What We Need to Know about Rings and Modules

Class Notes for Mathematics 700 by Ralph Howard

October 31, 1995

Contents

1 Rings

1.1 The Definition of a Ring

We have been working with fields, which are the natural generalization of familiar objects like the real, rational and complex numbers where it is possible to add, subtract, multiply and divide. However there are some other very natural objects like the integers and polynomials over a field where we can add, subtract, and multiply, but where it not possible to divide. We will call such rings. Here is the official definition:

Definition 1.1 *A **commutative ring** $(R, +, \cdot)$ is a set R with two binary operations $+$ and $\cdot$ (as usual we will often write $x \cdot y = xy$) so that*

1. *The operations $+$ and $\cdot$ are both commutative and associative:*

$$x + y = y + x, \quad x + (y + z) = (x + y) + z, \qquad xy = yx, \quad x(yz) = (xy)z.$$

2. *Multiplication distributes over addition:*

$$x(y + z) = xy + xz.$$

3. *There is a unique element $0 \in R$ so that for all $x \in R$*

$$x + 0 = 0 + x = x.$$

*This element will be called the **zero** of R.*

4. *There is a unique element $1 \in F$ so that for all $x \in R$*

$$x \cdot 1 = 1 \cdot x = x.$$

*This element is called the **identity** of R.*

5. *$0 \neq 1$. (This implies R has at least two elements.)*

6. *For any $x \in R$ there is a unique $-x \in R$ so that*

$$x + (-x) = 0.$$

*(This element is called the **negative** of x. And from now on we write $x + (-y)$ as $x - y$.)*

We will usually just refer to "the commutative ring R" rather than "the commutative ring $(R, +, \cdot)$". Also we will often be lazy and refer to R as just a "ring" rather than a "commutative ring"[1]. As in the case of fields we can view the positive integer n as an element of ring R by setting

$$n := \underbrace{1 + 1 + \cdots + 1}_{n \text{ terms}}$$

Then for negative n we can set $n := -(-n)$ where $-n$ is defined by the last equation. That is $5 = 1 + 1 + 1 + 1 + 1$ and $-5 = -(1 + 1 + 1 + 1 + 1)$.

While in a general ring it is not possible to divide by arbitrary nonzero elements (that is to say that arbitrary nonzero elements do not have inverses as division is defined in terms of multiplication by the inverse), it may happen that there are some elements that do have inverses and we can divide by these elements. We give a name to these elements.

Definition 1.2 *Let R be a commutative ring. Then an element $a \in R$ is a **unit** or has an **inverse** b iff $ab = 1$. In this case we write $b = a^{-1}$.*

Thus when talking about elements of a commutative ring saying that a is a unit just means a has an inverse.

[1]For those of you how can not wait to know: A non-commutative ring satisfies all of the above except that multiplication is no longer assumed commutative (that is it can hold that $xy \neq yx$ for some $x, y \in R$) and we have to add that both the left and right distributive laws $x(y + z) = xy + xz$ and $(y + z)x = yx + zx$ hold. The natural example of such a non-commutative ring is the set of square $n \times n$ matrices over a field with the usual addition and multiplication.

1.2 Examples of Rings

1.2.1 The Integers

The integers $\mathbf{Z}$ are as usual the numbers $0, \pm 1, \pm 2, \pm 3, \ldots$ with the addition and multiplication we all know and love. This is the main example you should keep in mind when thinking about rings. In $\mathbf{Z}$ the only units (that is elements with inverses) are 1 and -1.

1.2.2 The Ring of Polynomials over a Field

Let $\mathbf{F}$ be a field and let $\mathbf{F}[x]$ be the set of all polynomials

$$p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

where $a_0, \ldots, a_n \in \mathbf{F}$ and $n = 0, 1, 2 \ldots$. These are added, subtracted, and multiplied in the usual manner. This is the example that will be most important to us, so we review a little about polynomials. First if $p(x)$ is not the zero polynomial and $p(x)$ is as above with $a_n \neq 0$ then n is the ***degree*** of $p(x)$ and this will be denoted by $n = \deg p(x)$. The the nonzero constant polynomials a have degree 0 and we do not assign any degree to the zero polynomial. If $p(x)$ and $q(x)$ are nonzero polynomials then we have

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

Also if given $p(x)$ and $f(x)$ with $p(x)$ not the zero polynomial we can "divide"[2] $p(x)$ into $f(x)$. That is there are unique polynomials $q(x)$ (the ***the quotient***) and $r(x)$ (the ***the reminder***) so that

$$f(x) = q(x)p(x) + r(x) \quad \text{where } \deg r(x) < \deg p(x) \text{ or } r(x) \text{ is the zero polynomial.}$$

This is called the division algorithm. If $p(x) = x - a$ for some $a \in \mathbf{F}$ then this becomes

$$f(x) = q(x)(x - a) + r \quad \text{where } r \in \mathbf{F}.$$

By letting $x = a$ in this equation we get the fundamental

Proposition 1.3 (Remainder Theorem) *If $x - a$ is divided into $f(x)$ then the remainder is $r = f(a)$. If particular $f(a) = 0$ if and only if $x - a$ divides $f(x)$. That is $f(a) = 0$ iff $f(x) = (x - a)q(x)$ for some polynomial $q(x)$ with $\deg q(x) = \deg f(x) - 1$.*

I am assuming that you know how to add, subtract and multiply polynomials, and that given $f(x)$ and $p(x)$ with $p(x)$ not the zero polynomial that you can divide $p(x)$ into $f(x)$ and find the quotient $q(x)$ and remainder $r(x)$.

Problem 1 Show that the units in $R := \mathbf{F}[x]$ are the nonzero constant polynomials.

[2]Here we are using the word "divide" in a sense other than "multiplying by the inverse". Rather we mean "find the quotient and remainder". I will continue to use the word "divide" in both these senses and trust it is clear from the context which meaning is being used.

1.2.3 The Integers Modulo n

This is not an example that will come up often, but it does illustrate that rings can be quite different than the basic example of the integers and the polynomials over a field. You can skip this example with no ill effects. Basically this is a generalization of the example of finite fields. Let $n > 1$ be an integer and let $\mathbf{Z}/n$ be the integers reduced modulo n. That is we consider two integers x and y to be "equal" (really congruent modulo n) if and only if they have the same remainder when divided by n in which case we write $x \equiv y \bmod n$. Therefore $x \equiv y \bmod n$ if and only if $x - y$ is evenly divisible by x. It is easy to check that

$$\begin{aligned} x_1 \equiv y_1 \bmod n \quad &\text{and} \quad x_2 \equiv y_2 \bmod n \quad \text{implies} \\ &x_1 + y_2 \equiv x_1 + y_2 \bmod n \quad \text{and} \quad x_1 x_2 \equiv y_1 y_2 \bmod n. \end{aligned}$$

Then $\mathbf{Z}/n$ is the set of congruence classes modulo n. It only takes a little work to see that with the "obvious" choice of addition and multiplication that $\mathbf{Z}/p$ satisfies all the conditions of a commutative ring. Show this yourself as an exercise.) Here is the case $n = 6$ in detail. The possible remainders when a number is divided by 6 are 0, 1, 2, 3, 4, 5. Thus we can use for the elements of $\mathbf{Z}/6$ the set $\{0, 1, 2, 3, 4, 5\}$. Addition works like this. $3 + 4 = 1$ in $\mathbf{Z}/6$ as the remainder of $4 + 3$ when divided by 6 is 1. Likewise $2 \cdot 4 = 2$ in $\mathbf{Z}/6$ as the remainder of $2 \cdot 4$ when divided by 6 is 2. Here are the addition and multiplication tables for $\mathbf{Z}/6$

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	4	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

This is an example of a ring with ***zero divisors***, that is nonzero elements a and b so that $ab = 0$. For example in $\mathbf{Z}/6$ we have $3 \cdot 4 = 0$. This is different from what we have seen in fields where $ab = 0$ implies $a = 0$ or $b = 0$. We also see from the multiplication table that the units in $\mathbf{Z}/6$ are 1 and 5. In general the units of $\mathbf{Z}/n$ are the correspond to the numbers x that are relatively prime to n.

1.3 Ideals in Rings

I can not think of a natural way to motivate this idea, which is unfortunate as it very useful and it *is* very natural in the sense that once you start doing anything nontrivial with rings ideals force themselves on you. However if for the time being it does not look like a natural idea don't worry, it gets easier.

Definition 1.4 *Let R be a commutative ring. Then a nonempty subset $A \subset R$ is an* ***ideal*** *if and only if it is closed under addition and multiplication by elements of R. That is*

$$a, b \in A \quad \textit{implies} \quad a + b \in A$$

(this is closure under addition) and

$$a \in A,\ r \in R \quad \textit{implies} \quad ar \in A$$

(this is closure under multiplication by elements of R).

There are two trivial examples of ideals in any R. The set $A = \{0\}$ is an ideal as is $A := R$. While it is possible to give large numbers of other examples of ideals in various rings for our work in this class we only really need to know one more example:

Problem 2 Let R be a commutative ring and let $a \in R$. Let $\langle a \rangle$ be the set of all multiples of a by elements of R. That is

$$\langle a \rangle := \{ra : r \in R\}.$$

Then show $A := \langle a \rangle$ is an ideal in R.

Definition 1.5 *If R is a commutative ring and $a \in R$, then $\langle a \rangle$ as defined in the last exercise is the **principle ideal** defined generated by a.*

2 Euclidean Domains

2.1 The Definition of Euclidean Domain

As we said above for us the most important examples of rings are the ring of integers and the ring of polynomials over a field. We now make a definition that captures many of the basic properties these two examples have in common.

Definition 2.1 *A commutative ring R is a **Euclidean domain** iff*

1. *R has no zero divisors[3]. That is if $a \neq 0$ and $b \neq 0$ then $ab \neq 0$. (Or in the contrapositive form $ab = 0$ implies $a = 0$ or $b = 0$.)*
2. *Then is a function $\delta : (R \setminus \{0\}) \to \{0, 1, 2, 3, \ldots\}$ (that is δ maps nonzero elements of R to nonnegative integers) so that*
   (a) *If $a, b \in R$ are both nonzero then $\delta(a) \leq \delta(ab)$.*
   (b) *The **division algorithm** holds in the sense that if $a, b \in R$ and $a \neq 0$ then we can divide a into b to get a **quotient** q and a **reminder** r so that*

$$b = aq + r \quad \textit{where } \delta(r) < \delta(a) \textit{ or } r = 0$$

2.2 The Basic Examples of Euclidean Domains

Our two basic examples of Euclidean domains are the integers $\mathbf{Z}$ with $\delta(a) = |a|$, the absolute value of a and $\mathbf{F}[x]$, the ring of polynomials over a field $\mathbf{F}$ with $\delta(p(x)) = \deg p(x)$. We record this as theorems:

Theorem 2.2 *The integers $\mathbf{Z}$ with $\delta(a) := |a|$ is a Euclidean domain.*

[3] In general a commutative ring R with no zero divisors is called an *integral domain* or just a *domain*.

Theorem 2.3 *The ring of polynomials* $\mathbf{F}[x]$ *over a field* $\mathbf{F}$ *with* $\delta(p(x)) = \deg p(x)$ *is a Euclidean domain.*

PROOFS: These follow form the usual division algorithms in $\mathbf{Z}$ and $\mathbf{F}[x]$. ❑

2.3 Primes and Factorization in Euclidean Domains

We now start to develop the basics of "number theory" in Euclidean domains. By this is meant that we will show that it is possible to define define things like "primes" and greatest "common divisors" and show that they behave just as in the case of the integers. Many of the basic facts about Euclidean domains are proven by starting with subset S of the Euclidean domain in question and then choosing an element a in S that minimizes $\delta(a)$. While it is more or less obvious that it is always possible to do this we record (without proof) the result that makes it all work.

Theorem 2.4 (Axiom of Induction) *Let* $\mathbf{N} := \{0, 1, 2, 3, \ldots\}$ *be the natural numbers (which is the same thing as the nonnegative integers). Then any nonempty subset* S *of* $\mathbf{N}$ *has a smallest element.*

We start with some elementary definitions:

Definition 2.5 *Let* R *be a commutative ring. Let* $a, b \in R$.

1. *Then* a *is a* ***divisor*** *of* b*, (or* a *a* ***divides*** b*, or* a *is a* ***factor*** *of* b*) iff there is* $c \in R$ *so that* $b = ca$*. This is written as* $a \mid b$.

2. b *is a* ***multiple*** *of* a *iff* a *divides* b*. That is iff there is* $c \in R$ *so that* $b = ac$.

3. *The element* $b \neq 0$ *is a* ***prime***[4]*, also called an* ***irreducible****, iff* b *is not a unit and if* $a \mid b$ *then either* a *is a unit, or* $a = ub$ *for some unit* $u \in R$.

4. *The element* c *of* R *is a* ***greatest common divisor*** *of* a *and* b *iff* $c \mid a$, $c \mid b$ *and if* $d \in R$ *is any other element of* R *that divides both* a *and* b *then* $d \mid c$*. (Note that greatest common divisors are not unique. For example in the integers* $\mathbf{Z}$ *there both* 4 *and* -4 *are greatest common divisors of* 12 *and* 20*, while in the polynomial ring* $\mathbf{R}[x]$ *if element the* $c(x-1)$ *is a greatest common divisor of* $x^2 - 1$ *and* $x^2 - 3x + 2$ *for any* $c \neq 0$.*)*

5. *The elements* a *and* b *are* ***relatively prime*** *iff* 1 *is a greatest common divisor of* a *and* b*. Or what is the same thing the only elements that divide both* a *and* b *are units.*

There are commutative rings where some pairs of elements do not have any greatest common divisors. We now show that this is not the case in Euclidean domains.

Theorem 2.6 *Let* R *be a Euclidean domain. Then every ideal in* R *is principle. That is if* I *is an ideal in* R *then there is an* $a \in R$ *so that* $I = \langle a \rangle$*. Moreover if* $\{0\} \neq I = \langle a \rangle = \langle b \rangle$ *then* $a = ub$ *for some unit* u.

Problem 3 Prove this along the following lines:

[4]I have to be honest and remark that this is not the usual definition of a prime in a general ring, but is the usual definition of an irreducible. Usually a prime is defined by the property of Theorem 2.9. In our case (Euclidean domains) the two definitions turn out to be the same.

1. By the Axiom of induction, Theorem 2.4, the set $S := \{\delta(r) : r \in I, r \neq 0\}$ has a smallest element. Let a be a nonempty element of I that minimizes $\delta(r)$ over nonzero elements of I. Then for any $b \in I$ show that there is a $q \in R$ with $b = aq$ by showing that if $b = aq + r$ with $r = 0$ or $\delta(r) < \delta(a)$ (such q and r exist by the definition of Euclidean domain) than in fact $r = 0$ so that $b = qa$.

2. With a as in the last step show $I = \langle a \rangle$, and thus conclude I is principle.

3. If $\langle a \rangle = \langle b \rangle$ then $a \in \langle b \rangle$ so there is a c_1 so that $a = c_1 b$. Likewise $b \in \langle a \rangle$ implies there is a $c_2 \in R$ so that $b = c_2 a$. Putting these together implies $a = c_1 c_2 a$. Show this implies $c_1 c_2 = 1$ so that c_1 and c_2 are units. HINT: Use that $a(1 - c_1 c_2) = 0$ and that in a Euclidean domain there are no zero divisors. ❑

Theorem 2.7 *Let R be a Euclidean domain and let a and b be nonzero elements of R. Then a and b have at least one greatest common divisor. More over if c and d are both greatest common divisors of a and b then $d = cu$ for some unit $u \in R$. Finally if c is any greatest common divisor of a and b then there are elements $x, y \in R$ so that*

$$c = ax + by.$$

Problem 4 Prove this as follows:

1. Let $I := \{ax + by : x, y \in R\}$. Then show that I is an ideal of R.

2. Because I is an ideal by the last theorem the ideal I is principle so $I = \langle c \rangle$ for some $c \in R$. Show that c is a greatest common divisor of a and b and that $c = ax + by$ for some $x, y \in R$. HINT: That $c = ax + by$ for some $x, y \in R$ follows from the definition of I. From this show c is a greatest common divisor of a and b.

3. If c and d are both greatest common divisors of a and b then by definition $c \mid d$ and $d \mid c$. Use this to show $d = uc$ for some unit u. ❑

Theorem 2.8 *Let R be a Euclidean domain and let $a, b \in R$ be relatively prime. Then there exist $x, y \in R$ so that*

$$ax + by = 1.$$

Problem 5 Prove this as a corollary of the last theorem. ❑

Theorem 2.9 *Let R be a Euclidean domain and let $a, b, p \in R$ with p prime. Assume that $p \mid ab$. Then $p \mid a$ or $p \mid b$. That is if a prime divides a product, then it divides one of the factors.*

Problem 6 Prove this by showing that if p does not divide a then it must divide b. Do this by showing the following:

1. As p is prime and we are assuming p does not divide a then a and p are relatively prime.

2. There are x and y in R so that $ax + py = 1$.

3. As $p \mid ab$ there is a $c \in R$ with $ab = cp$. Now multiply both sides of $ax + py = 1$ by b to get $abx + pby = b$ and use $ab = cp$ to conclude p divides b. ❑

Corollary 2.10 *If p is a prime in the Euclidean domain R and p divides a product $a_1 a_2 \cdots a_n$ then p divides at least one of a_1, a_2, ..., a_n.*

PROOF: This follows from the last proposition by a straight forward induction. ❑

Lemma 2.11 *Let R be a Euclidean domain. Then a nonzero element a of R is a unit iff $\delta(a) = \delta(1)$.*

Problem 7 Prove this. HINT: First note that if $0 \neq r \in R$ then $\delta(1) \leq \delta(1r) = \delta(r)$. Now use the division algorithm to write $1 = aq + r$ where either $\delta(r) < \delta(a) = \delta(1)$ or $r = 0$. ❑

Proposition 2.12 *Let R be a Euclidean domain and a and b nonzero elements of R. If $\delta(ab) = \delta(a)$ then b is a unit.*

Problem 8 Prove this. HINT: Use the division algorithm to divide ab into a. That is there are q and $r \in R$ so that $a = (ab)q + r$ so that either $r = 0$ or $\delta(r) < \delta(a)$. Then write $r = a(1 - bq)$ and use that if x and y are nonzero $\delta(x) \leq \delta(xy)$ to show $(1 - bq) = 0$. From this show b is a unit.) ❑

Theorem 2.13 (Fundamental Theorem of Arithmetic) *Let a be a non-zero element of a Euclidean domain that is not a unit. Then a is a product $a = p_1 p_2 \cdots p_n$ of primes $p_1, p_2, \ldots, p_n$. Moreover we have the following uniqueness. If $a = q_1 q_2 \cdots q_m$ is anther expression of a as a product of primes, then $m = n$ and after a reordering of $q_1, q_2, \ldots, q_n$ there are units $u_1, u_2, \ldots, u_n$ so that $q_i = u_i p_i$ for $i = 1, \ldots, n$.*

Problem 9 Prove this by induction on $\delta(a)$ in the following steps.

1. As a is not a unit the last lemma implies $\delta(a) > \delta(1)$. Let $k : \min\{\delta(r) : r \in R, \delta(r) > \delta(1)\}$. Show that if $\delta(a) = k$ than a is a prime. (This is the base of the induction.)

2. Assume that $\delta(a) = n$ and that it has been shown that for any $b \neq 0$ with $\delta(b) < n$ that either b is a unit or b is a product of primes. Then show that a is a product of primes. HINT: If a is prime then we are done. Thus it can be assumed that a is not prime. In this case $a = bc$ where b and c are not units. a is a product $a = bc$ with both b and c not units. By the last proposition this implies $\delta(b) < \delta(a)$ and $\delta(c) < \delta(a)$. So by the induction hypothesis both b and c are products of primes. This shows $a = bc$ is a product of primes.

3. Now show uniqueness in the sense of the statement of the theorem. Assume $a = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$ where all the p_i's and q_j's are prime. Then as p_1 divides the product $q_1 q_2 \cdots q_m$ by Corollary 2.10 this means that p_1 divides at least one of $q_1, q_2, \ldots, q_m$. By reordering we can assume that p_1 divides q_1. As both p_1 and q_1 are primes this implies $q_1 = u_1 p_1$ for some unit u_1. Continue in this fashion to complete the proof. ❑

3 Modules

3.1 The Definition of a Module

A module is basically a vector space over a ring. While at the level of definitions this seems to be all there is to say, at the deeper level of what theorems hold in vector spaces over fields

as opposed to the results that hold for modules over rings they differ a great deal. As a basic example all vector spaces have a basis, while "most" modules over rings do not. One of the main theorems of this course is that finitely generated (*i.e.* modules spanned by a finite number of elements) over a Euclidean domain have something that is very like a basis.

Definition 3.1 *Let R be a commutative ring. Then M is a* ***module*** *over R (or an R-module) iff M has an operation $+$ of addition and a zero element 0 so that*

1. *The operation $+$ is both commutative and associative. That is*

$$x + y = y + x, \quad x + (y + z) = (x + y) + z$$

   for all $x, y, z \in M$.

2. *For all $x \in M$ we have $0 + x = x + 0 = x$.*

3. *There is an operation of multiplying "vectors" (elements of M) by "scalars" (elements of the base ring R) so that multiplication distributes over addition. If $(r, x) \mapsto rx$ from $R \times M$ is the scalar multiplication map (which is just the high brow way of saying that rx denotes the scalar product of $r \in R$ and $x \in M$. The distributive laws are then*

$$(r_1 + r_2)x = r_1x + r_2y \qquad r(x_1 + x_2) = rx_1 + ry_2.$$

4. *Finally we assume that if 1 is the unit element of R that $1x = x$ for all $x \in M$.*

A submodule of an R module is defined just as a subspace of a vector space is defined.

Definition 3.2 *Let R be a module over the commutative ring R. Then $A \subset M$ is a* ***submodule*** *iff for all $x_1, x_2 \in A$ and $r_1, r_2 \in R$ we have $r_1x_1 + r_2x_2 \in A$. That is A is closed under linear combinations where the scalars come out of the ring R.*

3.2 Examples of Modules

These are easy to come by:

3.2.1 R and its Submodules.

If R is a commutative ring then we can set $M = R$ in the definition of a module and see that R is a module over itself. A subset $A \subseteq R$ is easily checked to be a submodule iff it is an ideal in R.

3.2.2 The Coordinate Space R^n.

Just as in the case of the vector space $\mathbf{F}^n$ of n tuples over a field $\mathbf{F}$ we can start with a commutative ring R and form the space of n tuples of elements of R. That is

$$R := \{(x_1, x_2, \ldots, x_n) : x_1, x_2, \ldots, x_n \in R\}.$$

This is an R module with the usual operations:

$$(x_1, x_2, \ldots, x_n) + (y_1, y_2, \ldots, y_n) = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)$$
$$r(x_1, x_2, \ldots, x_n) = (rx_1, rx_2, \ldots, rx_n).$$

3.2.3 Modules over the Polynomial Ring $\mathbf{F}[x]$ Defined by a Linear Map.

Let $\mathbf{F}$ be a field and V a vector space over $\mathbf{F}$. Let $T : V \to V$ be a linear map from V to V. Using T we can now make V into an module over the ring $\mathbf{F}[x]$. We already know how to add elements of V so we just need to define how to multiple elements of V by elements of $\mathbf{F}[x]$. This is done by the rule

$$f(x) \cdot v := f(T)v.$$

That is if $f(x) = a_0 + a_1x + \cdots + a_nx^n$ first plug T into $f(x)$ to get $f(T) = a_0I + a_1T + \cdots + a_nT^n$ which will also be a linear map $f(T) : V \to V$. Then $f(x) \cdot v$ is the image of v under $f(T)$.

3.3 Direct Sums of Submodules

Definition 3.3 *Let M be a module over the commutative ring R and let $U_1, \ldots, U_n$ be submodules of M. Then $U_1, \ldots, U_n$ are **linearly independent** iff*

$$x_1 + x_2 + \cdots + x_n = 0 \text{ with } x_i \in U_i \quad \text{implies} \quad x_1 = x_2 = \cdots = x_n = 0.$$

Definition 3.4 *Let $U_1, \ldots, U_n$ be submodules of M where M is a module over the commutative ring R. Then there M is a direct sum of $U_1, \ldots, U_n$ iff $U_1 + U_2 + \cdots + U_n = M$ and also $U_1, \ldots, U_n$ are linearly independent. In this case we write either*

$$M = U_1 \oplus U_2 \oplus \cdots \oplus U_n \qquad \text{or} \qquad M = \bigoplus_{i=1}^{n} U_i.$$

Proposition 3.5 *If M is an R module and $U_1, \ldots, U_n$ are submodules so that $M = U_1 \oplus U_2 \oplus \cdots \oplus U_n$ then every element $x \in M$ can be uniquely expressed as $x = x_1 + x_2 + \cdots + x_n$ where $x_i \in U_i$.*

Problem 10 Prove this. ❑