Week 2 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.

1.1 Is the polynomial ring a PID?

Recall that a PID is a ring in which every ideal is generated by a single element. The following should be an easy exercise from Algebra II.

Proposition 1.1

Let R be a ring. Then R is a field if and only if $R[x]$ is a PID.

Proof. " $\Longrightarrow$ ": If R is a field, then in fact $R[x]$ is a Euclidean domain in the sense that **division algorithm** works for all polynomials in $R[x]$ (in general, it only works for polynomials whose leading coefficient is a unit in R). Let I be a non-zero ideal of $R[x]$. We choose $f \in I$ such that $\deg f = \min\{\deg g \mid g \in I \setminus \{0\}\}$. For $h \in I$, there exists $q, r \in I$ such that $h = qf + r$ with either $r = 0$ or $\deg r < \deg f$. As $f, h \in I$, $r = h - qf \in I$. We must have $r = 0$ by minimality of $\deg f$. Hence $h = qf \in \langle f \rangle$. We have $I = \langle f \rangle$. So $R[x]$ is a principal ideal domain.

" $\Longleftarrow$ ": Consider the surjective ring homomorphism $\varphi : R[x] \to R$ such that $\varphi(r) = r$ for all $r \in R$ and $\varphi(x) = 1$. Then by first isomorphism theorem we have $R[x]/\ker\varphi \cong R$. Note that $\varphi(x-1) = 0$ so $x - 1 \in \ker\varphi$. Since $R[x]$ is a PID, $\ker\varphi = \langle f \rangle$ for some $f \in R[x]$. It follows that f divides $(x-1)$. Since $(x-1)$ is irreducible, we have $\ker\varphi = \langle x - 1 \rangle$, which is a maximal ideal. Therefore $R \cong R[x]/\langle x-1 \rangle$ is a field. □

1.2 Row echelon form

For an ideal generated by linear polynomials the problem of finding a Gröbner basis is purely linear algebra.

Proposition 1.2

Let k be a field and $R := k[x_1, ..., x_n]$ a polynomial ring. Let $I = \langle g_1, ..., g_m \rangle$ be an ideal generated by $g_1, ..., g_m \in R$ where each $g_i = \sum_{j=1}^{n} a_{ij} x_j$ is a linear polynomial. Suppose that the matrix $M = (a_{ij})$ is in its row echelon form. Then $\{g_1, ..., g_m\}$ is a Gröbner basis (with respect to a suitable lexicographic ordering) for I.

1.3 Noetherian rings and Hilbert basis theorem

The problem of existence of Gröbner basis for any ideal is a corollary of Hilbert basis theorem, which holds not only for polynomial rings over a field but for any Noetherian ring. These materials might be covered in the later lectures.

Proposition 1.3

Suppose that R is a ring. The following statements are equivalent:

1. Every ideal of R is finitely generated.
2. (**Ascending Chain Condition**) Suppose that we have an ascending chain of ideals of R:

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

Then there exists $m \in \mathbb{N}$ such that $I_m = I_{m+n}$ for all $n > 0$.

If R satisfies those conditions, then R is called a **Noetherian ring**.

Proof. $1 \implies 2$: Consider an ascending chain of ideals:

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

Let $I := \bigcup_{n=1}^{\infty} I_n$. By assumption I is finitely generated. Let $i = \langle x_1, ..., x_m \rangle$. For each i there exists $n_i \in \mathbb{N}$ such that $x_i \in I_{n_i}$. Take $N := \max\{n_1, ..., n_m\}$. Then we have $I_N = I$ and hence $I_N = I_{N+1} = I_{N+2} = \cdots$.

$2 \implies 1$: Suppose that $I \triangleleft R$ is not finitely generated. First pick a $x_1 \in I$. For each $n > 0$, there exists $x_{n+1} \in I \setminus \langle x_1, ..., x_n \rangle$, for otherwise I would be generated by the set $\{x_1, ..., x_n\}$. Therefore we can construct a non-terminating ascending chain:

$$\langle x_1 \rangle \subsetneq \langle x_1, x_2 \rangle \subsetneq \langle x_1, x_2, x_3 \rangle \subsetneq \cdots$$

This contradicts the ACC. □

Theorem 1.4. Hilbert basis theorem

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

This is one of the foundational theorems in commutative algebra. You may find the proof in

- Theorem 1.27 of Chunyi's notes; or
- Theorem 3.6 of Miles' book; or
- Theorem 7.5 of Atiyah & MacDonald.

The point is that using ACC dramatically simplifies the proof (at least conceptually). The following is the historical version of Hilbert basis theorem, but it is now an easy corollary.

Corollary 1.5

Let k be a field. Then every ideal of $k[x_1, ..., x_n]$ is finitely generated.

A direct (and probably more computational?) proof without using ACC of this fact can be found in Theorem 2.5.4 of CLO.