MA3201 Rings and Modules, 2014

Syllabus

The syllabus of the course is

Chapter 9	All sections
Chapter 10	All sections
Chapter 14	14.1-14.5
Chapter 19	19.1-19.3
Chapter 20	All sections
Chapter 21	All sections

from the book:

Bhattacharya, P. B.; Jain, S. K.; Nagpaul, S. R. Basic abstract algebra. Second edition. Cambridge University Press, Cambridge, 1994,

with the modifications and additions given below.

Chapter 9

Our definition of rings differs from the book: we assume that all rings have a multplicative identity element, i.e. an element 1_R in the ring R such that $1_R a = a 1_R = a$ for all $a \in R$.

Integral domains, division rings and fields must all be non-zero rings.

Since we assume our rings to have a multiplicative identity, we define a subring of a ring as in the book, but with the additional property that the multiplicative identity element of the ring lies in the subring.

We did not discuss boolean rings, the ring of formal Laurent series, or the group algebra of a group.

Chapter 10

Since we assume rings have a multiplicative identity, the expressions for ideals generated by elements in a ring on page 183 have a simpler form.

In our setup, a ring homomorphism from R to S must send 1_R to 1_S. So, for example, the only ring homomorphism from $\mathbb{Z}$ to $\mathbb{Z}$ is the identity homomorphism.

The sum $A + B$ considered in Examples 3.4 on p199 is not in general a ring in our setup, as it may not have a multiplicative identity element.

We did not consider comaximal ideals (page 203).

We omitted the proofs of Theorem 1.2 on page 181 (although we did consider the case when R is a field), Theorem 2.5 on page 191, Theorem 4.2 on p204, Theorem 4.6 on p206, Theorem 4.7 on page 207. We omitted Theorem 2.4 on page 190.

Chapter 11

We needed some material from Chapter 11 in order to discuss Chapters 20 and 21: Units; irreducible and prime elements; that if an element in a commutative integral domain is prime then it is irreducible, with proof; that in a principal ideal domain (PID) an irreducible element is prime (without proof); unique factorization domains (UFDs); associates; unique factorization in a UFD (without proof); that every PID is a UFD (without proof); greatest common divisors (gcds); existence of gcds in a UFD and uniqueness up to multiplication by a unit (without proof); the following result (Lemma 6.12 from lectures):

Lemma. Let R be a PID and $a, b \in R \setminus \{0\}$. Then there are $s, t \in R$ such that $sa + tb = gcd(a, b)$.

Proof. Let $d \in R$ be such that $(d) = (a, b)$ (where (a, b) is the ideal generated by a and b). Since $a \in (d)$ we have $d|a$. Since $b \in (d)$, we have $d|b$. Suppose $c|a$ and $c|b$. Then $a \in (c)$ and $b \in (c)$, so $(a, b) \subseteq (c)$. Hence $(d) \subseteq (c)$, so $c|d$.

Therefore, d is a gcd of a and b. Since $d \in (a,b)$, there are $s,t \in R$ such that $d = sa+tb$. Any other gcd of a and b is an associate of d, so has the same property. □

Chapter 14, Sections 1–5

Note that for a module M in our setup, we include the axiom $1_R m = m$ for all $m \in M$.

We did not consider exact sequences (page 259). We used the term *semisimple* instead of *completely reducible* in Section 14.4 (page 260 and onwards).

We omitted the proofs of Theorem 5.1 on page 265, Theorem 5.3 on page 265, Theorem 5.4 on page 265. We omitted Theorem 5.2 on page 265.

Chapter 19, Sections 1–3

We did not discuss finitely cogenerated modules (page 368) or the proof of Theorem 2.2 on page 370.

For us, a ring is noetherian if it is both left and right noetherian, not as in the book, and similarly a ring is artinian if it is both left and right artinian.

We called the rings satisfying the equivalent conditions in Theorem 3.6 on page 386 *semisimple* (rather than *semisimple artinian* as in the book).

We omitted Theorems 2.7, 2.8 on page 375, Lemma 2.10 and Theorem 2.11 on page 374, Theorem 2.12 on page 375, the Hilbert Basis Theorem (Theorem 2.14 on page 375), Maschke's Theorem (Theorem 3.5 on page 385) and Theorem 3.8 on page 387.

Chapter 20

We omitted the proof of Lemma 1.1.

A remark was made on how the Smith Normal Form can be obtained in the case of $\mathbb{Z}$ and $\mathbb{F}[x]$, $\mathbb{F}$ a field - more details now follow.

Suppose we are given $A \in M_{m,n}(\mathbb{Z})$. If every entry of A is zero, we are done. If not, we find a_{ij} with $|a_{ij}|$ minimal and apply row and column exchanges to move the entry to the top left corner of A. We then try to reduce the first row of the matrix to zeros.

Step 1: If $a_{1t} \neq 0$ and $a_{11}|a_{1t}$ for some $t \neq 1$, we can apply:

$$C_t - \frac{a_{1t}}{a_{11}} C_1$$

to reduce this entry to zero. We do this for all possible t.

Step 2: If there is still some non-zero entry a_{1t} in A with $t \neq 1$, we write $a_{1t} = qa_{11} + r$ where $0 < r < |a_{11}|$. We then apply the operations:

$$C_t - qC_1, \qquad C_1 \leftrightarrow C_t$$

which reduce the entry a_{1t} to r and swap it into the $(1,1)$ position.

Repeating Steps 1 and 2, we must have $a_{12} = \cdots = a_{1n} = 0$ after finitely many iterations, since in Step 2 the absolute value of the $1,1$ entry decreases.

We apply the same procedure to the first column. Note that while doing this, we may swap rows so that the first row has non-zero entries again (apart from the $1,1$ entry). We therefore repeat the first step, clearing the first row again (making $a_{12} = \cdots = a_{1n} = 0$), then the first column, and so on.

Since the absolute value of the $1,1$-entry decreases each time we go back to the first row, this process must terminate after finitely many steps, with the first row and column cleared, i.e. with $a_{12} = \cdots = a_{1n} = 0$ and $a_{21} = \cdots = a_{m1} = 0$. The rest of the algorithm is as in the general PID case considered in lectures and the book. In particular, at the end of the proof, when we need to reduce a matrix:

$$\begin{pmatrix} a_1 & & & & \\ & a_2 & & & \\ & & \ddots & & \\ & & & a_k & \\ & & & & \\ & & & & \end{pmatrix}$$

where $a_1 \nmid a_2$, we apply $R_1 + R_2$ and then apply the whole of the above procedure. Each time we do this, $|a_1|$ decreases in value, so eventually we reach a point where $a_1|a_2$ (since this is true for $a_1 = \pm 1$).

A similar approach can be used for $\mathbb{F}[x]$, using the degree function instead of absolute value. In general this approach works for any Euclidean domain (see page 217, Section 11.3 of the book for the definition, and the solution to Problem 2 on Problem Sheet 6). We get an explicit algorithm, while for a general PID the proof is not constructive (as the elements s, t in the Lemma stated in the section on Chapter 11 above are not constructed explicitly by the proof, although we note that for a Euclidean domain they could be computed using the Euclidean algorithm).

Chapter 21

In Section 2 we considered only the statement of Theorem 2.3, and not its proof. An extra proposition was used in the discussion of the Jordan canonical form, and there was some extra discussion of characteristic and minimal polynomials; see below for both.

Proposition 9.1. Let R be a PID and let $r, s \in R$, with $\gcd(r, s) = 1$. Then:

$$\frac{R}{(rs)} \cong \frac{R}{(r)} \oplus \frac{R}{(s)}.$$

Proof. Define a map

$$\varphi : R \to \frac{R}{(r)} \oplus \frac{R}{(s)}$$

by sending $x \in R$ to $(x + (r), x + (s))$. Then it is easy to show that φ is an R-homomorphism. If $\varphi(x) = 0$ then $x \in (r) \cap (s)$, so $x = rp = sq$ for some $p, q \in R$. Since $\gcd(r, s) = 1$, we have, by Lemma 6.12 in lectures, that there are $a, b \in R$ such that $ar + bs = 1$. Then

$$x = 1x = arx + bsx = arsq + bsrp,$$

so $x \in (rs)$. If $x \in (rs)$ then $x \in (r) \cap (s)$ so $\varphi(x) = 0$. Hence $\ker(\varphi) = (rs)$.

Let

$$(x + (r), y + (s)) \in \frac{R}{(r)} \oplus \frac{R}{(s)}.$$

Then

$$x - y = (x - y)(ar + bs) = (x - y)ar + (x - y)bs,$$

so

$$z = x - (x - y)ar = y + (x - y)bs.$$

We have

$$\varphi(z) = (x - (x - y)ar + (r), y + (x - y)bs + (s)) = (x + (r), y + (s)).$$

Hence φ is onto. By the Fundamental Theorem of R-Homomorphisms,

$$\frac{R}{\ker(\varphi)} \cong \mathrm{im}(\varphi),$$

giving the result. □

Characteristic and minimal polynomials:

Definition 8.4. Let $\mathbb{F}$ be a field and $A \in M_n(\mathbb{F})$. Then $c_A = \det(A - xI_n)$ is the *characteristic polynomial* of A. It is nonzero, has degree n, and the coefficient of the highest degree term is $(-1)^n$.

If V is an n-dimensional $\mathbb{F}$-vector space and $T : V \to V$ is a linear transformation, then the *characteristic polynomial* of T is $c_T = c_A$, where $A = M_B^B$ is the matrix representing T for some basis B of V.

Remark 8.5. The characteristic polynomial c_T is independent of the choice of basis B: If $A' = M_{B'}^{B'}(T)$ for some basis B' of V, then $A' = P^{-1}AP$ for some invertible matrix P. So

$$\begin{aligned} c_{A'} &= \det(A' - xI_n) \\ &= \det(P^{-1}AP - P^{-1}IP) \\ &= \det(P^{-1}(A - xI_n)P) \\ &= \det(P)^{-1}\det(A - xI)\det(P) \\ &= \det(A - xI_n) = c_A. \end{aligned}$$

If $f \in \mathbb{F}[x]$, $f = a_0 + a_1x + \cdots + a_nx^n$, then $f(A)$ is defined to be

$$f(A) = a_0 + a_1A + \cdots + a_nA^n,$$

and $f(T)$ is defined to be

$$f(T) = a_0 + a_1T + \cdots + a_nT^n.$$

We have seen in the proof of Theorem 8.1 in lectures (Smith Normal Form) that there are invertible $n \times n$ matrices P, Q such that

$$P(A - xI_n)Q = \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & f_1 & & \\ & & & & \ddots & \\ & & & & & f_k \end{pmatrix} = D,$$

where $f_1|f_2|\cdots|f_k$ are the nonunit invariant factors of $A - xI_n$. Note that we can always apply the operations uR_i, for a unit u, to ensure that the units in the Smith Normal Form are reduced to 1 as above and the f_i are monic.

We have

$$\det(P)\det(A - xI_n)\det(Q) = \det(D) = f_1 \cdots f_k.$$

Hence, noting that $\det(P)$ and $\det(Q)$ are units, we have:

Theorem 8.6. Let A be an $n \times n$ matrix and $f_1, \dots, f_k$ the non-unit invariant factors of $A - xI_n$, chosen to be monic. Then the characteristic polynomial of A satisfies:

$$c_A = f_1 \cdots f_k u,$$

where $u \in \mathbb{F}[x]$ is a unit (i.e. an element of $\mathbb{F} \setminus \{0\}$). In fact, since the f_i are monic, u is the leading term of c_A, which is $(-1)^n$.

Theorem 8.7. Let V be an $\mathbb{F}$-vector space and $T : V \to V$ a nonzero linear transformation. Let $A = M_B^B(T)$, where B is a basis of V. Let $f_1|f_2|\cdots|f_k$ be the non-unit invariant factors of $A - xI_n$, chosen to be monic. Then $f_k(T) = 0$ and $f(T) = 0$ if and only if $f \in (f_k)$. Furthermore, $f_k(A) = 0$ and $f(A) = 0$ if and only if $f \in (f_k)$.

Proof. We have seen that (Theorem 4.1, page 411):

$$V \cong \frac{\mathbb{F}[x]}{(f_1)} \oplus \cdots \oplus \frac{\mathbb{F}[x]}{(f_k)}.$$

So

$$V = \{(g_1 + (f_1), \dots, g_k + (f_k)) \,:\, g_i \in \mathbb{F}[x], i = 1, \dots, k\}.$$

Let $f \in \mathbb{F}[x]$. Then $f(T) = 0$ if and only if $f(T)v = 0$ for all $v \in V$. This is equivalent to $f(v) = 0$ for all $v \in V$. This is equivalent to

$$f(g_1 + (f_1), \dots, g_k + (f_k)) = (0 + (f_1), \dots, 0 + (f_k))$$

for all $g_i \in \mathbb{F}[x]$, $i = 1, \dots, k$.

This is equivalent to

$$f(1 + (f_1), \dots, 1 + (f_k)) = (0 + (f_1), \dots, 0 + (f_k)),$$

which is equivalent to $f \in (f_i)$ for $i = 1, \dots, k$. This is equivalent to $f \in (f_k)$, since

$$(f_k) \subseteq (f_{k-1}) \subseteq \cdots \subseteq (f_1).$$

The second statement follows from the first. □

Definition 8.8. In the situation of Theorem 8,7, the invariant factor f_k is called the *minimum polynomial* m_T of T. It is the monic polynomial of minimal degree such that $f(T) = 0$. Similarly, f_k is the minimum polynomial of $A = M_B^B(T)$.

Corollary 8.9. Let $T : V \to V$ be a nonzero linear transformation. Then $m_T | c_T$.

Proof. We have $m_T = f_k$ and $c_T = f_1 \cdots f_k$. □

Theorem 8.10. (Cayley Hamilton Theorem)
Let $A \in M_n(\mathbb{F})$. Then $c_A(A) = 0$.

Proof. We have

$$\begin{aligned} c_T(A) &= (f_1 \cdots f_k)(A) \\ &= f_1(A) \cdots f_k(A) = 0, \end{aligned}$$

since $f_k = m_A$. □

For example, if $A = \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}$, then

$$c_A = \det \begin{pmatrix} 1 - x & 2 \\ 1 & 3 - x \end{pmatrix} = (1 - x)(3 - x) - 2 = x^2 - 4x + 1.$$

We can check that

$$c_A(A) = A^2 - 4A + I_2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Finally, some information on quivers and differential equations, not covered in the book.

1. Quivers

1.1. **Path algebra of a quiver.** : A *quiver* Q is a directed graph, i.e. a pair $Q = (Q_0, Q_1)$ consisting of vertices Q_0 and a set of arrows Q_1 between them. We will consider only finite quivers, i.e. quivers Q in which Q_0 and Q_1 are both finite.

For example:

(1)

$$1 \qquad 2$$

(2)

$$1 \xrightarrow{\alpha} 2$$

(3)

$$1 \xrightarrow{\alpha} 2 \xrightarrow{\beta} 3$$

(4)

$$\begin{tikzcd} 1 \arrow[r, bend left] \arrow[r, bend right] \arrow[rr, bend left=40] & 2 & 3 \arrow[l] \end{tikzcd}$$

Given a quiver Q and a field $\mathbb{F}$, we can form the *path algebra* $\mathbb{F}Q$. We take a vector space over $\mathbb{F}$ with basis given by the paths in Q, including the trivial paths. A trivial path is of the form e_i for $i \in Q_0$.

For example (3) above, a basis for $\mathbb{F}Q$ is given by:

$$\{e_1, e_2, e_3, \alpha, \beta, \beta\alpha\}.$$

Elements of $\mathbb{F}Q$ have the form

$$a_1e_1 + a_2e_2 + a_3e_3 + a_4\alpha + a_5\beta + a_6\beta\alpha,$$

where $a_1, \dots, a_6$ lie in $\mathbb{F}$. Note that $\beta\alpha$ denotes the path given by following arrow α followed by arrow β.

The product in $\mathbb{F}Q$ is given by composition of paths, when possible, and zero otherwise.

So, for example, $\alpha e_1 = u$, $e_1\alpha = 0$ (cannot compose), $e_1^2 = e_1$, $e_1e_2 = 0$, $\alpha^2 = 0$.

It can be shown that $\mathbb{F}Q$ is a ring. The zero linear combination of paths is the zero element (all $a_i = 0$ in the above), and $\sum_{i \in Q_0} e_i$ is the identity element. In addition, $\mathbb{F}Q$ is an $\mathbb{F}$-algebra.

As an example, consider

$$\begin{tikzcd} 1 \arrow[loop left, "\alpha"] \end{tikzcd}$$

In this case, the paths are $e_1, \alpha, \alpha^2, \dots$ and an element of $\mathbb{F}Q$ is of the form

$$a_0e_1 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n$$

for some n. It can be seen that $\mathbb{F}Q \cong \mathbb{F}[x]$.

1.2. **Idempotents.** : Let $\mathbb{F}$ be a field and Q the quiver:

$$1 \xrightarrow{u} 2 \xrightarrow{v} 3$$

Then the idempotent paths e_1, e_2, e_3 in $\mathbb{F}Q$ satisfy the assumptions of Lemma 2.36 from lectures. We have $R = Re_1 \oplus Re_2 \oplus Re_3$; Re_i has basis given by paths in Q starting at i. So, for example, Re_1 has $\mathbb{F}$-basis e_1, u.

1.3. **Representations of quivers.** : Let Q be the quiver: $1 \xrightarrow{\alpha} 2$. Let $\mathbb{F}$ be a field. A *representation of Q* over $\mathbb{F}$ is a pair of vector spaces, V_1 and V_2 over $\mathbb{F}$, together with a linear map $f_\alpha : V_1 \to V_2$. We can construct an $\mathbb{F}Q$-module M as follows. Take

$$M = V_1 \oplus V_2 = \{(v_1, v_2) \, : \, v_1 \in V_1, \; v_2 \in V_2\},$$

the direct sum of V_1 and V_2 as vector spaces. Note that M is an abelian group. Then set

$$\begin{aligned} e_1(v_1, v_2) &= (v_1, 0) \\ e_2(v_1, v_2) &= (0, v_2) \\ \alpha(v_1, v_2) &= (0, f_\alpha(v_2)) \\ (a_1e_1 + a_2e_2 + a_3\alpha)(v_1, v_2) &= a_1e_1(v_1, v_2) + a_2e_2(v_1, v_2) + a_3\alpha(v_1, v_2). \end{aligned}$$

As another example, we consider the quiver: $1 \xrightarrow{\alpha} 2 \xrightarrow{\beta} 3$. A representation of this quiver over $\mathbb{F}$ is of the form: $V_1 \xrightarrow{f_\alpha} V_2 \xrightarrow{f_\beta} V_3$ where V_1, V_2, V_3 are $\mathbb{F}$-vector spaces and f_α and f_β are linear maps. We have, for example, $e_2(v_1, v_2, v_3) = (0, v_2, 0)$ and $\beta(v_1, v_2, v_3) = (0, 0, f_\beta(v_3))$.

1.4. **Left noetherian.** :

We have seen above that the path algebra $\mathbb{F}Q$ associated to the quiver Q:

$$1 \xrightarrow{\alpha} 2 \xrightarrow{\beta} 3$$

is 6-dimensional. It follows that it is left noetherian (see Example 4.15 in lectures).

R. J. Marsh, 17/11/14.