \in R^* \setminus U(R)$, $d = \prod_{i=1}^{s} p_i^{\alpha_i}$ with $p_i$ primes, $i \neq j \Rightarrow p_i \neq p_j$. Then $\frac{R}{(d)} \cong \bigoplus_{i=1}^{s} \frac{R}{(p_i^{\alpha_i})}$

Proof – Induction on $s$.

If $R$ is a PID, $M = T(M)$ torsion $R$-module. $M \cong \frac{R}{(d_1)} \oplus \cdots \oplus \frac{R}{(d_r)}$, $d_1 | d_2 | \cdots | d_r$. We can write $d_1 = p_1^{\alpha_{1,1}} p_2^{\alpha_{2,1}} \cdots p_s^{\alpha_{s,1}}$, $d_2 = p_1^{\alpha_{1,2}} p_2^{\alpha_{2,2}} \cdots p_s^{\alpha_{s,2}}$, …, $d_r = p_1^{\alpha_{1,r}} p_2^{\alpha_{2,r}} \cdots p^{\alpha_{s,r}}$.

Then we get that $0 \le \alpha_{i,1} \le \alpha_{i,2} \le \cdots \le \alpha_{i,r}$ $\forall i = 1, \ldots, s$. Moreover, $\alpha_{i,r} > 0$ $\forall i = 1, \ldots, s$. Also, $\forall j = 1, \ldots, r$, $\exists i$ s.t. $\alpha_{j,i} \ge 1$ (otherwise $d_j \in U(R)$, which we have eliminated). If $M = \bigoplus_{i=1}^{r} \frac{R}{(d_i)}$ with <u>invariant factors</u> $d_1, \ldots, d_r$ of $M$, then we call the table $\{p_i^{\alpha_{j,i}}\}$ the <u>elementary divisors</u>. Then we have: $\frac{R}{(d_i)} = \frac{R}{(p_1^{\alpha_{1,i}})} \oplus \cdots \oplus \frac{R}{(p_s^{\alpha_{s,i}})}$

Instead, we examine information by columns: Then $\boxed{M = \bigoplus_{j=1}^{s} \left( \bigoplus_{i=1}^{r} \frac{R}{(p_i^{\alpha_{j,i}})} \right)}$ which is the elementary divisor decomposition of $M$.

12 December 2013.
Dr. Javier LÓPEZ-PEÑA
Maths 500

**Definition** If $R$ PID, $M$ $R$-mod, $p \in R$ prime. We define $M_p = \{m \in M \mid \exists t \in \mathbb{N}$ s.t. $p^t m = 0\}$ [i.e. $p^t \in \mathrm{ann}(m)$ for some $t$, $p \in \mathrm{rad}(\mathrm{ann}(m))$]. $M_p \le M$ submodule is called the <u>p-primary component of M</u>. Then the elements of $M_p$ are called <u>p-torsion elements</u>.

**Proposition** $M = \bigoplus_{i=1}^{s} \left[ \bigoplus_{j=1}^{r} \frac{R}{(q_i^{\alpha_{i,j}})} \right] \Rightarrow M_{p_i} = \bigoplus_{j=1}^{r} \frac{R}{(p_i^{\alpha_{i,j}})}$

Proof – Let $N_i = \bigoplus_{j=1}^{r} \frac{R}{(p_i^{\alpha_{i,j}})}$. We want $M_{p_i} = N_i$. $p_i^{\alpha_{i,r}} N_i = 0 \Rightarrow N_i \le M_{p_i}$. Moreover, $M = N_1 \oplus \cdots \oplus N_s$. Take $m \in M$, assume $m \in M_{p_i}$. $m = (a_1, \ldots, a_s)$ with $a_j \in N_j$.

$\exists t \in \mathbb{N}$ s.t. $p_i^t \cdot m = 0$. $(p_i^t a_1, \ldots, p_i^t a_s) = 0 \Rightarrow p_i^t \cdot a_j = 0$ $\forall j = 1, \ldots, s$. If $j \neq i$, $\left.\begin{matrix} p_i^t \in \mathrm{ann}(a_j) \\ p_j^{\alpha_{j,r}} \in \mathrm{ann}(a_j) \end{matrix}\right\} \xrightarrow{R \text{ PID}} \gcd(p_i^t, p_j^{\alpha_{j,r}}) \in \mathrm{ann}(a_j) \Rightarrow 1 \cdot a_j = 0$

$\Rightarrow a_j = 0 \Rightarrow m = (0, 0, \ldots, 0, a_1, 0, \ldots, 0) \Rightarrow N_i = M_{p_i}$.

Remark – Moreover, $M = \bigoplus_{i=1}^{s} M_{p_i}$.

3201-18.

Assume $M = \bigoplus_{i=1}^{r} \bigoplus_{j=1}^{s} \frac{R}{(p_i^{\alpha_{ij}})} = \bigoplus_{i=1}^{r} \bigoplus_{j=1}^{s'} \frac{R}{(p_i^{\beta_{ij}})} \Rightarrow M_{p_i} = \bigoplus_{j=1}^{s} \frac{R}{(p_i^{\alpha_{ij}})} = \bigoplus_{j=1}^{s'} \frac{R}{(p_i^{\beta_{ij}})}$. To prove uniqueness of decomposition, we can restrict ourselves to the case $M = M_p = \bigoplus_{i=1}^{r} \frac{R}{(p^{\alpha_i})}$.

$\boxed{\text{Proposition}}$ If $M$ is an $R$-module, $x \in R$ s.t. $xM = 0$ $(x \in \text{ann}(M)) \Rightarrow M$ is also an $\frac{R}{(x)}$-module with action $(r + (x)) \cdot m = rm$.

Proof – We only have to check that homomorphism is well defined.

$\boxed{\text{Corollary}}$ If $A$ is an $R$-module, $x \in R$, $xA = \{xa \mid a \in A\} \leq A$ submodule. $x \cdot \frac{A}{xA} = \frac{xA}{xA} = 0. \Rightarrow \boxed{\frac{A}{xA} \text{ is an } \frac{R}{(x)}\text{-module}}$

Assume $M = M_p = \frac{R}{(p^{\alpha_1})} \oplus \cdots \oplus \frac{R}{(p^{\alpha_r})}$. Then $1 \leq \alpha_1 \leq \alpha_2 \leq \cdots \leq \alpha_r$. $\forall i \in \mathbb{N}$, $p^i M \leq M$, $p^{i+1} \cdot M = p(p^i M) \leq p^i M$. Then $\frac{p^i M}{p^{i+1} M}$ is an $\frac{R}{(p)}$-module. $\left.\begin{matrix} p \text{ prime} \\ R \text{ PID} \end{matrix}\right\} \Rightarrow (p)$ maximal ideal

$\Rightarrow \frac{R}{(p)} = \mathbb{F}$ field; it is thus also an $\mathbb{F}$ vector space.

- If $\alpha \leq i$, $p^i \frac{R}{(p^\alpha)} = 0$, and clearly $p^{i+1} \frac{R}{(p^\alpha)} = 0$ as well. $\Rightarrow \frac{p^i R/(p^\alpha)}{p^{i+1} R/(p^\alpha)} = 0/0 = 0$.
- If $\alpha > i$, then $p^i \frac{R}{(p^\alpha)}$ is non-zero. Then $\frac{p^i R/(p^\alpha)}{p^{i+1} R/(p^{\alpha+1})} = \frac{(p^i)/(p^\alpha)}{(p^{i+1})/(p^\alpha)} \overset{3^{rd} \text{ Isom}}{\cong} \frac{(p^i)}{(p^{i+1})} = \frac{Rp^i}{Rpp^i} = \frac{R}{(p)} = \mathbb{F}$.

Then $\frac{p^i M}{p^{i+1} M} = \mathbb{F}^{n_i}$ where $n_i = \#\{\alpha_j \mid \alpha_j > i\}$ [because $M = \frac{R}{(p^{\alpha_1})} \oplus \cdots \oplus \frac{R}{(p^{\alpha_r})}$]. On the other hand, $n_i = \dim_{\mathbb{F}} \frac{p^i M}{p^{i+1} M}$. This does not depend on the decomposition.

Also, we seek $m_k = \#\{\alpha_j \mid \alpha_j = k\}$ (which will determine the decomposition) $= \#\{\alpha_j \mid \alpha_j > k-1\} - \#\{\alpha_j \mid \alpha_j > k\} = n_{k-1} - n_k$. Thus as a consequence, $\alpha$is are unique.

$\Rightarrow$ decomposition of a torsion module is unique, using elementary divisors. Only thing left to do is to recover $d_j$ terms from $p_i^{\alpha_{i,j}}$ terms. We have that…

$$\begin{matrix} d_1 = p_1^{\alpha_{1,1}} p_2^{\alpha_{2,1}} \cdots p_s^{\alpha_{s,1}} \\ \vdots \quad \vdots \quad \ddots \quad \vdots \\ d_r = p_1^{\alpha_{1,r}} \cdots \cdots p_s^{\alpha_{s,r}} \end{matrix}$$

This will enable us to decompose accordingly, or recover numbers in opposite computation.

Example – Suppose $A = \mathbb{Z}_2 \oplus \mathbb{Z}_{20} \oplus \mathbb{Z}_{60} \oplus \mathbb{Z}_{120}$. This is an invariant factor decomposition, since $2 | 20 | 60 | 120$. Then

$$\begin{matrix} 2 = 2^1 \cdot 3^0 \cdot 5^0 \\ 20 = 2^2 \cdot 3^0 \cdot 5^1 \\ 60 = 2^2 \cdot 3^1 \cdot 5^1 \\ 120 = 2^3 \cdot 3^1 \cdot 5^1 \end{matrix}$$

is the table of elementary divisors.

Then $A \cong [\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_8] \oplus [\mathbb{Z}_3 \oplus \mathbb{Z}_3] \oplus [\mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5]$. How can we recover $d_j$ terms? We have $2, \underline{4}, 4, 8, 3, 3, \underline{5}, 5, 5$. Start from largest divisor, take highest power of each prime factor and delete them, then repeat downwards. We get $2^3 \cdot 3 \cdot 5$, $2^2 \cdot 3 \cdot 5$, $2^2 \cdot 5$, $2 \Rightarrow$ $d_4 = 120$, $d_3 = 60$, $d_2 = 20$, $d_1 = 2$.

then number the factors backwards.

END OF SYLLABUS.

END OF COURSE.