Rings and Modules

Paul Taylor
Trinity College
January 1984

1. Rings

A ring is a structure with notions of addition, subtraction and multiplication, whilst a field has division as well. The addition renders it an Abelian group and is always considered in a "pointwise" fashion. The multiplication may arise (i) pointwise, (ii) by composition or (iii) from an underlying structure. A module is a linear structure upon which something additional acts which itself is equipped with multiplication.

Formally a ring is a set R with elements $0,1$, binary operations $+,*$ and a unary operation $-$ such that

$$0,1 \in R; \quad +,* : R\times R \to R; \quad -: R \to R;$$
$$\left.\begin{array}{l} (a+b)+c = a+(b+c); \quad a*(b*c)=(a*b)*c; \\ a+0 = a = 0+a; \quad a*1 = a = 1*a; \\ a+(-a) = (-a)+a = 0; \\ a+b = b+a; \\ a*(b+c) = (a*b)+(a*c); \quad (b+c)*a = (b*a)+(c*a) \end{array}\right\} \text{ for all } a,b,c \in R$$

Note that $0,1$ need not be distinct: there is a unique (up to isomorphism) ring with $0=1$, namely the zero or singleton ring. Some authors define rings without 1, but this convention is unnatural and archaic.

There are three principal classes of examples of rings besides the basic ones of $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, etc., namely

(i) functions $X \to R$ satisfying certain properties such as continuity or differentiability, where X is a (topological) space and R a ring such as $\mathbb{R}$ or $\mathbb{C}$.

(ii) endomorphisms $V \to V$ of a vector space (possibly with other structure such as an inner product) with composition as multiplication

(iii) linear combinations of elements of a structure possessing its own multiplication, with $(\Sigma_i \lambda_i a_i) * (\Sigma_j \mu_j b_j)$ defined as $\Sigma_{ij} \lambda_i \mu_j (a_i * b_j)$ where $\lambda_i, \mu_j \in R$ (a ring such as $\mathbb{Z}, \mathbb{R}$ or $\mathbb{C}$), and $a_i, b_j \in (X, *)$. Write RX for this. Examples: if $X = (\mathbb{N}, 0, *)$ (where $*$ is actually addition of natural numbers) then $\mathbb{R}\mathbb{N}$ is the ring of polynomials

(usually called $\mathbb{R}[t]$)
in one variable with real coefficients. If $X=(*,1,*)$ is a group, $\mathbb{R}G$ is called the group ring of G over $\mathbb{R}$ and is studied in Part II Representation Theory

A ring is commutative if $a*b=b*a$ for all $a,b\in R$: the examples in (i) are commutative iff R is, those in (ii) are rarely commutative and those in (iii) are iff R and X both are. An element $a\in R$ is invertible or a unit if $a*b=b*a=1$ for some $b\in R$; b is then unique and called the inverse of a, written a^{-1}. The invertible elements of a ring form a group, called the group of units. A field is a commutative ring every nonzero element of which is invertible; Cohn and some other authors do not require commutativity but the terms skew field or division ring are normally used then.

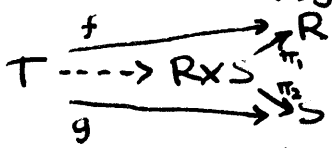
2. Homomorphisms, subrings, ideals and products.

Naturally enough, a homomorphism of rings is a function preserving $0,1,+,*$ and $-$. Hence also the terms endomorphism, monomorphism and isomorphism. Some care should be exercised with the term epimorphism since it does not mean the same as surjective homomorphism. Consider the inclusion $i:\mathbb{Z}\to\mathbb{Q}$ which is plainly not surjective; nevertheless if $f,g:\mathbb{Q}\to R$ are any two ring homomorphisms with $if=ig$ (that is, $f|_{\mathbb{Z}}=g|_{\mathbb{Z}}$) then $f=g$, which property is called being epi[c].

A subring is a subset of a ring including $0,1$ and closed under $+,*,-$. The image of a homomorphism is a subring whilst the inclusion of a subring is a homorphism whose image is the given subring. An intersection of subrings is a subring, so we may speak of the subring generated by a subset; as with groups this consists of the words in $0,1,+,*,-$ and the elements of the subset.

The product of two or more rings is the cartesian product of their underlying set equipped with the componentwise operations. As with sets and groups the product diagram $R\times S \overset{\pi_1}{\to} R$, $R\times S \overset{\pi_2}{\to} S$ is

universal in the sense that if $f: T \to R$, $g: T \to S$ are any two homomorphisms then there's a unique homomorphism (called $(f,g) : T \to R \times S$) such that



commutes. Of course $(t)(f,g) = (tf, tg)$. The product of larger collections of rings is calculated in the obvious way, and that of the empty collection (ie the terminal object) is the zero ring.

The kernel, I, of a homomorphism is the set of elements mapped to zero. This is clearly closed under 0, $+$ and $-$ and also

$$x \in I,\ r \in R \Rightarrow x*r,\ r*x \in I.$$

A subset satisfying these conditions is called a (two-sided) ideal of R. If we merely have $x*r \in I$ it's called a right ideal (likewise left), but since we shall in this course be dealing with commutative rings these terms do not concern us here. Write $I \trianglelefteq R$ and $I \lhd R$ as with groups.

Observe that $1 \in I$ iff $I = R$, so an ideal is not in a general a subring, unlike the case with groups. As with groups and vector spaces, we have a quotient ring R/I for any ideal $I \trianglelefteq R$, so every ideal is a kernel. R/R is the zero ring, whilst $R/0 \cong R$.

If $x \in R$, where R is a commutative ring, the set $\{xr : r \in R\} = \langle x \rangle = xR$ is an ideal, the principal ideal generated by x. In rings such as $\mathbb{Z}$ and $K[t]$ every ideal is principal so these are called Principal Ideal Domains (PIDs).

3. Prime & Maximal ideals and Prime & Irreducible elements.

Consider the ring $\mathbb{Z}[\sqrt{-5}]$ whose elements are of the form $a + \sqrt{-5}b$ with $a, b \in \mathbb{Z}$ and $(a+\sqrt{-5}b)(a'+\sqrt{-5}b') = (aa' - 5bb') + \sqrt{-5}(ab' + a'b)$. Then

$$(1 + \sqrt{-5}.1)(1 - \sqrt{-5}.1) = 6 = 2.3$$

so unique factorisation fails. All four factors are

irreducible, ie $x = ab \Rightarrow$ either a or b is invertible, but they fail to be prime, ie $p \mid ab \Rightarrow p \mid a$ or $p \mid b$. (Of course $x \mid y$ means $\exists z \in R: xz = y$, since from now on we're assuming commutativity throughout). Clearly prime $\Rightarrow$ irreducible but not conversely.

The notion of primeness extends to ideals. We say $P \lhd R$ is prime if $xy \in P \Rightarrow x \in P$ or $y \in P$. Then $p \in R$ is prime iff $\langle p \rangle \lhd R$ is prime.

An ideal M is maximal if $M \neq R$ but $M \lhd I \trianglelefteq R \Rightarrow I = R$. Then maximal $\Rightarrow$ prime, for if $xy \in M$ but $y \notin M$ consider $I = \langle M, y \rangle$, the ideal generated by M and y. The elements of this are of the form $m + yr$ with $m \in M$ and $r \in R$ and since $M \lhd I \trianglelefteq R$ we have $I = R$; so $1 \in I$, say $1 = m + yr$. Then $x = xm + xyr \in M$.

In section 5 we shall discuss quotient rings. Then for a commutative ring R, R/M is a field iff M is maximal, since a commutative ring is a field iff it has no nontrivial ideals whilst the ideals of R/I are exactly of the form J/I with $I \trianglelefteq J \trianglelefteq R$ (also $(R/I)/(J/I) \cong R/J$).

Also, R/P is an integral domain (a commutative ring where $xy = 0 \Rightarrow x = 0$ or $y = 0$) iff P is prime.

4. Zorn's Lemma and the existence of Maximal Ideals.

Discussion of maximal ideals affords a useful opportunity to introduce Zorn's lemma, but don't be fooled by this into thinking that no previous course in the Tripos has used Choice. The equivalence of Zorn's lemma, the Axiom of Choice and the well-ordering principle (every set has a total ordering such that every nonempty subset has a least element) is demonstrated in the Part II Set Theory & Logic course. The result of this section is in fact weaker in the sense that there are models of set theory in which every ring has a maximal ideal but choice fails; there are also models of ZF in which this result fails.

Recall that a <u>partially ordered set</u> or <u>poset</u> is a set X together with a binary relation $(\leq) \subseteq X \times X$ which is reflexive ($x \leq x$), transitive ($x \leq y \leq z \Rightarrow x \leq z$) and antisymmetric ($x \leq y \leq x \Rightarrow y = x$). A <u>total order</u> or <u>chain</u> is a partial order which is <u>trichotomic</u> ($x \leq y$ or $x = y$ or $x \geq y$). <u>Zorn's Lemma</u> states that a poset in which every chain has an upper bound has a maximal (but not necessarily greatest) element.

Apply this to the collection of proper ideals of a ring R, partially ordered by inclusion. Observe that the union of a chain of proper ideals is also a proper ideal, so the conditions are satisfied.

A union of a chain of ideals is an ideal because of the finitary way in which they are defined. For if a, b are in the union they're in some terms, say $a \in I$, $b \in J$. Then either $I \subseteq J$ or $J \subseteq I$ (suppose the former) so $a, b, a+b, ar \in I$ (where $r \in R$). This applies to subgroups of a group, but the following observation does not. The union of a chain of proper ideals cannot be the whole ring since none of the ideals contains 1 (recall $1 \in I \subseteq R \Leftrightarrow I = R$).

In a countable ring (so we have $\varphi : \mathbb{N} \cong R$, a bijection of sets) we may prove the result without choice. For put $I_0 = 0$, the zero ideal, and $M = \bigcup I_n$ where

$$I_{n+1} = \begin{cases} \langle I_n, \varphi(n) \rangle & \text{so long as this is} < R \\ I_n & \text{if } 1 \in \langle I_n, \varphi(n) \rangle \end{cases}$$

Then if $a = \varphi(m) \in R \setminus \bigcup I_n$, it must be because $\langle I_m, a \rangle = R$ whence $\langle M, a \rangle = R$, so M is indeed maximal.

5. Quotient rings and field extensions.

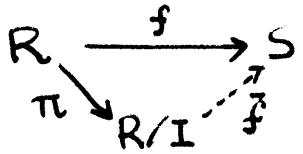
Let R be a commutative ring and I an ideal of it. As with groups and vector-spaces, we construct the quotient, R/I, as the set of cosets with the obvious operations, so

$$(a + I) + (b + I) = (a + b) + I$$

$$(a + I) * (b + I) = ab + I.$$

It is easily verified that R/I is indeed a ring,

and the projection map, $\pi: R \to R/I$ by $a \mapsto a+I$, is a ring homomorphism with the universal property that, if $f: R \to S$ is any homomorphism with $xf = 0$ for all $x \in I$, there is a unique $\bar{f}: R/I \to S$ making the following diagram commute:



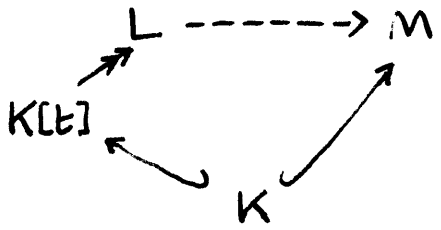
The most familiar example of a quotient ring is arithmetic modulo n. Recall that the set $\{kn : k \in \mathbb{Z}\} = n\mathbb{Z}$ is the principal ideal, $\langle n \rangle \trianglelefteq \mathbb{Z}$. This is prime (indeed maximal) iff n is prime ($\equiv$ irreducible, in $\mathbb{Z}$). Then $\mathbb{Z}/n\mathbb{Z}$ is the ring of integers mod n; it's a field iff n is prime.

The second most important example is where $R = K[t]$, the ring of polynomials in one indeterminate with coefficients in a field K. We shall show later that $\mathbb{Z}$ and $K[t]$ are PIDs and thence that the concepts of prime ideal, maximal ideal, prime element and irreducible element coincide. Then if $f(t) \in K[t]$ is an irreducible polynomial of degree r then $L = K[t]/\langle f \rangle$ is a field, called the <u>extension of K by a root of f</u>.

Consider the composite $K \hookrightarrow K[t] \twoheadrightarrow L$, of which the first factor takes $k \in K$ to the "constant" polynomial $k + 0.t + 0.t^2 + \ldots \in K[t]$. This, like any field homomorphism, is injective, so we may identify K with its image as a subfield of L. The restriction to $L \times K$ of the multiplication $*: L \times L \to L$ renders L a vector-space over K. In this case its dimension is n. Now let α be the image of $t \in K[t]$ in L and consider the polynomial $f(t)$ "multiplied out" in L by substituting α for t and considering the coefficients as elements of L. Then clearly $f(\alpha) = 0$, whence we say α is a <u>root</u> of f in L. Since it generates L over K we ~~write~~ call it $K(\alpha)$

Conversely let M be a field containing K which has an element β such that $f(\beta) = 0$ in the above sense. There is a unique ring homomorphism $K[t] \to M$ which identifies $K \subset K[t]$ with $K \subset M$ and sends t to β, namely by $k_0 + k_1 t + k_2 t^2 + \ldots \mapsto k_0 + k_1\beta + k_2\beta^2 + \ldots$

This clearly maps f, and hence the whole of the ideal $\langle f \rangle$, to zero, so there's a unique homomorphism $L \to M$ making the following diagram commute



and such that $\alpha \mapsto \beta$. Thus L is (isomorphic to) a subfield of M, namely that generated by K and β. Hence $L = K(\beta)$.

There is a familiar example of this with $K = \mathbb{R}$ and $f(t) = 1 + t^2$. We usually write i for α and then $L = \mathbb{C} = \mathbb{R}(i)$.

6. Field of fractions of an integral domain.

The construction of $\mathbb{Q}$ from $\mathbb{Z}$ should be familiar. We shall perform this in the general setting of an integral domain. Note that the assumption of commutativity is vital.

For an integral domain R, let K be the quotient of $R \times R^*$ (where $R^* = R \setminus \{0\}$) by the (equivalence) relation

$$(r,s) \sim (r',s') \quad \text{if} \quad rs' = sr' \text{ in } R$$

In anticipation of the result we shall write (r/s) for the equivalence class of (r,s) under $\sim$, and also $1 = (1/1)$, $0 = (0/1)$.

Now let $(r/s) + (r'/s') = (rs' + sr')/r's'$ and $(r/s) * (r'/s') = (rr'/ss')$. Somewhat tediously it may be verified that $\sim$ is an equivalence relation with respect to which $+$ and $*$ are well-defined, and that $(K, +, *, 1, 0, -)$ is a field, where of course $(r/s)^{-1} = (s/r)$. Moreover $R \hookrightarrow K$ by $r \mapsto (r/1)$

This construction satisfies a (restricted) universal property. If $R \hookrightarrow L$ is a monomorphism into a field, then there's a unique extension $K \hookrightarrow L$ such that $R \overset{K}{\hookrightarrow} L$ commutes. The example of $\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ shows

that the hypothesis of injectivity cannot be dropped.

For want of a better or standard notation, write $f of(R)$ for K, the <u>field of fractions</u> of R.

7. Characteristic, prime subring and finite fields.

For any ring R, there is a unique ring homomorphism $\mathbb{Z} \to R$, so $\mathbb{Z}$ is the <u>initial object</u> in the category of rings. Of course this has $0 \mapsto 0$, $1 \mapsto 1$, $2 \mapsto 1+1$, $3 \mapsto 1+1+1, \ldots, -1 \mapsto -1$, etc. If this map is injective we say R <u>has characteristic zero</u>; some authors will try to persuade you that this makes sense (instead of infinity), but it's really just a (standard) convention. On the other hand, if the kernel is $\langle n \rangle \trianglelefteq \mathbb{Z}$ we say R <u>has char. n</u>. Only the zero ring has char. 1, and the char. of an integral domain is prime. For this reason the image of $\mathbb{Z}$ in R is called the <u>prime subring</u>: it is contained in every other subring. In the case of a field of nonzero characteristic the prime subring is a subfield, but a field of characteristic zero contains (a subfield isomorphic to) $\mathbb{Q}$ and it is then this which we call the <u>prime subfield</u>.

We now more or less have the tools to describe the finite fields, although this will be done properly in Part II Galois Theory. A finite field is a (finite-dimensional) vector space over its (finite) prime subfield, so has order p^n. There is a unique (up to isomorphism) field of each such order, denoted $GF(p^n)$ after its discoverer, or else just $\mathbb{F}_{p^n}$.

Since $K^* = (K \setminus \{0\}, *)$ is a group of order $p^n - 1$, every element of the field satisfies $x^{p^n} - x = 0$ and there is no polynomial equation of strictly lower degree for which this happens [<u>Exercise</u>: why?]. It follows immediately that K^* is cyclic [why?] but we can also use this polynomial to construct the field.

Given any field k and a polynomial $f(t) \in k[t]$, we may extend k to $k(\alpha)$ by adjoining a root of a nontrivial irreducible factor of f (if there is one) as in §5. Doing this repeatedly we eventually obtain a

field in which f splits into linear factors: this is called the splitting field for f over K. As in §5 we may show that it is (isomorphic to) a subfield of any field containing k in which f splits, so it's unique up to isomorphism. Applying this with k the familiar p-element field and $f(t) = t^{p^n} - t$ we deduce the existence and uniqueness of $GF(p^n)$.

8. The Euclidean algorithm

$\mathbb{Z}$ and $K[t]$ are equipped with functions $\mu : R^* \to \mathbb{N}$ (namely absolute value and degree respectively) such that (i) if $x, y \in R^*$ there exist $q, r \in R$ with $x = qy + r$ and either $r = 0$ or $\mu(r) < \mu(y)$, and (ii) if $x, y \in R^*$ then $xy \in R^*$ and $\mu(x) \leq \mu(xy)$. Any integral domain with such a function we shall call a Euclidean Domain since it admits Euclid's algorithm.

Given $x, y \in R^*$ we may apply the division repeatedly, and since the degrees $\mu(r_i)$ of the remainders form a strictly decreasing sequence of natural numbers we must eventually have $r_k = 0$, and we may suppose k is least for which this happens:

$$\begin{aligned}
x &= q_0 y + r_0 && \mu(r_0) < \mu(y) \\
y &= q_1 r_0 + r_1 && \mu(r_1) < \mu(r_0) \\
r_0 &= q_2 r_1 + r_2 && \mu(r_2) < \mu(r_1) \\
&\vdots \\
r_{k-3} &= q_{k-1} r_{k-2} + r_{k-1} && \mu(r_{k-1}) < \mu(r_{k-2}) \\
r_{k-2} &= q_k r_{k-1}
\end{aligned}$$

Proceeding from the last equation to the first we see $r_{k-1} | r_i$ $(0 \leq i \leq k-1)$ and hence $r_{k-1} | x, y$. Conversely if $c | x, y$ then $c | r_0$ and likewise $c | r_i$ $(0 \leq i \leq k-1)$; in particular $c | r_{k-1}$. Hence we call r_{k-1} the highest common factor of x and y, writing $r_{k-1} = (x, y)$ so long as this notation is clear. Note that (x, y) is defined only up to multiplication by a unit (invertible) of R: both 5 and -5 are hcfs of $(15, 35)$ in $\mathbb{Z}$. Also observe that we have defined hcf *before* showing that we have prime factorisation in R.

Now observe that the remainders, (r_i), were defined by adding and subtracting multiples of x, y and so there are $a, b \in R$ (which may without

difficulty be expressed as polynomials in the (q_i) such that $r_{k-1} = ax + by$. This means that $\langle r_{k-1}\rangle \leq \langle x,y\rangle$ but the converse inclusion follows from $r_{k-1} \mid x,y$, so that $\langle x,y\rangle$ is a principal ideal.

In fact every ideal is principal. The zero ideal is trivially so choose $x \in I \setminus \{0\}$ with $\mu(x)$ minimal and let $y \in I \setminus \{0\}$. By hypothesis on R there are $q, r \in R$ with $y = qx + r$ and $r = 0$ or $\mu(r) < \mu(x)$. Since $I \subseteq R$ we have $r \in I$, but if $r \neq 0$ we have a contradiction to the choice of x. Hence $x \mid y$, ie $y \in \langle x\rangle$, and $I = \langle x\rangle$ is principal. Thus Euclidean $\Rightarrow$ PID.

9. Unique Factorisation.

We shall now prove unique factorisation for principal ideal domains (eg $\mathbb{Z}$, $K[t]$) and polynomial rings. So PID $\Rightarrow$ UFD but $\mathbb{Z}[t]$ or $K[t,u]$ are counterexamples to the converse. A unique factorisation domain is an integral domain in which every nonzero element is expressible as a product of primes, uniquely up to permutation and multiplication by units; in particular the notions of irreducible and prime coincide. The latter fact is easily seen to be sufficient to prove uniqueness, so we need to show this and that divisibility is well-founded (ie decomposition must terminate).

Recall that in general a maximal ideal is prime and a prime element is irreducible. Since in a PID the notions of element and ideal coincide, it suffices to show that irreducible $\Rightarrow$ maximal. But clearly if $\langle a\rangle \subsetneq I \subsetneq R$ with a irreducible, $I = \langle b\rangle$ with $b \mid a$ so $\langle a\rangle$ is indeed maximal.

Now suppose $a_0, a_1, \ldots \in R$ with $a_{i+1} \mid a_i$: we must show that the sequence is eventually constant up to multiplication by units. Consider the ideals $I_i = \langle a_i\rangle$: we have $I_0 \subseteq I_1 \subseteq \ldots$ so put $I = \bigcup I_n$; this is a principal ideal so $I = \langle a\rangle$ and $a \in I_n$ for some n. Hence $\langle a_i\rangle = \langle a_n\rangle$ for $i > n$, which is to say $a_i = \varepsilon_i a_n$ for some invertible ε_i.

Now let R be a UFD and consider the polynomial ring $R[t]$: this too is a UFD. By induction the polynomial

ring in any finite number of variables is also a UFD, and since the ring axioms are finitary (infinite sums are not allowed) the result extends to infinitely many generators.

Let $K = \mathrm{fof}(R)$, so that $K[t]$ is a PID and hence a UFD. Well-foundedness of division in $R[t]$ follows from that in $K[t]$, so a factorisation exists. We therefore have only to show that for $f(t) \in R[t]$, if f is reducible (resp. prime) in $K[t]$ then so it is also in $R[t]$. This is Gauss' lemma and it is an easy calculation [Exercise].

10. Chinese Remainder Theorem

It is a familiar fact that if we know a number mod 3 and mod 5 then we know it mod 15. More generally if $I, J \trianglelefteq R$ are comaximal, ie $\langle I, J\rangle \equiv I+J \equiv \{i+j : i\in I,\ j\in J\} = R$, then $R/(I\cap J) = (R/I)\times(R/J)$. There is a map by $a+I\cap J \mapsto (a+I, a+J)$ which is easily seen to be well-defined: we must show that it's an isomorphism. Injectivity is easy and doesn't use the condition $I+J=R$. So let $(a+I, b+J)\in(R/I)\times(R/J)$. Then $a\in R = I+J$ so $a = a'+i$ with $a'\in J$, $i\in I$; similarly $b = b'+j$ with $b'\in I$, $j\in J$. Then $a'+b'+I\cap J$ is mapped to $(a'+I, b'+J) = (a+I, b+J)$ as required.

We may express this in the form that

$$\begin{array}{ccc} R/(I\cap J) & \longrightarrow & R/I \\ \downarrow & & \downarrow \\ R/J & \longrightarrow & R/(I+J) \end{array}$$

is both a pullback and a pushout. Thus if $R/J \leftarrow S \rightarrow R/I$ are two ring homomorphisms whose composites with $R/I \rightarrow R/(I+J) \leftarrow R/J$ are equal then there's a unique $S \rightarrow R/(I\cap J)$ making the triangles commute (pullback). Also $R/J \rightarrow T \leftarrow R/I$ give $R/(I+J) \rightarrow T$ (pushout)

11. Modules.

A module is to a ring what a vector space is to a field, so a module over a ring R is an abelian group $(M,+)$ with an action $R\times M \to M$ such that $1m = m$, $r(m+m') = rm + rm'$, $(r+r')m = rm+r'm$, $0m = 0$, $(rr')m = r(r'm)$ and $(-r)m = -(rm)$. Several results which hold for fields (eg every vector space is free, ie has a basis, and a tensor product of two nonzero vector spaces is nonzero) fail, however, for modules. It is therefore tempting to believe that modules are "inferior" to vector spaces, but this is not the case: in applications the ring R is usually an algebra, ie it contains a field K (centrally), so that an R-module is a K-vector space with additional structure.

A module homomorphism $\theta: M \to M'$ is a function preserving the structure, ie an (abelian) group homomorphism such that $\theta(rm) = r\theta(m)$ [not $\theta(r)\theta(m)$, which doesn't make sense!]. Thus a module homomorphism between vector spaces is simply a vector space homomorphism.

Besides vector spaces, the other major example of modules is Abelian groups. A $\mathbb{Z}$-module is precisely the same thing as an abelian group (and the homomorphisms also coincide).

The first part of the Algebra III course was concerned with the properties of a vector space equipped with a particular endomorphism. This is the same as a $K[t]$-module: hence the relevance of polynomials in that course.

A linear representation of a group G on a vector space V is an assignment of an endomorphism (or matrix) of V to each element of the group in such a way that identity, composition and inverse are preserved, ie a group homomorphism $\rho: G \to GL(V)$. As remarked in §1, the group ring KG consists of K-linear combinations of elements of G. A representation (V,ρ) of G is then precisely a KG-module.

As remarked before, all rings in this course are commutative. In the non-commutative case there are left- and right-modules.

12. Submodules and Quotient Modules, etc.

As usual we may look at the image and kernel of a module homomorphism: these are <u>submodules</u>; ie subsets closed under $0, +, -$; and multiplication by elements of the ring. A ring may be regarded as a module over itself; the submodules of this are precisely the ideals.

As with vectorspaces and abelian groups, every submodule is a congruence (kernel of a homomorphism), and the quotient module is constructed in the obvious way by means of cosets, and has the universal property. Moreover image factorisation holds: let K be the kernel of a module homomorphism $\theta : M \to N$; then θ factorises as $M \twoheadrightarrow M/K \hookrightarrow N$ and the quotient M/K is isomorphic to the image $\theta(M)$.

An intersection of submodules is again a submodule, so we may speak of the submodule generated by a subset. This consists of finite sums of R-multiples of elements of the set (including 0).

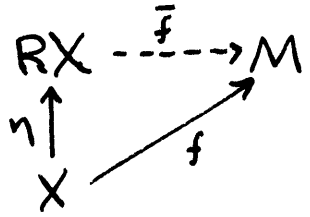
Products of modules exist: they are constructed in the obvious way and satisfy the universal property for products. As with vector spaces the product of two modules is also their coproduct, so this is usually called the <u>direct sum</u>. If a module is generated by a pair of disjoint submodules then it is their direct sum, but (unlike vectorspaces) a submodule need not have a complement.

The above properties may be formalised to give the notion of an Abelian Category, which essentially characterises categories of modules and homomorphisms over rings; these are used in homological algebra.

If M is a module over a ring S and $\varphi : R \to S$ is a ring homomorphism, then M may be regarded as an R-module by $rm = \varphi(r)m$; likewise an S-module homom. gives rise to an R-module homomorphism, preserving identity and composition. This is a functor from Mod-S to Mod-R called Mod-φ; moreover this assignment is itself functorial, except that Mod-$(\varphi\psi) = (\text{Mod-}\psi)(\text{Mod-}\varphi)$.

13. Free modules.

Let R be a (commutative) ring and X a set. Denote by RX the set of (finite) R-linear combinations of elements of X. The obvious (set) map $\eta: X \to RX$ satisfies the universal property that if $f: X \to M$ is any (set) map into an R-module M then there's a unique R-module homomorphism $\bar{f}: RX \to M$ extending f.



RX is then the <u>free</u> R-<u>module on</u> X. The zero module is free on $\emptyset$ whilst $R(X \amalg Y) = RX \oplus RY$. R considered as a module for itself is free on one generator.

Of course a vector space is free on any basis and (with Choice) every vector space has a basis. However not every module is free. There may in particular be <u>torsion elements</u>: $m \in M, r \in R$ with $rm = 0$ with $m \neq 0, r \neq 0$; for example any finite $\mathbb{Z}$-module (Abelian group).

The <u>rank</u> of a free module is the cardinality of a generating set. We know that this is unique for a vector space, but that this is messy to prove. Accordingly to prove it for a ring we must find a way of reducing the result to the known case. We do this for a nonzero ring (with Choice) by considering a maximal ideal $I \lhd R$ so that R/I is a field. IM is a submodule and we show that M/IM is a free R/I-module on X. [<u>Exercise</u>]

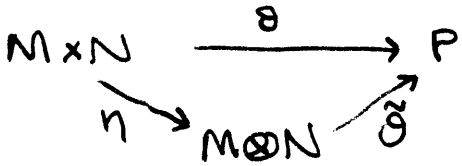
14. Bilinear maps.

A <u>bilinear map</u> is a function $\theta: M \times N \to P$ linear in each variable separately (M, N, P being R-modules). There were many examples of this for vector spaces in Algebra III, but the same abstract idea occurs elsewhere. Consider the commutator map $(x,y) \mapsto [x,y] = x^{-1}y^{-1}xy$ on the quaternion group Q. This is well-defined as a function $Q/2 \times Q/2 \to 2$ where $Q/2$ is the quotient by the centre $2 = Z(Q)$ and $2 = \{\pm 1\}$ is the cyclic group of order 2. $Q/2$ is

an abelian group of order 4 and so may be considered as a module for $\mathbb{Z}$ (or $\mathbb{Z}_2$); moreover $[-,-]: Q/2 \times Q/2 \to 2$ is a (symmetric) bilinear map.

For R-modules N, P let $[N \to P]$ denote the set of R-module homomorphisms from N to P. As in the case of vector-spaces this may be given an R-module structure by pointwise addition and scalar multiplication. Now if $\theta: M \times N \to P$ is bilinear, there is a linear map $\bar{\theta}: M \to [N \to P]$ by $m \mapsto (n \mapsto \theta(m,n))$; indeed the bilinear maps $M \times N \to P$ and the linear maps $M \to [N \to P]$ are in (natural) bijection (with addition and scalar multiplic^n also preserved). The <u>tensor product</u> $M \otimes N$ is a module such that these maps are also in bijection with the linear maps $M \otimes N \to P$.

There is a bilinear map $\eta: M \times N \to M \otimes N$ which is denoted by $(m,n) \mapsto m \otimes n$, so $(r_1 m_1 + r_2 m_2) \otimes n = r_1(m \otimes n) + r_2(m_2 \otimes n)$ etc. (In particular $0 \otimes n = 0$). This has the universal property that any bilinear map $\theta: M \times N \to P$ factors



<u>Exercise</u> (i) any two modules with this property (ie that satisfied by $M \otimes N$ and η) are isomorphic.
(ii) $M \otimes N \cong N \otimes M$ (iii) $M \otimes (N \otimes P) \cong (M \otimes N) \otimes P$
(iv) $R \otimes M \cong M \cong M \otimes R$ (v) $0 \otimes M \cong 0 \cong M \otimes 0$.
(vi) $M \otimes (N \oplus P) \cong (M \otimes N) \oplus (M \otimes P)$

15. <u>Tensor products of vector spaces</u>.

Let us specialise to the case of finite dimensional vector spaces over a field $K = \mathbb{R}$. Choosing a basis, we may represent a vector as a row or column vector of its components, (x_i). A bilinear map is then a matrix (a^{ij}) which is evaluated as $((x_i),(y_j)) \mapsto \sum a^{ij} x_i y_j$: it is a linear function of the matrix $(x_i y_j)$

Let M, N, P above be real vector spaces of dimension m, n, p respectively. $[N \to P]$ has dimension

np from Algebra II and $[M \to [N \to P]]$ has dimension mnp so $M \otimes N$ must have dimension mn. If $({}^{(i)}e_{i'}) = (\delta_{ii'})$ is the i^{th} basis element of M and similarly $({}^{(j)}f_{j'})$ of N then $({}^{(i)}e_{i'}, {}^{(j)}e_{j'})$ is a basis element of $M \otimes N$: it's the matrix with a 1 in the (ij) position and 0 elsewhere.

If $\underline{x} = (x_i)$, $\underline{y} = (y_j)$ we denote the matrix $(x_i y_j)$ by $\underline{x} \otimes \underline{y}$. Not every matrix has this form (this matrix is singular, for instance), but by taking sums of such matrices we generate them all, in other word $\{\underline{x} \otimes \underline{y} : \underline{x} \in M, \underline{y} \in N\}$ span the space $M \otimes N$. Hence it suffices to define a linear map on this subset.

The convention adopted above (with upper and lower suffices) is used in [Part II] General Relativity. A tensor with k upper and l lower suffices is an element of the vector space $(V^* \otimes \cdots \otimes V^*) \otimes (V \otimes \cdots \otimes V)$ with k factors V^* and l factors V, where V is the four-dimensional space representing local space-time and V^* is its dual. According to the <u>summation convention</u>, a suffix occuring once in each of the upper and lower positions has implied summation, according to the <u>evaluation map</u> $V^* \otimes V \to \mathbb{R}$ (otherwise known as the scalar product).

16 <u>Tensor products of modules</u>.

Having seen the structure of the tensor product of two finite dimensional vector spaces, we shall now demonstrate the existence of the tensor product in general. This construction is, however, quite unweildy and entirely unsuitable for calculations: its significance is simply that it exists, and one should not be frightened by it.

As remarked before, the tensor product $M \otimes N$ is spanned (generated) by symbols of the form $m \otimes n$ with $m \in M$, $n \in N$. Take these as *formal* generators of a free R-module F. We want certain equations to hold in $M \otimes N$, so let R be the submodule of F generated by all the expressions of the form

$$(r_1m_1+r_2m_2)\otimes n - r_1(m_1\otimes n) - r_2(m_2\otimes n)$$
$$m\otimes(r_1n_1+r_2n_2) - r_1(m\otimes n_1) - r_2(m\otimes n_2)$$

for $r_1, r_2 \in R$; $m, m_1, m_2 \in M$; $n, n_1, n_2 \in N$. Now $M\otimes N = F/R$ and $\eta: (m,n) \longmapsto m\otimes n = m\otimes n + R$. The universal property should now be verified [exercise].

It is important to notice that the tensor product depends on the ring R. For example let $M = \{p+q\sqrt{2} : p,q \in \mathbb{Q}\}$, which has dimension 2 over $\mathbb{Q}$ and 1 over $\mathbb{Q}(\sqrt{2})$. In $M\otimes_{\mathbb{Q}} M$ there are elements $\sqrt{2}\otimes 1$ and $1\otimes\sqrt{2}$ which are not equal since "we can't pass $\sqrt{2}$ through the $\otimes$"; $M\otimes_{\mathbb{Q}} M$ has dimension 4 over $\mathbb{Q}$, having basis $1\otimes 1$, $\sqrt{2}\otimes 1$, $1\otimes\sqrt{2}$ and $\sqrt{2}\otimes\sqrt{2}$ (it cannot be made into a $\mathbb{Q}(\sqrt{2})$ module). $M\otimes_{\mathbb{Q}(\sqrt{2})} M$ has dimension 1 over $\mathbb{Q}(\sqrt{2})$ and hence 2 over $\mathbb{Q}$, since it is isomorphic to M.

In general let M, N be S-modules and $\theta: R \to S$ be any ring homomorphism. M, N may therefore be regarded as R-modules as in §12, ie $rm = \theta(r)m$ etc. The S-bilinear map $M\times N \to M\otimes N$ is then R-bilinear, so there's an R-linear $M\otimes_R N \to M\otimes_S N$ (in the above example this takes the basis elements to $1, \sqrt{2}, \sqrt{2}, 2$ respectively times the unique basis element $1\otimes 1$ of $M\otimes_{\mathbb{Q}(\sqrt{2})} M$). This map is always surjective [why?]. If θ is an inclusion of fields of dimension n then this quotient map reduces the dimension by a factor of n.

Finally we shall consider the example of two Abelian groups ($\mathbb{Z}$-modules), for simplicity two cyclic groups (the general case will become apparent in due course). Let the orders be m, n and let the hcf of these be c. $m\otimes n$ is generated by $1\otimes 1$ [why?] and so is cyclic. If $c = pm + qn$ then $c(1\otimes 1) = pm(1\otimes 1) + qn(1\otimes 1)$ $= p(m\otimes 1) + q(1\otimes n) = 0$, but on the other hand there's a bilinear map $m\times n \to c$ so c (ie $\mathbb{Z}_c$) is indeed the tensor product. In particular if m, n are coprime their tensor-product is trivial.

17. Symmetric and Skew-symmetric bilinear maps.

From now on the two modules will coincide. We may then consider symmetric and antisymmetric bilinear

maps $M \times M \to N$, ie such that $\theta(m_1, m_2) = \pm\theta(m_2, m_1)$. In the symmetric case (the antisymmetric case is simpler) $m_1 \otimes m_2$ and $m_2 \otimes m_1$ are mapped to the same element of N, so the linear map $M \otimes M \to N$ factors through the quotient by the submodule generated by $\{m_1 \otimes m_2 - m_2 \otimes m_1 : m_1, m_2 \in M\}$. This is called the symmetric square of M and is denoted by $S^2(M)$; it satisfies the same universal property as $M \otimes M$ but for symmetric bilinear maps. In the antisymmetric case we have the alternating square, $\Lambda^2(M)$.

$S^2(M)$ and $\Lambda^2(M)$ may also be seen as submodules of $M \otimes M$, generated by $\frac{1}{2}(m_1 \otimes m_2 + m_2 \otimes m_1)$ and $\frac{1}{2}(m_1 \otimes m_2 - m_2 \otimes m_1)$ respectively, so long as $\frac{1}{2}$ (ie the multiplicative inverse of $2 = 1+1$) exists in R. In this case $M \otimes M \cong S^2(M) \oplus \Lambda^2(M)$. For a vector space over a field of characteristic other than 2, the dimensions of $M \otimes M$, $S^2(M)$ and $\Lambda^2(M)$ are respectively n^2, $\frac{1}{2}n(n+1)$ and $\frac{1}{2}n(n-1)$ where M has dimension n. [Exercise]

We may of course take more than two factors, and since the products are associative up to isomorphism we may unambiguously write $\otimes^r M$, $S^r M$ and $\Lambda^r M$ for these, where for $r = 0, 1$ all three are taken to be R, M respectively. If M is a vector space of dimension n, the dimensions are n^r, $n(n+1)\ldots(n+r-1)/r!$ and $\binom{n}{r}$ respectively. In particular $S^3 M \oplus \Lambda^3 M \neq \otimes^3 M$, $\Lambda^{n-1} M \cong M^*$ and $\Lambda^n M \cong R$ [Exercise]. The second of these (if $n=3$) gives rise to the vector product from Part IA Vector Calculus, whilst the last gives rise to the determinant.

18 Determinants

The foregoing definitions are functorial, which means that they apply to homomorphisms as well as objects (modules). Given a linear map $\theta : M \to N$ we can construct $\theta \otimes \theta : M \otimes M \to N \otimes N$ by $m_1 \otimes m_2 \longmapsto \theta(m_1) \otimes \theta(m_2)$ [Exercise: why is this well-defined?] and likewise $\otimes^r \theta$, $S^r \theta$ and $\Lambda^r \theta$. In particular,

if $M=N$ and $r=n=\dim M$, there is a map $\Lambda^n\theta : \Lambda^n M \to \Lambda^n M$. However this is a linear endomorphism of a 1-dimensional vector space, which is simply multiplication by a scalar. This scalar is called the <u>determinant</u>, $\det\theta$.

The most obvious thing about det from this definition is that it preserves products. This follows immediately from the functoriality: a functor preserves identity and composition, so easily $\det 1=1$ and $\det(\alpha\beta)=(\det\alpha)(\det\beta)$. An invertible endomorphism therefore has nonzero determinant.

We must show that this definition coincides with the one from Algebra II, which said that the determinant of a matrix is a (the) alternating multilinear function of the rows such that $\det 1=1$. We've implicitly chosen a basis, so $M=K^n$; the rows are $r_1, r_2, \ldots, r_n \in M$ so we have an alternating multilinear $M\times\ldots\times M\to K$, ie a linear $M\wedge M\wedge\ldots\wedge M\to K$. But as remarked, $\Lambda^n M$ is one-dimensional, so this is unique up to scalar multiplication, and $\det 1=1$ fixes it. Thus the definitions coincide and are well-defined.

It remains to show that an endomorphism with nonzero determinant is invertible. But an endomorphism of a finite dimensional vector space is invertable iff it has full rank. Suppose $\theta: M\to M$ does not have full rank, so its image $N\leq M$ has dimension strictly less than n. Then we have $\Lambda^n\theta : \Lambda^n M\to\Lambda^n N$ but $\Lambda^n N=0$ so this is the zero map and $\det\theta=0$

There are some Tripos questions demanding explicit calculation of $\Lambda^n\theta$: you will find that this is precisely the same as the usual calculation of $\det\theta$.

A subring of a Nötherian ring need not be Nötherian.

Let $J \subset R$ consist of 0 and the leading coefficients of polynomials in I; then $J \subset k[x_1, \ldots, x_{n-1}]$. By hypothesis it's finitely generated, say by $b_1, \ldots, b_m$ where these are the leading coefficients of some $f_1, \ldots, f_m \in I$ of degree at most n. Now any polynomial in I can be expressed as an $k[x_1, \ldots, x_{n-1}]$-linear combination of the $f_1, \ldots, f_m$ together with a polynomial in I of degree strictly less than n. Consider now the set J_{n-1} consisting of 0 and the leading coefficients of polynomials in I of degree at most $n-1$; this is an ideal and so finitely generated, say by $b_{m+1}, \ldots, b_{m'}$ which are the leading coefficients of polynomials $f_{m+1}, \ldots, f_{m'}$ of degree at most $n-1$. By means of these, any polynomial in I may be reduced to degree at most $n-2$. Proceeding in the obvious fashion we obtain a finite list of generators for I.

Now if A is a finitely (say n) generated R-algebra with R Noetherian, then it is a quotient of $R[x_1, \ldots, x_n]$, which is Noetherian by the above and obvious induction, and hence itself Noetherian. For example $\mathbb{Z}$ is a PID and so it and its polynomial rings $\mathbb{Z}[x_1, \ldots, x_n]$ are Noetherian. Hence Noetherian $\not\Rightarrow$ UFD; on the other hand $\mathbb{Z}[x, xy, \ldots]$ is UFD but not Noetherian, however since $\mathbb{Z}$ is Noetherian one can show that every irreducible is prime so it is UFD.

Noetherian rings are important in algebraic geometry, where the number of generators gives a notion of dimension.

21. Cyclic decompositions of Modules

The first result in the course is that any finitely generated module over a PID is a direct sum of cyclic submodules (ie generated by one element). Recall that $\mathbb{Z}$ and $K[t]$ are PIDs and that their modules are respectively Abelian groups and vector spaces equipped with a particular endomorphism, so this says that a finite Abelian group is a direct sum of cyclic groups whilst an endomorphism of a vector space has a matrix (wrt some basis) which is a direct sum of cyclic matrices, which

one block of the form

[rational] $\begin{pmatrix} C & 1 & & \\ & C & 1 & \\ & & C & \\ & & & \ddots \\ C & & & & 0 & 1 \\ a_0 & a_1 & a_2 & \cdots & a_{k-2} & a_{k-1} \end{pmatrix}$ [Jordan] $\begin{pmatrix} \lambda & 1 & & \\ & \lambda & 1 & \\ & & \lambda & \\ & & & \ddots \\ 0 & & & & \lambda & 1 \\ & & & & & \lambda \end{pmatrix}$

Moreover we can specify the constituents uniquely in either of the forms: (i) successive elementary divisors or (ii) prime power which give rise respectively to the rational and Jordan canonical form for matrices.

Let M be generated by x and let $I = \{r \in R : rx = 0\}$ be the set of annihilators of x, ie $\{r \in R : rx = 0\}$ then $I = \langle z \rangle$ for some $z \in R$, which is called the order of x (or M). For $R = \mathbb{Z}$, M is a cyclic group with generators of order z, where $z = 0$ gives the infinite cyclic group $\mathbb{Z}$. For $R = K[t]$, M is a vector space with basis $x, tx, t^2x, \ldots$ and z is the minimum polynomial of x; thus x has the rational matrix above. Alternatively, if $z = (t-1)^n$ x has matrix of the Jordan form wrt some basis. In the successive divisor form, the constituents are ~~etc~~ ordered s.t. $z_i \mid z_{i+1}$ for each i. We prove this form and easily deduce the prime power form.

The largest z in the sequence is the exponent of M, ie the generator of $\{r \in R : rm = 0 \text{ for all } m \in M\}$. The strategy is to prove that there is some element of this order and that the submodule it generates is a direct summand (has a complement). The same method is applied to the complement and so on; by finite generation the process must terminate. The choice of summands is not determined uniquely, but the sequence of orders (in either of the two forms) is unique.

22. Torsion and Torsion-free Modules.

A torsion element of a module is one with nonzero order; a module is torsion or periodic if every element is torsion and is torsion-free if zero is the only torsion element. The torsion elements of a module form a submodule the quotient by which is torsion-free [easy exercise]. We shall show that (for a finitely generated module over a PID) is both free and a direct summand; also, a submodule of a

finitely-generated free module over a PID is free of no bigger rank. Recall that the rank of a free module over a nonzero ring is well-defined (§13)

Simply by choosing inverse images of the generators, if a free module is a quotient of a module then it's a direct summand. More generally, a module P is <u>projective</u> if whenever we have $M \twoheadrightarrow N \leftarrow P$ then there's some $P \to M$ (not necessarily unique) s.t. the triangle commutes. A <u>retract</u> of a module is the image of an idempotent endomorphism; a module is projective iff it is a retract of a free module [exercise].

Let R be a PID, F a free R-module of rank n and S a submodule of F. For $n=1$, $F \cong R$ and $S \lhd R$ so $S = \langle \mu \rangle$ and is free on this one generator, so suppose the result for smaller values of n. Then $F \cong R^n$ so let $\theta : F \to R$ be the projection on the first component; its kernel is free on $n-1$ generators. The image S_1 of S under θ is free on at most one generator, and its kernel S_0, being a submodule of R^{n-1}, is free on at most $n-1$ generators. By the previous result $S \cong S_0 \oplus S_1$ and is free on at most n generators.

Let R be a PID and F a torsion-free R-module which is finitely-generated. Let $K = \mathrm{fof}(R)$ and $V = K \otimes_R F$ (eg for $R = \mathbb{Z}$ and F a lattice = f.g. torsion-free $\mathbb{Z}$-module, $K = \mathbb{Q}$ and V consists of "fractional" lattice points) so V is a finite-dimensional vector space with basis $v_1, \ldots, v_n$. Each of these is a rational (ie K-) multiple of an element of F, so wlog $v_1, \ldots, v_n \in F$. They generate a free submodule G of F, which is such that for each $a \in F$ there's some $r \in R^*$ with $ra \in G$. Hence there's some $r \in R^*$ such that $ra \in G$ for every one of the original generators (and hence every element) $a \in F$. Multiplication by r embeds F as a submodule of G which is free by the previous result; this multiplication is injective since F is torsion-free.

The rank of the free component of a finitely generated Abelian group is called its Betti number; if the group arose as the n^{th} Homology group of a topological space X then this counts the "n-dimensional holes" of X. We are left with the problem of classifying torsion finitely generated modules over a PID, in which case the exponent is well-defined and nonzero.

23. Cyclic decomposition concluded.

Let M be a module of exponent $\mu \neq 0$ for a PID R. We have to show that M has an element a of order μ and that $C = \langle a \rangle$ is a direct summand of M.

Let $\mu = u p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ where $p_1, \dots, p_k$ are non-associate (ie not ~~invertible~~ mutual multiples) primes, u is invertible and $\alpha_1, \dots \alpha_k \in \mathbb{N}$. This decomposition and its uniqueness were shown in §9. By definition of μ (as the lcm of the orders of nonzero elements) there are elements $a_1, \dots, a_k$ of orders $p_1^{\alpha_1} m_1, p_2^{\alpha_2} m_2, \dots, p_k^{\alpha_k} m_k$; taking suitable multiples, viz. $m_1 a_1, \dots, m_k a_k$, w.l.o.g. $m_1 = \dots = m_k = 1$. Then $a = a_1 a_2 \dots a_k$ has order $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, ie μ (the order is defined only up to multiplication by invertibles).

In order to prove that C is a direct summand of M, and hence complete the proof of the decomposition, it suffices to prove that C is <u>injective</u> in the category of [finitely generated] $R/(\mu)$ modules, ie if $A \hookrightarrow B$ is an inclusion of [f.g.] R-modules in which $\mu b = 0$ for all $b \in B$ (and so $\mu a = 0$ for all $a \in A$) then any $A \to C$ extends to some $B \to C$, for which it suffices to show ~~that~~ for $B = \langle A, b \rangle$; for applying this successively to $C \hookrightarrow \langle C, m_1 \rangle \hookrightarrow \dots \langle C, m_1, \dots, m_k \rangle = M$ we obtain $M \to C$ whose kernel is a complement for C in M.

Let $C \xleftarrow{\varphi} A \hookrightarrow \langle A, b \rangle = B$ as above, so B/A is cyclic with generator $b + A$ of order ν dividing μ, say $\mu = \nu\lambda$. Then $b\nu \in A$ and $\varphi(b\nu)$ is an element of C of order dividing λ, whence it can be written ~~(uniquely)~~ as $c\nu$ for some $c \in C$ (not necessarily the generator). Let $\psi : A \oplus R \to C$ by $a \mapsto \varphi(a)$ and $r \mapsto rc$, so that in the diagram

$$R \xrightarrow{j} A \oplus R \xrightarrow{\theta} B \qquad \text{where } j(r) = rb\nu - r\nu$$
$$\downarrow \psi$$
$$C$$

$R \to A \oplus R \to B$ and $R \to A \oplus R \to C$ are both zero, $A \oplus R \to B$ is surjective and so if we can show that R is the kernel of $A \oplus R \to B$ it will follow that the latter factorises through $A \oplus R \to C$, giving the required extension of $A \to C$. If $\theta(a + s) = 0$, ie $a + sb = 0$ then $sb \in A$, so $\nu | s$ by definition of ν, say $s = \nu r$; then $a + s = rb\nu - r\nu = j(r)$ so $R \to A \oplus R \to B$ is exact at $A \oplus C$. $j : R \hookrightarrow A \oplus R$ since R is an integral domain, so multiplication by ν has zero kernel.

This completes the proof of the existence of the decomposition – uniqueness is outside the course.