Week 3 Notes

Warning: These are unofficial notes which address some questions in the support class. The contents are not necessarily part of the lectures and may not be examinable. Please use them at your own discretion.

In this course, all rings are assumed to be commutative rings with multiplicative identity 1.

2.1 Dickson's lemma

Proposition 2.1. Dickson's Lemma

Let $S = k[x_1, ..., x_n]$ be a polynomial ring and $I = \langle x^{\boldsymbol{u}} \mid \boldsymbol{u} \in A \rangle$ be a monomial ideal, where $A \subseteq \mathbb{N}^n$. Then there exists $\boldsymbol{a}_1, ..., \boldsymbol{a}_s \in A$ such that $I = \langle x^{\boldsymbol{a}_1}, ..., x^{\boldsymbol{a}_s} \rangle$.

Proof. We prove this by induction on n.

Base case: for $n = 1$, $I = \langle x^\alpha \rangle$ where α is the smallest integer in the set $A \subseteq \mathbb{N}$.

Induction case. Suppose that the result holds for $S_{n-1} = k[x_1, ..., x_[n-1]]$. Then $S = S_{n-1}[y]$ where $y := x_n$. Consider the ideal

$$J := \langle x^\alpha \in S_{n-1} \mid x^\alpha y^m \in I \text{ for some } m \in \mathbb{Z}_+ \rangle \triangleleft S_{n-1}.$$

By induction hypothesis, $J = \left\langle x^{\alpha(1)}, ..., x^{\alpha(s)} \right\rangle$ for some $\alpha(1), ..., \alpha(s) \in \mathbb{N}^{n-1}$. For each i, there exists some $m_i \in \mathbb{N}$ such that $x^{\alpha(i)} y^{m_i} \in I$. Let $m := \max\{m_1, ..., m_s\}$. For each $\ell \in \{0, ..., m-1\}$, consider the ideals

$$J_\ell := \left\langle x^\alpha \in S_{n-1} \mid x^\alpha y^\ell \in I \right\rangle \triangleleft S_{n-1}.$$

By induction hypothesis, $J_\ell = \left\langle x^{\alpha_\ell(1)}, ..., x^{\alpha_\ell(m_\ell)} \right\rangle$. Now we claim that I is generated by the polynomials

$$\begin{aligned}
&x^{\alpha(1)} y^m, \ldots, x^{\alpha(s)} y^m; \\
&x^{\alpha_0(1)}, \ldots, x^{\alpha_0(s_0)}; \\
&x^{\alpha_1(1)} y, \ldots, x^{\alpha_1(s_1)} y; \\
&\ldots; \\
&x^{\alpha_{m-1}(1)} y^{m-1}, \ldots x^{\alpha_{m-1}(s_{m-1})} y^{m-1}.
\end{aligned}$$

As I is a monomial ideal, it suffices to check that all monomials in I can be generated by these elements. Let $x^u y^j \in I$. If $j \geqslant m$, then since $x^u \in J$ we have $x^{\alpha(i)} \mid x^u$ for some i. Hence $x^{\alpha(i)} y^m \mid x^u y^j$. If $j < m$, then $x^u \in J_j$ and hence $x^{\alpha_j(i)} \mid x^u$ for some i. Hence $x^{\alpha_j(i)} y^j \mid x^u y^j$.

We have proven that I is generated by $x^{b_1}, \ldots, x^{b_s}$ for some $b_1, \ldots, b_s \in \mathbb{N}^n$. By the lemma in the lectures, for each i there exists $\boldsymbol{a}_i \in A$ such that $x^{a_i} \mid x^{b_i}$. Hence I is generated by $x^{a_1}, \ldots, x^{a_s}$ with $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_s \in A$. □

2.2 Hilbert basis theorem for power series rings

We can mimic the proof of Hilbert basis theorem to prove a similar result for the rings of power series.

Proposition 2.2

Let R be a Noetherian ring. Then $R[\![x]\!]$ is also Noetherian.

Proof. Instead of the degree of a polynomial, for $f \in R[\![x]\!]$ we consider $d(f) := \min\{n \in \mathbb{N} \mid f \in \langle x^n \rangle\}$. That is, $d(f)$ is the degree of the lowest non-zero term of f. Let $b(f) \in R$ be the coefficient of the term of degree $d(f)$ of f. That is, $f(x) = b(f)x^{d(f)} + \sum_{n=d(f)+1}^{\infty} c_n x^n$.

Suppose that $I \triangleleft R[\![x]\!]$ is not finitely generated. We may construct a non-stabilising ascending chain of ideals of $R[\![x]\!]$:

$$\langle f_1 \rangle \subsetneq \langle f_1, f_2 \rangle \subsetneq \langle f_1, f_2, f_3 \rangle \subsetneq \cdots$$

where $f_{m+1} \in I \setminus \langle f_1, \ldots, f_m \rangle$ is with the largest $d(f)$ among all elements of $I \setminus \langle f_1, \ldots, f_m \rangle$ for each $m \in \mathbb{N}$. We claim that $b(f_{m+1}) \notin \langle b(f_1), \ldots, b(f_m) \rangle$. Suppose the contrary holds. Then $b(f_{m+1}) = \sum_{i=1}^{m} r_i b(f_i)$ for some $r_1, \ldots, r_m \in R$. Consider $f'_{m+1} := f_{m+1} - \sum_{i=1}^{m} r_i f_i$. Then we note that $f'_m \in I \setminus \langle f_1, \ldots, f_m \rangle$ and $d\left(f'_{m+1}\right) > d(f_{m+1})$. This contradicts the maximality assumption on f_{m+1}. Hence $b(f_{m+1}) \notin \langle b(f_1), \ldots, b(f_m) \rangle$. But now we have a non-stabilising ascending chain of ideals of R :

$$\langle b(f_1) \rangle \subsetneq \langle b(f_1), b(f_2) \rangle \subsetneq \langle b(f_1), b(f_2), b(f_3) \rangle \subsetneq \cdots$$

This contradicts that R is Noetherian. Hence I is finitely generated so $R[\![x]\!]$ is Noetherian. □

In the class you are told to determine if $k[\![x]\!]$ is a Noetherian ring, where k is a field. Of course this is a special case of the result proven above. Nonetheless, a simpler proof can be given for this case. In particular we can prove that $k[\![x]\!]$ is a PID.

Lemma 2.3

Let k be a field. Then $k[\![x]\!]$ is a PID. Moreover, every ideal of $k[\![x]\!]$ is of the form $\langle x^n \rangle$ for some $n \in \mathbb{Z}_{\geqslant 0}$.

Proof. We will be using the following fact: $f \in k[\![x]\!]$ is a unit if and only if f has non-zero constant term. Indeed, if $f(x) = \sum_{n=0}^{\infty} a_n x^n$, f is a unit if we can find $g(x) = \sum_{n=0}^{\infty} b_n x^n \in k[\![x]\!]$ such that $f(x)g(x) = 1$. We can solve b_n inductively:

$$1 = a_0 b_0; \qquad \sum_{i=0}^{n} a_i b_{n-i} = 0, \ \forall\, n > 0.$$

So there exists a sequence $(b_n)_{n \geqslant 0}$ that solves the above equation if and only if $a_0 \neq 0$. In this case, g exists and f is a unit.

Now let $I \triangleleft k[\![x]\!]$. Let $f \in I$ such that $d(f)$ is minimal among all elements in I (the same $d(f)$ as in the previous proof) and let $n = d(f)$. That is, $f \in \langle x^n \rangle$ and $f \notin \left\langle x^{n+1} \right\rangle$. We claim that $I = \langle x^n \rangle$.

On one hand, we may write $f(x) = x^n g(x)$ where $g \in k[\![x]\!]$ has non-zero constant term. This means there exists $h \in k[\![x]\!]$ such that $gh = 1$. Therefore $x^n = x^n g(x)h(x) = f(x)h(x) \in \langle f(x) \rangle \subseteq I$. On the other hand, for $f' \in I$, by assumption we have $f'(x) = x^m g'(x)$ where $m \geqslant n$ and $g' \in k[\![x]\!]$ has non-zero constant term. So $f'(x) = x^n \cdot x^{m-n} g'(x) \in \langle x^n \rangle$. This finishes the proof. □

2.3 An example of Noetherian ring

Proposition 2.4

$\mathbb{Z}[2^{-1}] := \{a/b \in \mathbb{Q} \mid \gcd(a, b) = 1,\ b = 2^n \text{ for some } n \in \mathbb{Z}_{\geqslant 0}\}$ is a Noetherian ring.

$\mathbb{Z}[2^{-1}]$ is an example of localisation of $\mathbb{Z}$. In general, a localisation of a Noetherian ring R is also Noetherian. Although in this case direct proofs are easier. We present two proofs.

Proof 1. Consider the ring homomorphism $\varphi : \mathbb{Z}[x] \to \mathbb{Z}[2^{-1}]$ induced by $x \longmapsto 1/2$. It is clear that φ is surjective, and $\varphi(2x-1) = 0$. We claim that $\ker\varphi = \langle 2x-1\rangle$. Indeed, suppose that $f \in \ker\varphi$. Consider $f \in \mathbb{Q}[x]$. We have $f(1/2) = 0$ by construction of φ. Hence $f(x) = (2x-1)g(x)$ for some $g(x) \in \mathbb{Q}[x]$. Suppose that $f(x) = \sum_n a_n x^n$ and $g(x) = \sum_n b_n x^n$. Then

$$a_n = -b_n + 2b_{n-1}, \quad \forall n \in \mathbb{Z}_{>0}; \qquad a_0 = -b_0.$$

Since $a_n \in \mathbb{Z}$ for all n, by induction we have that $b_n \in \mathbb{Z}$ for all n. Hence $g \in \mathbb{Q}[x]$. So we have $f(x) = (2x-1)g(x)$ in $\mathbb{Z}[x]$. That is, $f \in \langle 2x-1\rangle$. This proves the claim. Now by first isomorphism theorem we have $\mathbb{Z}[x]/\langle 2x-1\rangle \cong \mathbb{Z}[2^{-1}]$.

Finally, $\mathbb{Z}$ is Noetherian because it is a PID; $\mathbb{Z}[x]$ is Noetherian by Hilbert basis theorem; and $\mathbb{Z}[x]/\langle 2x-1\rangle$ is Noetherian since it is a quotient of a Noetherian ring. □

Proof 2. We can also show directly that $\mathbb{Z}[2^{-1}]$ is a PID. For $I \lhd \mathbb{Z}[2^{-1}]$, consider the ideal

$$J := \langle a \in \mathbb{Z} \mid a/b \in I \text{ for some } b = 2^n\rangle \lhd \mathbb{Z}.$$

Since $\mathbb{Z}$ is a PID, we have $J = \langle a_0\rangle$ for some $a_0 \in \mathbb{Z}$. Now we claim that $I = \langle a_0/1\rangle$ in $\mathbb{Z}[2^{-1}]$.

On one hand, by definition $a_0/b_0 \in I$ for some b_0. Then $a_0/1 = a_0/b_0 \cdot b_0/1 \in I$. On the other hand, if $a/b \in I$, then $a \in J$ and hence $a = ca_0$ for some $c \in \mathbb{Z}$. Now $a/b = c/b \cdot a_0/1 \in \langle a_0/1\rangle$. This finishes the proof. □

2.4 An example of non-Noetherian ring

Proposition 2.5

Let k be a field and R be the k-algebra generated by the semi-group $\{x, xy, xy^2, xy^3, \ldots\}$. That is, R is a subring of $k[x, y]$ in which every polynomial is of the form $f(x, y) = \sum_{\substack{i\geqslant 1\\ j\geqslant 0}} a_{ij}x^i y^j$. Then R is not a Noetherian ring.

Proof. We claim that the following ascending chain of ideals of R does not stabilise:

$$\langle x\rangle \subseteq \langle x, xy\rangle \subseteq \left\langle x, xy, xy^2\right\rangle \subseteq \cdots$$

Inductively we shall prove that $xy^{n+1} \notin \langle x, xy, \ldots, xy^n\rangle$. Suppose that the contrary holds. Let

$$xy^n = \sum_{i=0}^{n} f_i(x, y)xy^i.$$

Since R is an integral domain, $y^n = \sum_{i=0}^n f_i(x, y)y^i$. Note that each $f_i \in R$ is divisible by x in $k[x, y]$, but y is not divisible by x in $k[x, y]$. So this is a contradiction. □