Queen Mary
University of London

# MAS 305 Algebraic Structures II

## Notes 13 Autumn 2006

---

## More about Noetherian rings

**Theorem** Let $R$ be a Noetherian ring. If $I$ is an ideal of $R$ then $R/I$ is Noetherian.

**Proof** Let $J_1 \subset J_2 \subseteq \cdots \subseteq J_i \subseteq J_{i+1} \subseteq \cdots$ be an ascending chain of ideals in $R/I$. By the Correspondence Theorem, $R$ has ideals $K_i$ $(i = 1, 2, \ldots)$ such that $I \subseteq K_i$ and $K_i/I = J_i$ and $K_i \subseteq K_{i+1}$ for all $i$. Then $I \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_i \subseteq K_{i+1} \subseteq \cdots$ is an ascending chain of ideals of $R$. Since $R$ is Noetherian, there is some $N$ such that $K_i = K_N$ whenever $i \geqslant N$, so $J_i = K_i/I = K_N/I = J_N$ for $i \geqslant N$. Hence $R/I$ is Noetherian. $\square$

**Corollary** If $R$ is Noetherian and $\phi: R \to S$ is a ring homomorphism then $\mathrm{Im}(\phi)$ is Noetherian.

**Definition** Given a non-empty set $\mathcal{S}$ of ideals of a ring, an ideal $M$ is *maximal* in $\mathcal{S}$ if

(a) $M \in \mathcal{S}$

(b) if $I \in \mathcal{S}$ and $I \supseteq M$ then $I = M$.

**Note:** $\mathcal{S}$ may have *no* maximal elements, or it may have more than one.

**Example** Let $\mathcal{S}$ be the set of all ideals of $\mathbb{Z}$ different from $\mathbb{Z}$ itself and $\{0\}$, so that $\mathcal{S} = \{n\mathbb{Z} : n \geqslant 2\}$. Since $n\mathbb{Z} \subseteq m\mathbb{Z}$ if and only if $m$ divides $n$, the maximal elements of $\mathcal{S}$ are $p\mathbb{Z}$ for primes $p$.

**Theorem** A ring $R$ is Noetherian if and only if every non-empty set of ideals of $R$ contains a maximal element.

**Proof** $\Longleftarrow$ Let $I_1 \subseteq I_2 \subseteq \cdots$ be an ascending chain of ideals of $R$. Put $\mathcal{S} = \{I_1, I_2, \ldots\}$. If every non-empty set of ideals contains a maximal element then $\mathcal{S}$ contains a maximal element, say $I_N$. If $j \geqslant N$ then $I_N \subseteq I_j$ so $I_j = I_N$ because $I_N$ is maximal in $\mathcal{S}$. Therefore $R$ is Noetherian.

$\Longrightarrow$ Suppose that $R$ is Noetherian and $\mathcal{S}$ is a non-empty set of ideals of $R$ with no maximal element. Choose any ideal $I_1$ in $\mathcal{S}$. Because $I_1$ is not maximal, we can choose $I_2$ in $\mathcal{S}$ with $I_1 \subset I_2$ and $I_1 \neq I_2$. Continuing like this, when we have chosen $I_n$ in $\mathcal{S}$ we know that $I_n$ is not maximal so we can choose $I_{n+1}$ in $\mathcal{S}$ with $I_n \subset I_{n+1}$ and $I_n \neq I_{n+1}$. This gives the infinite ascending chain

$$I_1 \subset I_2 \subset I_3 \subset \cdots \subset I_n \subset I_{n+1} \subset \cdots,$$

which contradicts ACC. $\square$

**Definition** An ideal $I$ of a ring $R$ is *finitely generated* if there is a finite subset $A$ of $R$ such that $I = \langle A \rangle$.

**Example** Every principal ideal is finitely generated.

**Theorem** A ring $R$ is Noetherian if and only if every ideal of $R$ is finitely generated.

**Proof** $\Longleftarrow$ Suppose that $I_1 \subseteq I_2 \subseteq \cdots$ are ideals of $R$. Put $I = \bigcup_{n=1}^{\infty} I_n$. Then $I$ is an ideal of $R$. If $I$ is finitely generated then there are elements $a_1, \ldots, a_m$ of $R$ such that $I = \langle \{a_1, \ldots, a_m\} \rangle$. For $i = 1, \ldots, m$, $a_i \in I$ so there is some $n_i$ such that $a_i \in I_{n_i}$. Put $N = \max\{n_1, \ldots, n_m\}$. Then

$$n_i \leqslant N \text{ so } a_i \in I_{n_i} \subseteq I_N \qquad \text{for } i = 1, \ldots, m$$

so $I \subseteq I_N$. If $j \geqslant N$ then $I_j \subseteq I \subseteq I_N \subseteq I_j$ so $I_j = I_N$. Hence ACC is satisfied and so $R$ is Noetherian.

$\Longrightarrow$ Suppose that $R$ is Noetherian. Let $I$ be an ideal of $R$, and let

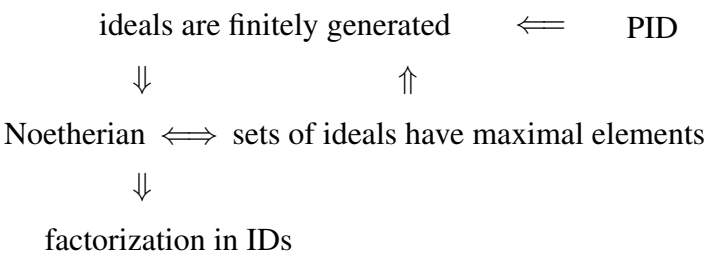
$$\mathcal{S} = \{K : K \trianglelefteq R,\ K \subseteq I,\ K \text{ is finitely generated}\}.$$

Then $\{0_R\} \in \mathcal{S}$, so $\mathcal{S}$ is not empty, so $\mathcal{S}$ contains a maximal element $M$. Then $M$ is finitely generated, so there is a finite subset $A$ of $R$ with $M = \langle A \rangle$.

Let $x \in I$. Put $B = A \cup \{x\}$ and $J = \langle B \rangle$. Then $B$ is finite so $J$ is finitely generated, and $J \subseteq I$ because $B \subseteq I$. Therefore $J \in \mathcal{S}$. But $M \subseteq J$, and $M$ is maximal, so $M = J$, so $x \in M$. This is true for all $x$ in $I$, so $I \subseteq M$. But $M \subseteq I$, because $M \in \mathcal{S}$. Therefore $I = M$, so $I$ is finitely generated. $\square$

## Aside on the Axiom of Choice

We can summarize some of the recent proofs as follows.




This diagram shows that one of our proofs was redundant! Apart from that, let's take another look at two proofs.

In the proof that in a Noetherian integral domain every (reasonable) element can be factorized as a product of irreducibles, we made the following argument.

> For $i = 1, 2, \ldots$, we have $r_i = r_{i+1}s_{i+1}$, and at least one of $r_{i+1}$, $s_{i+1}$ cannot be factorized, so *choose* the labelling so that $r_{i+1}$ cannot be factorized.

In the proof that in a Noetherian ring every non-empty set of ideals contains a maximal element, we made following argument.

> For $i = 1, 2, \ldots$, we have an ideal $I_i$ in $\mathcal{S}$, and $I_i$ is not maximal in $\mathcal{S}$, so we can *choose* an ideal $I_{i+1}$ in $\mathcal{S}$ with $I_i \subset I_{i+1}$ and $I_i \neq I_{i+1}$.

Both arguments use the *Axiom of Choice*, which states that:

> If $F_n$ is a non-empty set for $n \in \mathbb{N}$, then we can choose an element $x_n$ in $F_n$ for all $n$ in $\mathbb{N}$.

This axiom is not needed if we make only finitely many choices. It is independent of the other axioms of set theory—you can make one consistent mathematical theory by assuming it, or another consistent mathematical theory by assuming that it is not true. Some mathematicians think that the Axiom of Choice is so intuitively reasonable that they do assume it. However, the axiom has the consequence that the real numbers can be put into a total (linear) order in such a way that every subset of the real numbers has a first element. This consequence seems so intuitively unreasonable that there are other mathematicians who do not assume the Axiom of Choice.

Here is a nice way of picturing it. I have one drawer with countably infinitely many pairs of shoes, and another with countably infinitely many pairs of socks. If I ask you to take out one shoe from each pair you can do it, because you can follow some specification such as 'take the left shoe from each pair'. If I ask you to take out one sock from each pair then you cannot do it without the axiom of choice.

## Noetherian rings and polynomials

**Notation** Let $R$ be a ring. If $I$ is an ideal of $R[x]$, put

$$L_n(I) = \{a_n \in R : \exists a_0, a_1, \ldots, a_{n-1} \in R \text{ with } a_0 + a_1 x + \cdots + a_n x^n \in I\}$$

for $n \geqslant 0$.

**Lemma** If $R$ is a commutative ring with identity and $I$, $J$ are ideals of $R[x]$ then the following hold.

(a) $L_n(I)$ is an ideal of $R$;

(b) $L_n(I) \subseteq L_{n+1}(I)$;

(c) if $I \subseteq J$ then $L_n(I) \subseteq L_n(J)$;

(d) if $I \subseteq J$ and $L_n(I) = L_n(J)$ for all $n \geqslant 0$ then $I = J$.

**Proof** (a) (i) $0_R \in L_n(I)$ because $0 + 0x + \cdots + 0x^n = 0_{R[x]} \in I$.

(ii) If $a_n$ and $b_n$ are in $L_n(I)$ then there are polynomials $a_0 + a_1 x + \cdots + a_n x^n$ and $b_0 + b_1 x + \cdots + b_n x^n$ in $I$. Then

$$(a_0 - b_0) + (a_1 - b_1)x + \cdots + (a_n - b_n)x^n \in I,$$

so $a_n - b_n \in L_n(I)$.

(iii) If $a_n \in L_n(I)$ then there is a polynomial $a_0 + a_1 x + \cdots + a_n x^n$ in $I$. If $r \in R$ then $r \in R[x]$ and so $ra_0 + ra_1 x + \cdots + ra_n x^n \in I$, so $ra_n \in L_n(I)$.

(b) If $a_n \in L_n(I)$ then there is a polynomial $a_0 + a_1 x + \cdots + a_n x^n$ in $I$. Since $R$ has an identity, $x \in R[x]$. Therefore $0_R + a_0 x + a_1 x^2 + \cdots + a_n x^{n+1} \in I$. Thus $a_n \in L_{n+1}(I)$.

(c) If $I \subseteq J$ and $a_0 + a_1 x + \cdots + a_n x^n \in I$ then $a_0 + a_1 x + \cdots + a_n x^n \in J$, so if $a_n \in L_n(I)$ then $a_n \in L_n(J)$.

(d) Suppose that $J \supset I$ but $J \neq I$. Take a polynomial $f(x)$ of smallest degree in $J \setminus I$. Suppose that $f(x) = b_0 + b_1 x + \cdots + b_n x^n$. Then $b_n \in L_n(J) = L_n(I)$, so there is a polynomial $g(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} + b_n x^n$ in $I$. Then $g(x) \in I \subset J$ so $f(x) - g(x) \in J$. If $f(x) - g(x) = 0$ then $f(x) = g(x)$ so $f(x) \in I$, which is a contradiction. Otherwise, $f(x) - g(x)$ has smaller degree than $f(x)$, so $f(x) - g(x) \in I$, so $f(x) \in I$, which is also a contradition. $\square$

**Hilbert's Basis Theorem** Let $R$ be a commutative ring with identity. If $R$ is Noetherian then $R[x]$ is Noetherian.

**Proof** Let $I_1 \subseteq I_2 \subseteq \cdots$ be an ascending chain of ideals in $R[x]$. Put

$$\mathcal{S} = \{L_n(I_m) : n \geqslant 0,\ m \geqslant 1\}.$$

By part (i) of the lemma, this is a non-empty set of ideals of $R$. Since $R$ is Noetherian, $\mathcal{S}$ has a maximal element, say $L_p(I_q)$.

Part (ii) of the lemma shows that $L_0(I_m) \subseteq L_1(I_m) \subseteq L_2(I_m) \subseteq \cdots$ for all $m$, and part (iii) shows that $L_n(I_1) \subseteq L_n(I_2) \subseteq L_n(I_3) \subseteq \cdots$ for all $n$. Hence if $n \geqslant p$ and $m \geqslant q$ then

$$L_p(I_q) \subseteq L_n(I_q) \subseteq L_n(I_m)$$

so $L_n(I_m) = L_p(I_q)$.

For each $n$, there is an integer $M_n$ such that the ascending chain

$$L_n(I_1) \subseteq L_n(I_2) \subseteq \cdots$$

becomes stationary at $L_n(I_{M_n})$. Put $N = \max\left\{q, M_0, M_1, \ldots, M_{p-1}\right\}$.

Suppose that $m \geqslant N$. Then $m \geqslant q$ and $N \geqslant q$ so $L_n(I_m) = L_n(I_N) = L_p(I_q)$ for all $n \geqslant p$. If $n < p$ then $m \geqslant M_n$ and $N \geqslant M_n$ so $L_n(I_m) = L_n(I_N) = L_n(I_{M_n})$. Therefore $L_n(I_m) = L_n(I_N)$ for all $n$, so $I_m = I_N$, by part (iv) of the lemma.

Thus ACC is satisfied in $R[x]$, so $R[x]$ is Noetherian. $\square$

| ideals in $R[x]$ | $I_1$ | $I_2$ | $I_3$ | $\ldots$ | $I_{M_1}$ | $\ldots$ | $I_q$ | $\ldots$ | $I_{M_0}$ | $\ldots$ |
|---|---|---|---|---|---|---|---|---|---|---|
| ideals in $R$ | | | | | | | | | | |
| | $L_0(I_1)$ | $L_0(I_2)$ | $L_0(I_3)$ | $\ldots$ | $L_0(I_{M_1})$ | $\ldots$ | $L_0(I_q)$ | $\ldots$ | $L_0(I_{M_0})$ | $\ldots$ |
| | $L_1(I_1)$ | $L_1(I_2)$ | $L_1(I_3)$ | $\ldots$ | $L_1(I_{M_1})$ | $\ldots$ | $L_1(I_q)$ | $\ldots$ | $L_1(I_{M_0})$ | $\ldots$ |
| | $\vdots$ | $\vdots$ | $\vdots$ | $\ddots$ | $\vdots$ | $\ddots$ | $\vdots$ | $\ddots$ | $\vdots$ | $\ddots$ |
| | $L_p(I_1)$ | $L_p(I_2)$ | $L_p(I_3)$ | $\ldots$ | $L_p(I_{M_1})$ | $\ldots$ | $L_p(I_q)$ | $\ldots$ | $L_p(I_{M_0})$ | $\ldots$ |
| | $\vdots$ | $\vdots$ | $\vdots$ | $\ddots$ | $\vdots$ | $\ddots$ | $\vdots$ | $\ddots$ | $\vdots$ | $\ddots$ |

**Corollary 1 to Hilbert's Basis Theorem** Let $R$ be a commutative ring with identity. If $R$ is Noetherian then $R[x_1,\ldots,x_n]$ is Noetherian.

**Proof** Use induction on $n$. $\square$

**Corollary 2 to Hilbert's Basis Theorem** Let $R$ be a commutative ring with identity. If $S$ is a subring containing $1_R$ and $S$ is Noetherian and there are elements $r_1$, ..., $r_n$ in $R$ such that every element can be expressed as $f(r_1,\ldots,r_n)$ with $f$ in $S[x_1,\ldots,x_n]$ then $R$ is Noetherian.

**Proof** By the previous corollary, $S[x_1,\ldots,x_n]$ is Noetherian. Define $\phi: S[x_1,\ldots,x_n] \to R$ by $f(x_1,\ldots,x_n)\phi = f(r_1,\ldots,r_n)$. In a commutative ring, the definition of addition and multiplication of polynomials makes the substitution $\phi$ a homomorphism. Then $R = \mathrm{Im}(\phi)$, which is Noetherian. $\square$

**Corollary 3 to Hilbert's Basis Theorem** If $F$ is a field then $F[x_1,\ldots,x_n]$ is Noetherian.

**Example** Put $R = \left\{a+b\sqrt{-5} : a,\ b \in \mathbb{Z}\right\}$. Then $R$ is a subring of $\mathbb{C}$, which is commutative. Also, $\mathbb{Z}$ is a subring of $R$, $\mathbb{Z}$ contains the identity of $R$, and every element of $R$ is $f(\sqrt{-5})$ for some $f$ in $\mathbb{Z}[x]$. Therefore $R$ is Noetherian. Moreover, $R$ is an integral domain, so every element of $R$ which is not a unit or zero can be factorized as a product of a finite number of irreducibles. However, $R$ is not a unique factorization domain, because factorization is not unique, as we shall now show.

If $(a+b\sqrt{-5})(c+d\sqrt{-5}) = e+f\sqrt{-5}$ then $(a-b\sqrt{-5})(c-d\sqrt{-5}) = e-f\sqrt{-5}$. Multiplying corresponding sides gives

$$(a^2+5b^2)(c^2+5d^2) = e^2+5f^2. \tag{1}$$

First put $e+f\sqrt{-5} = 1$. Then the only integer solution to (1) is $a = c = \pm 1$ and $b = d = 0$. Therefore the units of $R$ are just $\pm 1$.

More generally, (1) shows that $e+f\sqrt{f}$ is irreducible if $e^2+5f^2$ cannot be factorized as the product of two integers, neither of which is $\pm 1$ and both of which are congruent to 0, 1 or 4 modulo 5.

In $R$ we have

$$(1+2\sqrt{-5})(3+\sqrt{-5}) = -7+7\sqrt{-5} = 7(-1+\sqrt{-5}).$$

Then we get $1^2+5\times 2^2 = 21 = 3\times 7$, $3^3+5\times 1^2 = 14 = 2\times 7$, $7^2 = 7\times 7$ and $(-1)^2+5\times 1^2 = 6 = 2\times 3$. Since none of 2, 3 and 7 is congruent to 0, 1 or 4 modulo 5, the four elements $1+2\sqrt{-5}$, $3+\sqrt{-5}$, 7 and $-1+\sqrt{-5}$ are all irreducible. No pair are associates, because $x$ is an associate of $y$ if and only if $x = \pm y$. So we have a non-unique factorization of $-7+7\sqrt{-5}$.

**Example** We shall show that $2\mathbb{Z}$ is Noetherian but $2\mathbb{Z}[x]$ is not.

Let $I$ be a non-zero ideal of $2\mathbb{Z}$. If $a \in I$ then $-a \in I$ because $I$ is a subgroup of $(2\mathbb{Z}, +)$. Let $a$ be the smallest positive element of $I$. Suppose that $b \in I$ with $b > 0$. In $\mathbb{Z}$, there are integers $q$ and $r$ such that $b = qa + r$ and $0 \leqslant r < a$. Now,

$$qa = \underbrace{a + a + \cdots + a}_{q \text{ times}},$$

which is in $I$. Thus $b - qa \in I$ and so $r \in I$. Because $0 \leqslant r < a$, we must have $r = 0$. Therefore $I = \{qa : q \in \mathbb{Z}\}$ (of course, $a$ is even).

So every ideal of $2\mathbb{Z}$ is an ideal of $\mathbb{Z}$. We know that $\mathbb{Z}$ satisfies ACC, so $2\mathbb{Z}$ must also satify ACC.

If $2\mathbb{Z}[x]$ is Noetherian then it is finitely generated. Suppose that the generators are $f_1(x)$, ..., $f_n(x)$, where $f_i(x)$ has degree $d_i$. Put $N = \max\{d_1, \ldots, d_n\}$. Then if $g(x) \in \langle\{f_1(x), \ldots, f_n(x)\}\rangle$ then

***either*** the degree of $g(x)$ is at most $N$

***or*** every coefficient in $g(x)$ is divisible by 4.

Therefore $2x^{N+1} \notin \langle\{f_1(x), \ldots, f_n(x)\}\rangle$ but $2x^{N+1} \in 2\mathbb{Z}[x]$. This contradiction shows that $2\mathbb{Z}[x]$ is not Noetherian.

## Noetherian rings and matrices

**Theorem** (a) If the ring $R$ is not Noetherian then $M_n(R)$ is not Noetherian.

(b) If the ring $R$ has an identity and $R$ is Noetherian then $M_n(R)$ is Noetherian.

**Proof** (a) Let $I_1 \subset I_2 \subset \cdots \subset I_m \subset I_{m+1} \subset \cdots$ be an infinite ascending chain of ideals of $R$. Then $M_n(I_1) \subset M_n(I_2) \subset \cdots \subset M_n(I_m) \subset M_n(I_{m+1}) \subset \cdots$ is an infinite ascending chain of ideals of $M_n(R)$.

(b) Let $J_1 \subseteq J_2 \subseteq \cdots$ be an ascending chain of ideals of $M_n(R)$. Since $R$ has an identity, there are ideals $I_m$ of $M_n(R)$ such that $J_m = M_n(I_m)$ for $m = 1, 2, \ldots$. Then $I_1 \subseteq I_2 \subseteq \cdots$. Since $R$ is Noetherian, there is some $N$ such that $I_m = I_N$ whenever $m \geqslant N$. Then $J_m = M_n(I_m) = M_n(I_N) = J_N$ when $m \geqslant N$. $\square$

**Example** We know that $2\mathbb{Z}$ is Noetherian but does not contain an identity. We shall show that not all ideals of $M_2(2\mathbb{Z})$ have the form $M_2(I)$ for some ideal $I$ of $2\mathbb{Z}$.

Put

$$J = \left\{ \begin{bmatrix} 4a & 4b \\ 2c & 4d \end{bmatrix} : a,\ b,\ c,\ d \in \mathbb{Z} \right\} \subseteq M_2(\mathbb{Z}).$$

Then $(J,+)$ is a subgroup of $(M_2(2\mathbb{Z}),+)$. If $A \in J$ and $B \in M_2(2\mathbb{Z})$ then $AB \in M_2(4\mathbb{Z}) \subseteq J$ and $BA \in M_2(4\mathbb{Z}) \subseteq J$, so $J \lhd M_2(\mathbb{Z})$.

**Challenge!** Is $M_2(2\mathbb{Z})$ Noetherian?