Week 7 Notes

6.1 Even more localisations

We start with Question 4 of Part B of Assignment 2. There are some clever solutions which avoid listing all elements in each equivalence class.

Example 6.1. PS2.B.4

Let $R = \mathbb{Z}/10\mathbb{Z}$ and $U := \{1, 2, 4, 6, 8\} \subseteq \mathbb{Z}/10\mathbb{Z}$. Then

$$\mathbb{Z}/10\mathbb{Z}[U^{-1}] = \mathbb{Z}/10\mathbb{Z}[2^{-1}] \cong \mathbb{Z}/5\mathbb{Z}.$$

Proof 1. Consider the natural homomorphism $\varphi : \mathbb{Z}/10\mathbb{Z} \to \mathbb{Z}/10\mathbb{Z}[U^{-1}]$. Note that $a \in \ker \varphi$ if and only if there exists $u \in U$ such that $au = 0$ in $\mathbb{Z}/10\mathbb{Z}$. The only zero divisor in U is 2 and we have $5 \cdot 2 = 0$. Hence $\ker \varphi = \{0, 5\}$. Ne3xt we claim that φ is surjective. For this we note the equivalence

$$\begin{aligned} \frac{1}{2} &\sim \frac{3}{1} \in \mathbb{Z}/10\mathbb{Z}[U^{-1}] \qquad &&\text{as } 2 \cdot (3 \cdot 2 - 1 \cdot 1) = 0 \in \mathbb{Z}/10\mathbb{Z}; \\ \frac{1}{6} &\sim \frac{1}{1} \in \mathbb{Z}/10\mathbb{Z}[U^{-1}] \qquad &&\text{as } 2 \cdot (6 \cdot 1 - 1 \cdot 1) = 0 \in \mathbb{Z}/10\mathbb{Z}. \end{aligned}$$

For any $r \in \mathbb{Z}/10\mathbb{Z}$, $r = \frac{a}{u}$, where u is either 6 or a power of 2. This shows that $r = \frac{a'}{1}$ for some $a' \in \mathbb{Z}/10\mathbb{Z}$. So φ is surjective. Finally, by first isomorphism theorem,

$$\mathbb{Z}/10\mathbb{Z}[U^{-1}] \cong \frac{\mathbb{Z}/10\mathbb{Z}}{\{0, 5\}} \cong \mathbb{Z}/5\mathbb{Z}. \qquad \square$$

Proof 2. $\mathbb{Z}/10\mathbb{Z} \times U$ is an Abelian group with the addition

$$(a, b) + (c, d) := (ad + bc, bd),$$

identity $(0, 1)$, and inverse $-(a, b) = (10 - a, b)$. Moreover, the equivalence relation on $\mathbb{Z}/10\mathbb{Z} \times U$ defines a subgroup H via

$$(a, b) \sim (c, d) \iff (a, b) - (c, d) \in H.$$

In particular, the additive group $\mathbb{Z}/10\mathbb{Z}[U^{-1}]$ is identified with the quotient group $(\mathbb{Z}/10\mathbb{Z} \times U)/H$. To describe the subgroup H, note that

$$(a, b) \sim (0, 1) \iff \exists\, u \in U \ (au = 0) \iff a \in \{0, 5\}.$$

Hence $|H| = |U| \times |\{0, 5\}| = 2 \cdot 5 = 10$. By Lagrange's theorem,

$$|\mathbb{Z}/10\mathbb{Z}[U^{-1}]| = |\mathbb{Z}/10\mathbb{Z} \times U|/|H| = |\mathbb{Z}/10\mathbb{Z}| \times |U|/|H| = 5.$$

Finally, a ring with 5 elements must be isomorphic to $\mathbb{Z}/5\mathbb{Z}$. $\square$

Example 6.2. PS3.A.4

Let R be a local ring with maximal ideal $\mathfrak{m}$. Then $R_{\mathfrak{m}} \cong R$.

Remark. This is a special case of the general fact that, if $U \subseteq R^\times$, then $R \cong R[U^{-1}]$. Because "units are already invertible, so inverting them gives you nothing new".

Proof. We will use the fact that $U = R \setminus \mathfrak{m}$ consists of units of R. Consider the natural map $\varphi : R \to R_\mathfrak{m} = R[U^{-1}]$.

- φ is injective: for $a \in \ker\varphi$, $a/1 \sim 0/1 \in R[U^{-1}]$. So there exists $u \in U$ such that $au = 0$. Note that $u \in R \setminus \mathfrak{m}$ is a unit and thus not a zero divisor. We must have $a = 0$, which means φ is injective.
- φ is surjective: for $a/u \in R[U^{-1}]$, since $u \in R \setminus \mathfrak{m}$ is a unit, $u^{-1} \in R$. So $a/u \sim au^{-1}/1 \in \operatorname{im}\varphi$. Therefore φ is surjective.

We conclude that φ is an isomorphism. □

6.2 Reduced Gröbner basis

Many people found this homework question difficult so I attach a complete solution below.

Theorem 6.3. PS2.B.1

Let I be an ideal of $k[x_1, ..., x_n]$. Fix a term order $<$. We say that a Gröbner basis $G = \{g_1, ..., g_s\}$ of I is **reduced**, if:

1) The coefficient of each $\text{in}_<(g_i)$ is 1;
2) $\{\text{in}_<(g_1), ..., \text{in}_<(g_s)\}$ is an irredundant minimal generating set for $\text{in}_<(I)$;
3) No term of g_i is divisible by $\text{in}_<(g_j)$ for any $i \neq j$.

Any ideal I has a unique reduced Gröbner basis. This produces an algorithm to decide whether two ideals I and J are equal in $k[x_1, ..., x_n]$.

Remark. We say that a Gröbner basis is **minimal** if it satisfies (1) and (2).

Proof. First we prove the existence of a reduced Gröbner basis, and at the same time give a algorithm to compute it. Suppose that $I = \langle f_1, ..., f_m \rangle$ is an ideal. A Gröbner basis of I can be computed by the **Buchberger's algorithm** (this is not examinable, see CLO Section 2.7). So

Step 0: There exists a Gröbner basis $G = \{g_1, ..., g_s\}$ of I.

For (1), we divide each g_i by the coefficient $\text{LC}(g_i) \in k$ of $\text{in}_<(g_i)$, and replace g_i by this polynomial. Then G is a Gröbner basis in which every polynomial is monic.

For (2), we remove any $g_i \in G$ from G such that $\text{in}_<(g_i) \in \langle \text{in}_<(G \setminus \{g_i\}) \rangle$. After removing all suchb polynomials, G is still a Gröbner basis, and there are no $g_i, g_j \in G$ such that $\text{in}_<(g_i) \mid \text{in}_<(g_j)$. After this step, G becomes a minimal Gröbner basis.

For (3), we take $g \in G$ and replace it by the remainder g' of g divided by $G \setminus \{g\}$. Note that we have $\text{in}_<(g) = \text{in}_<(g')$, and no term of g' is divisible by elements of $\text{in}_<(G \setminus \{g\})$. We say that each g' is fully reduced. Continue this process until all elements of G are fully reduced. This process terminates after finitely many steps, because once a polynomial is fully reduced, it stays fully reduced since we never change the leading terms. Thus, we end up with a reduced Gröbner basis.

Next we prove the uniqueness. Suppose that $G = \{g_1, ..., g_n\}$ and $H = \{h_1, ..., h_m\}$ are two reduced Gröbner bases. Since $\{\mathrm{in}_<(g_1), .., \mathrm{in}_<(g_n)\}$ and $\{\mathrm{in}_<(h_1), ..., \mathrm{in}_<(h_m)\}$ are both minimal generating set of the monomial ideal $\mathrm{in}_<(I)$, they are equal. Therefore $n = m$, and after renumbering, we have $\mathrm{in}_<(g_i) = \mathrm{in}_<(h_i)$ for each i.

Consider $g_i - h_i \in I$. Since G is a Gröbner basis of I, the remainder of $g_i - h_i$ divided by G is zero. On the other hand, the initial terms of g_i and h_i cancel, and the remaining terms are divisible by none of $\mathrm{in}_<(G) = \mathrm{in}_<(H)$. Therefore the remainder of $g_i - h_i$ divided by G is equal to $g_i - h_i$. It follows that $g_i = h_i$ and hence $G = H$. □

6.3 Description of $\operatorname{Spec} \mathbb{Z}[x]$

Example 6.4. PS2.C.2

What are the prime ideals in $\mathbb{Z}[x]$?

Remark. The idea is to consider the projection $f : \operatorname{Spec} \mathbb{Z}[x] \to \operatorname{Spec} \mathbb{Z}$. We know that

$$\operatorname{Spec} \mathbb{Z} = \{\langle p \rangle \mid p = 0 \text{ or } p \text{ is prime}\}.$$

The fibre of f over $\langle p \rangle \in \operatorname{Spec} \mathbb{Z}$ is isomorphic to $\operatorname{Spec} \kappa(p)[x]$, where $\kappa(p) := \mathbb{Z}_{\langle p \rangle} / \langle p \rangle \mathbb{Z}_{\langle p \rangle}$ is the residue field.

Proof. We claim that

$$\begin{aligned} \operatorname{Spec} \mathbb{Z}[x] = &\{\langle 0 \rangle\} \cup \{\langle f \rangle \mid f \in \mathbb{Z}[x] \text{ irreducible}\} \\ &\cup \left\{ \langle p, f \rangle \mid p \in \mathbb{Z} \text{ prime},\ f \in \mathbb{Z}[x] \text{ is s.t. } \overline{f} \in \mathbb{F}_p[x] \text{ irreducible} \right\}. \end{aligned}$$

Let $\mathfrak{p} \in \operatorname{Spec} \mathbb{Z}[x]$. Then $\mathfrak{p} \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$. We know that $\operatorname{Spec} \mathbb{Z} = \{\langle 0 \rangle\} \cup \{\langle p \rangle \mid p \in \mathbb{Z} \text{ prime}\}$. The proof is divided into two cases:

- Suppose that $\mathfrak{p} \cap \mathbb{Z} = \{0\}$. We could have either $\mathfrak{p} = \{0\}$, or there exists some $g \in \mathfrak{p} \setminus \{0\}$. Since $\mathbb{Z}[x]$ is a UFD, $g = \prod_{i=1}^k f_i^{n_i}$ for some irreducible polynomials $f_1, ..., f_s \in \mathbb{Z}[x]$. Since $\mathfrak{p}$ is prime, there is some $f := f_i \in \mathfrak{p}$. We claim that $\mathfrak{p} = \langle f \rangle$. Let $j \colon \mathbb{Z}[x] \to \mathbb{Q}[x]$ be the natural inclusion, and $\mathfrak{p}^e$ the extended ideal of $\mathfrak{p}$ in $\mathbb{Q}[x]$. By Gauss' lemma, f is irreducible in $\mathbb{Q}[x]$ and hence $\langle f \rangle_{\mathbb{Q}[x]}$ is maximal. Since $\mathfrak{p} \cap \mathbb{Z} = \{0\}$, $1 \notin \mathfrak{p}^e$. Then we must have $\mathfrak{p}^e = \langle f \rangle_{\mathbb{Q}[x]}$. Now $\mathfrak{p} = \mathfrak{p}^e \cap \mathbb{Z}[x] = \langle f \rangle_{\mathbb{Q}[x]} \cap \mathbb{Z}[x] = \langle f \rangle_{\mathbb{Z}[x]}$.
- Suppose that $\mathfrak{p} \cap \mathbb{Z} = \langle p \rangle_{\mathbb{Z}}$ for some prime $p \in \mathbb{Z}$. Let $\pi : \mathbb{Z}[x] \twoheadrightarrow \mathbb{F}_p[x]$ be the projection. $\pi(\mathfrak{p})$ is an ideal of $\mathbb{F}_p[x]$ and we have an isomorphism $\mathbb{Z}[x]/\mathfrak{p} \cong \mathbb{F}_p[x]/\pi(\mathfrak{p})$. Now $\pi(\mathfrak{p})$ is an prime ideal of $\mathbb{F}_p[x]$. Since $\mathbb{F}_p[x]$ is a PID, $\pi(\mathfrak{p}) = \left\langle \overline{f} \right\rangle$ where $\overline{f} \in \mathbb{F}_p[x]$ is irreducible. It follows that $\mathfrak{p} = \langle p, f \rangle$, where $f \in \mathbb{Z}[x]$ is such that $\overline{f} = \pi(f)$. □

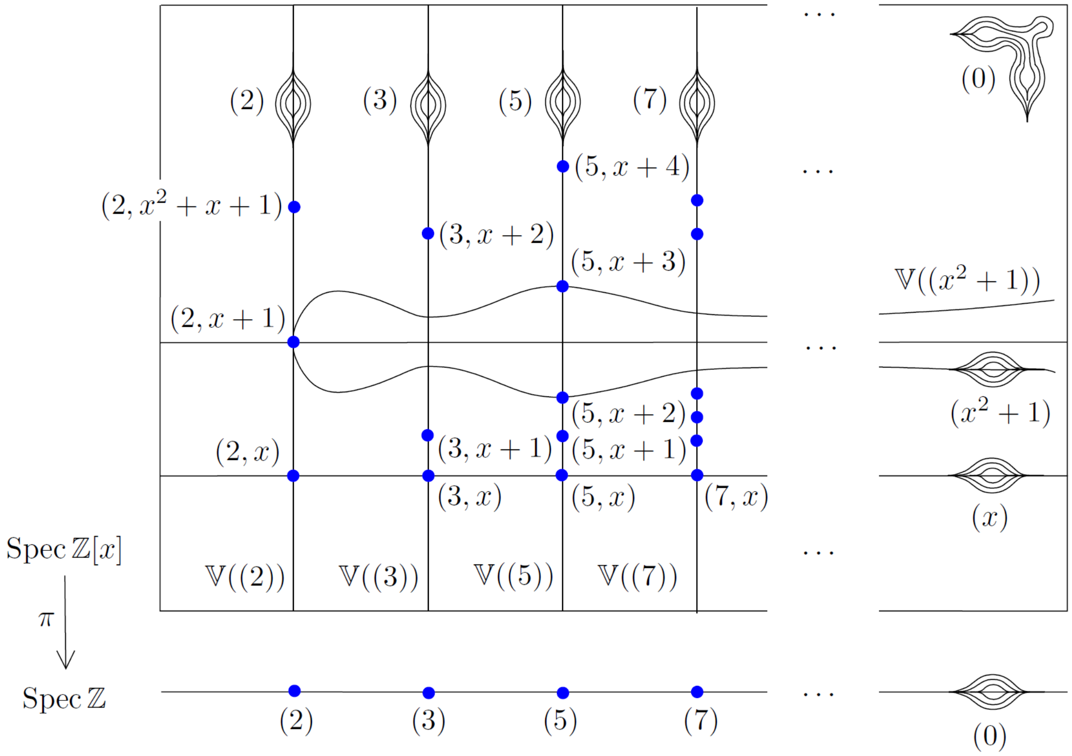

Figure 1: Mumford's picture of $\operatorname{Spec} \mathbb{Z}[x]$.