MA3G6 Commutative algebra :: Lecture notes

Lecturer: Diane Maclagan

Last edited: March 17, 2025

Contents

Week 1, lecture 1 starts here

What is this module about?

- Continuation of MA249,
- Back engine for algebraic geometry and (algebraic) number theory,
- Connection to other areas (combinatorics, applied maths, ...),
- Fun in its own right.

Recall

Definition 0.0.1. A *ring* $(R, +, \times)$ is a set R with binary operations $+ : R \times R \to R,\ \times : R \times R \to R$ such that

1. $(R, +)$ is an abelian group (identity denoted 0_R or given clear context simply 0),
2. $\times$ is associative and distributes over $+$,
3. $\exists 1_R \in R : 1_R \cdot a = a \cdot 1_R = a\ \forall a \in R$.

Within context of this module, we always add a 4th axiom:

4. $ab = ba\ \forall a, b \in \mathbb{R}$ commutativity

Example 0.0.2.
- $\mathbb{Z}$
- Polynomial ring
- $S = \mathbb{C}[x_1, \dots, x_n]$, $f \in S$, $f = \sum_{u \in \mathbb{N}^n} c_u x^u$, $c_u \in \mathbb{C}$, $x^u = x_1^{u_1} x_2^{u_2} \cdots x_n^{u_n}$ (this is called multiindex notation) and only finitely many $c_u \neq 0$. e.g. $x_1x_3 + 7x_2 \in \mathbb{C}[x_1, x_2, x_3]$ is written as $x^{(1,0,1)} + 7x^{(0,2,0)}$. One can also replace $\mathbb{C}$ with any field.

Definition 0.0.3. A *ring homomorphism* is a function $\varphi : R \to S$ where R, S rings that respects addition and multiplication: $\varphi(a + b) = \varphi(a) + \varphi(b)$, $\varphi(ab) = \varphi(a)\varphi(b)$ and $\varphi(1_R) = 1_S$.

The definition implies that homomorphisms preserve 0.

Definition 0.0.4. The *kernel* of a homomorphism φ is $\ker(\varphi) = \{a \in R : \varphi(a) = 0_S\}$.

Definition 0.0.5. A nonempty $I \subseteq R$ is an *ideal* if $a, b \in I \Rightarrow a + b \in I$ and $a \in I, r \in R \Rightarrow ra \in I$.

It immediately follows from the definition that kernel of $\varphi : R \to S$ is an ideal of R.

Example 0.0.6. $\varphi : \mathbb{Z} \to \mathbb{Z}/5\mathbb{Z}$ by $\varphi(n) = n \bmod 5$.

Definition 0.0.7. We say I is *generated* by $f_1, \dots, f_s \in R$ if

$$I = \left\{ \sum_{i=1}^{s} h_i f_i : h_i \in R \right\} =: \langle f_1, \dots, f_s \rangle$$

More generally, I is generated by $G \subseteq R$ if

$$I = \left\{ \sum_{i=1}^{s} h_i f_i : h_i \in R, f_i \in G, s \geq 0 \right\}.$$

This is closed under addition and multiplication by an element of R, hence an ideal.

Week 1, lecture 2 starts here

1 Gröbner basis

Example 1.0.1 (Motivating questions)**.** 1. Is $14 \in \langle 6, 26\rangle \subseteq Z$? Yes, since $14 = -2 \times 6 + 26$.

Do note that $\mathbb{Z}$ is a PID, and $\langle 6, 26\rangle = \langle 2\rangle$ where $2 = \gcd(6, 26)$.

2. Is $x + 7 \in \left\langle x^2 - 4x + 3, x^2 + x - 2\right\rangle \subseteq \mathbb{Z}[x]$? No, since $x^2 - 4x + 3 = (x - 1)(x - 3)$ and $x^2 + x - 2 = (x - 1)(x + 2)$, and $x - 1 \nmid x + 7$.
3. Is $x + 3y - 2z \in \langle x + y - z, y - z\rangle$? No, since any linear combination of the two generators have same coefficients for y and z. In linear algebra jargon, $(1, 3, -2)$ is not in rowspace of $\begin{pmatrix} 1 & 1 & -1 \\ 0 & 1 & -1 \end{pmatrix}$.

We do have enough specific knowledge to solve these, but not their general forms.

Example 1.0.2. Is $xy^2 - x \in \left\langle xy + 1, y^2 - 1\right\rangle$?

If we were not careful, we would try to divide $xy^2 - x$ by $xy + 1$ which leads to $xy^2 - x = y(xy + 1) + (-x - y)$, a dead end. But note that $xy^2 - x = x(y^2 - 1)$, which means it is in the ideal.

We now want to know how we can be 'careful'.

Definition 1.0.3. A *term order* (or monomial order) is a total order on monomials x^u in $S = K[x_1, \ldots, x_n]$ (where K is a field) such that

1. $1 \prec x^u \ \forall u \neq 0$
2. $x^u \prec x^v \Rightarrow x^{u+w} \prec x^{v+w} \ \forall u, v, w, \in \mathbb{N}^n$

Example 1.0.4. 1. Lexicographic term order: $x^u \prec x^v$ if the first nonzero element of $v - u$ is positive.

e.g. $x_2^2 \prec x_2^{10} \prec x_1 x_3 \prec x_1^2$. We can write them in multiindex notation:

$$x^{(0,2,0)}, x^{(0,10,0)}, x^{(1,0,1)}, x^{(2,0,0)},$$

and the result is clear. This is analogous to how we order words in a dictionary.

2. Degree lexicographic order: $x^u \prec x^v$ if $\deg(x^u) < \deg(x^v) = v_1 + \ldots + v_n$, or if they are equal, $x^u \prec_{\text{lex}} x^v$. e.g. $x_2^2 \prec x_1 x_3 \prec x_1^2 \prec x_2^{10}$.
3. (Degree) reverse lexicographic order (revlex): $x^u \prec x^v$ if $\deg(x^u) < \deg(x^v) = v_1 + \ldots + v_n$, or if they are equal, the last nonzero entry of $v - u$ is negative. e.g. $x_1 x_3 \prec x_2^2 \prec x_1^2 \prec x_2^{10}$.

Definition 1.0.5. Fix a term order $\prec$ on $K[x_1, \ldots, x_n]$. The *initial term* $\text{in}_\prec(f)$ of a polynomial $f = \sum c_u x^u$ is $c_v x^v$ if $x^v = \max_\prec\{x^u : c_u \neq 0\}$.

Example 1.0.6. Let $f = 3x^2 - 8xz^9 + 9y^{10}$. Then

- If $\prec =$ lex, $\text{in}_\prec(f) = 3x^2$
- If $\prec =$ deglex, $\text{in}_\prec(f) = -8xz^9$
- If $\prec =$ revlex, $\text{in}_\prec(f) = 9y^{10}$

Definition 1.0.7. Let $I \subseteq S$ be an ideal. The *initial ideal* of I is $\text{in}_\prec(I) := \langle \text{in}_\prec(f) : f \in I\rangle$.

Remark. If $I = \langle f_1, \ldots, f_s\rangle$ then $\langle \text{in}_\prec(f_1), \ldots, \text{in}_\prec(f_s)\rangle \subseteq \text{in}_\prec(I)$, but not necessarily equal.

Example 1.0.8. $I = \langle x + y + z, x + 2y + 3z\rangle$. Then $\text{in}_\prec(f_1) = \text{in}_\prec(f_2) = x$, so $\langle \text{in}_\prec(f_1)\text{in}_\prec(f_2)\rangle = \langle x\rangle$, but $y + 2z \in I$, $\text{in}_\prec(y + 2z) = y \notin \langle x\rangle$.

Definition 1.0.9. A set $\{g_1, \ldots, g_s\} \subseteq I$ is a *Gröbner basis* for I if $\text{in}_\prec(I) = \langle \text{in}_\prec(g_1), \ldots, \text{in}_\prec(g_s)\rangle$.

With this language, we can express Example 1.0.8 by saying '$\{x + y + z, x + 2y + 3z\}$ is not a Gröbner basis of the ideal'. We will see that every ideal in S has a Gröbner basis, and long division using a Gröbner basis solves the ideal membership problem ($f \in I$ iff the remainder on dividing by the Gröbner basis is 0).

Week 2, lecture 1 starts here

1.1 Division algorithm

Let $S = K[x_1, \dots, x_n]$.

- Input: $f_1, \dots, f_s, f \in S$ and $\prec$ the term order
- Output: an expression $f = \sum_{i=1}^{s} h_i f_i + r$, where
  1. $h_i, r \in S,\ r = \sum c_u x^u$
  2. If $c_u \neq 0$, then x^u is not divisible by any $\mathrm{in}_\prec(f_i)$
  3. If $\mathrm{in}_\prec(f) = c_u x^u,\ \mathrm{in}_\prec(h_i f_i) = c_{v_i} x^{v_i}$ then $x^u \succeq x^{v_i}\ \forall i$
- The algorithm:
  1. Initialize: $h_1, \dots, h_s = 0,\ r = 0,\ p = f,\ f = p + \sum h_i f_i + r$.
  2. Loop: At each stage, if $\mathrm{in}_\prec(p)$ is divisible by some $\mathrm{in}_\prec(f_i)$, subtract $\frac{\mathrm{in}_\prec(p)}{\mathrm{in}_\prec(f_i)} f_i$ from p and add $\frac{\mathrm{in}_\prec(p)}{\mathrm{in}_\prec(f_i)}$ to h_i.
     If $\mathrm{in}_\prec(p)$ is not divisible by any $\mathrm{in}_\prec(f_i)$, subtract it from p and add it to r.
  3. Termination: stop when $p = 0$ and output $h_1, \dots, h_s, r$.

Example 1.1.1. $f = \underline{x} + 2y + 3z,\ f_1 = \underline{x} + y + z,\ f_2 = \underline{5y} + 3z$, term order is $\prec_{\mathrm{lex}}$ and $x \succ y \succ z$.

1. Initialize: $h_1 = h_2 = r = 0,\ p = x + 2y + 3z$
2. 1st loop: The underlined are initial terms, and $\mathrm{in}_\prec(p) = x$ is divisible by $\mathrm{in}_\prec(f_1) = x$, so
$$p = p - \frac{\mathrm{in}_\prec(p)}{\mathrm{in}_\prec(f_1)} f_1 = x + 2y + 3z - (x + y + z) = y + 2z$$
   and $h_1 = 0 + \frac{\mathrm{in}_\prec(p)}{\mathrm{in}_\prec(f_1)} = 1$.
3. 2nd loop: $\mathrm{in}_\prec(p) = y$ is divisible by $\mathrm{in}_\prec(f_2) = 5y$, so
$$p = p - \frac{\mathrm{in}_\prec(p)}{\mathrm{in}_\prec(f_2)} f_2 = y + 2z - \frac{1}{5}(5y + 3z) = \frac{7}{5}z$$
   and $h_2 = 0 + \frac{\mathrm{in}_\prec(p)}{\mathrm{in}_\prec(f_2)} = \frac{1}{5}$.
4. Termination: $\mathrm{in}_\prec(p) = \frac{7}{5}z$ is not divisible by any $\mathrm{in}_\prec(f_i)$, so
$$p - \mathrm{in}_\prec(p) = 0,\ r = \mathrm{in}_\prec(p) = \frac{7}{5}z$$
   and we have the expression
$$x + 2y + 3z = 1(x + y + z) + \frac{1}{5}(5y + 3z) + \frac{7}{5}z.$$

Example 1.1.2. Divide $f = x^2$ by $f_1 = x + y + z$ and $f_2 = y - z$ with $\prec_{\mathrm{lex}}$ and $x \succ y \succ z$.

1. $h_1 = h_2 = r = 0,\ p = f = x^2$
2. $p = p - \frac{\mathrm{in}_\prec(p)}{\mathrm{in}_\prec(f_1)} f_1 = x^2 - \frac{x^2}{x}(x + y + z) = -xy - xz,\ h_1 = 0 + x = x$
3. $p = p - \frac{\mathrm{in}_\prec(p)}{\mathrm{in}_\prec(f_1)} f_1 = -xy - xz - (-y)(x + y + z) = -xz + y^2 + yz,\ h_1 = h_1 - y = x - y$
4. $p = p - \frac{\mathrm{in}_\prec(p)}{\mathrm{in}_\prec(f_1)} f_1 = -xz + y^2 + yz + z(x + y + z) = y^2 + 2yz + z^2,\ h_1 = h_1 - z = x - y - z$
5. $p = p - \frac{\mathrm{in}_\prec(p)}{\mathrm{in}_\prec(f_2)} f_2 = y^2 + 2yz + z^2 - y(y - z) = 3yz + z^2,\ h_2 = 0 + y = y$
6. $p = p - \frac{\mathrm{in}_\prec(p)}{\mathrm{in}_\prec(f_2)} f_2 = 3yz + z^2 - 3z(y - z) = 4z^2,\ h_2 = h_2 + 3z = y + 3z$
7. $4z^2$ not divisible by any $\mathrm{in}_\prec(f_i)$, so terminate. $p = p - \mathrm{in}_\prec(p),\ r = \mathrm{in}_\prec(p)$, output $h_1 = x - y - z,\ h_2 = y + 3z,\ r = 4z^2$, and check:
$$x^2 = (x - y - z)(x + y + z) + (y + 3z)(y - z) + 4z^2.$$

The coming punchline is that if f_i's are a Gröbner basis then remainder r is unique.

Lemma 1.1.3. Let $I = \langle x^u : u \in A \rangle$ for some $A \subseteq \mathbb{N}^n$, then

1. $x^v \in I$ iff $x^u \mid x^v$ for some $u \in A$
2. if $f = \sum c_v x^v \in I$, then each x^v is divisible by x^u for some $u \in A$

Proposition 1.1.4. If $\{g_1, \ldots, g_s\}$ is a Gröbner basis for I with respect to $\prec$, then $f \in I$ iff the division algorithm dividing f by $g_1, \ldots, g_s$ gives remainder 0.

Proof. $\Rightarrow$ Division algorithm writes $f = \sum h_i g_i + r$, so if $r = 0$ we have $f \in I$.

$\Leftarrow$ We prove the contrapositive: suppose $r \neq 0$. If $f \in I$ then $r \in I$, so $\mathrm{in}_\prec(r) \in \mathrm{in}_\prec(I)$. But by construction, $\mathrm{in}_\prec(r)$ is not divisible by $\mathrm{in}_\prec(g_i)$ for any i. This contradicts that $\mathrm{in}_\prec(I) = \langle \mathrm{in}_\prec(g_1), \ldots, \mathrm{in}_\prec(g_s) \rangle$. $\square$

Week 2, lecture 2 starts here (Chunyi Li)

2 Noetherian ring

Definition 2.0.1. A ring R is *Noetherian* if every ideal of R is finitely generated.

Example 2.0.2.

1. $\mathbb{R}$ and $\mathbb{C}$ are fields, so they only have two ideals $\langle 0 \rangle, \langle 1 \rangle$, so Noetherian.
2. $\mathbb{Z}$ and $\mathbb{C}[x]$ are principal ideal domains, this implies they are Noetherian.
3. $\mathbb{C}[x, y]$ and $\mathbb{Z}[x]$?
4. $R := \{f : \mathbb{R} \to \mathbb{R} : f \text{ continuous}\}$, probably not?
5. $\mathbb{C}[x_1, \ldots, x_n, \ldots] = \bigcup_{n=1}^{\infty} \mathbb{C}[x_1, \ldots, x_n]$, a polynomial ring which has infinite variables but finite nonzero terms.

Definition 2.0.3. A ring R satisfies *ascending chain condition* (ACC) if every chain of ideals $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$ eventually stabilizes, i.e. $\exists n \in \mathbb{N} : I_m = I_n \ \forall m \geq n$, i.e. $\nexists$ strictly ascending chain of ideals $I_1 \subsetneqq I_2 \subsetneqq \cdots \subsetneqq I_n \subsetneqq \cdots$.

Proposition 2.0.4. R is Noetherian iff R satisfies ACC.

Proof. $\Rightarrow$ Let $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots \lhd R$ and consider $J = \bigcup_{k=1}^{\infty} I_k$. Note $\forall r, s \in J,\ r \in I_j,\ s \in I_t$. WLOG assume $j \leq t$, then $r, s \in I_t$ and $r \pm s \in I_t \subset J$, and more generally $J \lhd R$. Since J is finitely generated, we write $J = \langle f_1, \ldots, f_m \rangle$. By definition $f_i \in I_{n_i}$, so $\exists N : f_i \in I_N \ \forall i$, implying $J \subseteq I_N$. But J is already the union of all ideals, so the chain must stabilize at I_N.

$\Leftarrow$ Let $I \lhd R$ and suppose I is not finitely generated. We know $\exists f_1 \neq 0 \in I$ and $I \neq \langle f_1 \rangle$, also $\exists f_2 \in I \setminus \langle f_1 \rangle$ and $I \neq \langle f_1, f_2 \rangle$. We can keep doing this and in general

$$\exists f_{n+1} \subset I \setminus \langle f_1, \ldots, f_n \rangle \Rightarrow I \neq \langle f_1, \ldots, f_{n+1} \rangle \quad \forall n \in \mathbb{N}$$

This gives us a strictly ascending chain $\langle f_1 \rangle \subsetneqq \langle f_1, f_2 \rangle \subsetneqq \cdots \subsetneqq \langle f_1, \ldots, f_n \rangle \subsetneqq \cdots$ which is a contradiction. $\square$

Example 2.0.5.

1. We now know the 4th of Example 2.0.2 is not Noetherian, since
$$\langle \sin x \rangle \subsetneqq \left\langle \sin \frac{x}{2} \right\rangle \subsetneqq \left\langle \sin \frac{x}{4} \right\rangle \subsetneqq \cdots \subsetneqq \left\langle \sin \frac{x}{2^n} \right\rangle \subsetneqq \cdots$$
is a strictly ascending chain or ideals.
2. Also,
$$\langle x_1 \rangle \subsetneqq \langle x_1, x_2 \rangle \subsetneqq \cdots \subsetneqq \langle x_1, \ldots, x_n \rangle \subsetneqq \cdots$$
so the 5th is also not Noetherian.

Theorem 2.0.6 (1st isomorphism theorem)**.** Let R, S be rings. If $\varphi : R \to S$ is a ring homomorphism then $\text{im}\,\varphi \cong R/\ker\varphi$. If φ is surjective then $\text{im}\,\varphi = S$ so we have $S \cong R/\ker\varphi$.

$\forall I \lhd R$, R/I is a ring, and there is a natural surjective homomorphism $\varphi : R \to R/I$ defined by $r \mapsto r + I$. Note that $I = \ker\varphi$, so this is a isomorphism.

Theorem 2.0.7 (4th isomorphism theorem)**.** For the same φ as above, there is a 1-1 correspondence

$$\varphi^{-1} : \{J \lhd R/I\} \to \{\widetilde{J} \lhd R : J \supseteq I \lhd R\}.$$

Proposition 2.0.8. If R is Noetherian then R/I is Noetherian $\forall I \lhd R$.

Week 2, lecture 3 starts here

Proof. Suppose $\exists J_1 \subsetneqq \cdots \subsetneqq J_n \subsetneqq \cdots \lhd R/I$. Then by 4th isomorphism theorem,

$$\exists \varphi^{-1}(J_1) \subsetneqq \cdots \subsetneqq \varphi^{-1}(J_n) \subsetneqq \cdots \lhd R,$$

a contradiction. $\square$

Theorem 2.0.9 (Hilbert basis theorem)**.** If R is Noetherian then $R[x]$ is Noetherian.

Proof (nonexaminable). Let $I \lhd R[x]$. Suppose I is not finitely generated. $\exists f_1 \in I$ with the minimal degree such that $I \neq \langle f_1 \rangle$. Now choose $f_2 \in I \setminus \langle f_1 \rangle$ with the minimal degree so that $I \neq \langle f_1, f_2 \rangle$. We proceed inductively and have

$$\exists f_{n+1} \in I \setminus \langle f_1, \ldots, f_n \rangle \text{ with minimal degree so that } I \neq \langle f_1, \ldots, f_{n+1} \rangle .$$

For every f_i we can write $f_i = r_i x^{n_i}$+lower degree terms and $n_1 \leq n_2 \leq \cdots n_m \leq \cdots$. We now claim that

$$\langle r_1 \rangle \subsetneqq \langle r_1, r_2 \rangle \subsetneqq \cdots \subsetneqq \langle r_1, \ldots, r_m \rangle \subsetneqq \cdots$$

is a strictly ascending chain of ideals in R, which gives a contradiction. To see this, suppose $r_{m+1} \in \langle r_1, \ldots, r_m \rangle$, i.e.

$$r_{m+1} = s_1 r_1 + \cdots + s_m r_m \quad \text{for some } s_1, \ldots, s_m \in R,$$

Now consider

$$\widetilde{f}_{m+1}(x) := f_{m+1}(x) - s_1 x^{n_{m+1}-n_1} f_1(x) - s_2 x^{n_{m+1}-n_2} f_2(x) - \cdots - s_m x^{n_{m+1}-n_m} f_m(x),$$

whose leading terms cancel and $\deg \widetilde{f}_{m+1} < \deg f_{m+1}$. But $\widetilde{f}_{m+1}$ still satisfies that it's not in $\langle f_1, \ldots, f_m \rangle$, contradicting the minimality of $\deg f_{m+1}$. $\square$

Corollary 2.0.10. If R is Noetherian then $R[x_1, \ldots, x_n]$ is Noetherian.

Proof. One knows $R[x]$ is Noetherian. Now assume $R[x_1, \ldots, x_m]$ is Noetherian. Then

$$R[x_1, \ldots, x_{m+1}] = (R[x_1, \ldots, x_m])[x_{m+1}]$$

is Noetherian, so by induction one has what's desired. $\square$

Example 2.0.11.

1. $\mathbb{Z}$ is a PID, so Noetherian, so $\mathbb{Z}[x]$ is Noetherian.
2. $\mathbb{Z}[\sqrt{5}] \cong \mathbb{Z}[x]/\left\langle x^2 - 5 \right\rangle$ is Noetherian.
3. $\mathbb{Z}[\sqrt{5}, \sqrt[4]{7}] \cong \mathbb{Z}[x, y]/\left\langle x^2 - 5, x^4 - 7 \right\rangle$ is Noetherian.
4. We have already seen that all fields are Noetherian, and any ring is a subring of its field of fractions. So it's not true that a subring of a Noetherian ring is Noetherian.

Definition 2.0.12. An ideal $I \lhd R$ is *prime* if

1. $I \neq R$
2. $\forall fg \in I,\ f$ or $g \in I$

Example 2.0.13. In $\mathbb{Z}$, $\langle p \rangle$ where p prime is a prime ideal by Euclid's lemma. Also $\langle 0 \rangle$ is prime, but $\langle 1 \rangle$ is not since it's the whole ring.

Week 3, lecture 1 starts here

2.1 Every ideal I in $\mathbb{C}[x_1, \ldots, x_n]$ has a finite Gröbner basis

Proof of Lemma 1.1.3. Note that 1 is a special case of 2, so it suffices to prove the latter.

If $f \in I$ write $f = \sum c_v x^v = \sum_{u \in A} h_u x^u$ with only finitely many $h_u \neq 0$. We expand the RHS as a sum of monomials, each monomial is divisible by some x^u with $u \in A$. Hence the same is true for x^v with $c_v \neq 0$ since these are terms remaining after cancellation. $\square$

Theorem 2.1.1 (Dickson's lemma)**.** Let $I = \langle x^u : u \in A \rangle \subseteq S = K[x_1, \ldots, x_n]$ for some $A \subseteq \mathbb{N}^n$. Then $\exists a_1, \ldots, a_s \in A$ with $I = \langle x^{a_1}, \ldots, x^{a_s} \rangle$.

Before diving into the proof let's think about two special cases.

$n = 1$ Consider $I = \left\langle x_1^3, x_1^7, x_1^{70000}, x_1^{1234}, \ldots \right\rangle$. One can see that x_1^3 is sufficient to generate the whole I.

$n = 2$ Consider $u, v \in \mathbb{N}^2$ as points on a lattice grid. Then x^u is divisible by x^v if it's top right of it, so we can get rid of unnecessary ones in a similar fashion.

Now let's turn these intuitions into a general proof.

Proof by induction. Straightforwardly, when $n = 1$, $I = \langle x_1^{\alpha_1} \rangle$ for $\alpha = \min\{j : x_j^I\}$. Now assume $n > 1$ and the theorem is true for $n - 1$.

Write the variables in S as $x_1, \ldots, x_{n-1}, y$ and let I be an ideal in S. Let $J = \langle x^u : x^u y^c \in I \text{ for some } c \geq 0 \rangle \subseteq K[x_1, \ldots, x_{n-1}]$. By inductive hypothesis, J is finitely generated, so write $J = \langle x^{a_{m_1}}, \ldots, x^{a_{m_r}} \rangle$ for $x^{a_{m_i}} y^{m_i} \in I$. Let $m = \max\{m_i\}$. For $0 \leq l \leq m-1$, let $J_l = \left\langle x^u : x^u y^l \in I \right\rangle \subseteq K[x_1, \ldots, x_{n-1}]$. Again J_l is finitely generated and write $J_l = \langle x^{a_{j_1}}, \ldots, x^{a_{j_{r_l}}} \rangle$. We claim that I is generated by $\{x^{a_{m_i}} y^{m_i} : 1 \leq i \leq r\} \cup \{x^{a_{j_i}} y^j : 1 \leq j \leq m-1,\ 1 \leq i \leq r_j\}$. Indeed, if $x^u y^j \in I$ then either

1. $j < m$, so $x^u \in J_j$, so $x^{j_i} \mid x^u$ for some i, and so $x^{a_{j_i}} y^j \mid x^u y^j$.
2. $j \geq m$, so $x^u \in J$, so $x^{a_{m_i}} \mid x^u$ for some i, and so since $m_i \leq m$, $x^{a_{m_i}} y^{m_i} \mid x^u y^j$.

So every monomial in I is a multiple of one of the claimed generators.

If any of these generators is not in our original set A, we can replace it by a monomial with exponent in A, and by Lemma 1.1.3 if they generate all monomials then they generate the whole I. $\square$

Week 3, lecture 2 starts here

Corollary 2.1.2. Every ideal in $S = K[x_1, \ldots, x_n]$ has a finite Gröbner basis with respect to a term order.

Proof. The initial ideal in $\text{in}_\prec(I) = \langle \text{in}_\prec(f) : f \in I \rangle$ is a monomial ideal (using that coefficients can be omitted since we are in a field). By Dickson's lemma, there are $g_1, \ldots, g_s \in I$ with $\langle \text{in}_\prec(g_1), \ldots, \text{in}_\prec(g_s) \rangle = \text{in}_\prec(I)$. Thus $\{g_1, \ldots, g_s\}$ is a Gröbner basis for I by definition. $\square$

Proposition 2.1.3. If $\{g_1, \ldots, g_2\}$ is a Gröbner basis for I with respect to $\prec$, then $I = \langle g_1, \ldots, g_2 \rangle$.

Proof. By division algorithm, any $f \in I$ can be written as $f = \sum h_i g_i$ with remainder 0 since $f \in I$. It follows that $f \in \langle g_1, \ldots, g_s \rangle$, which gives the desired since f is arbitrary. $\square$

Corollary 2.1.4 (Special case of Hilbert basis theorem)**.** Every ideal in $S = K[x_1, \ldots, x_n]$ is finitely generated.

Proof. Immediate from previous two results. $\square$

Exercise 2.1.5. Claim: $y = \left\{ \underline{x_2^2} - x_1 x_3, \underline{x_2 x_3} - x_1 x_4, \underline{x_3^2} - x_2 x_4 \right\}$ is a Gröbner basis with respect to revlex. Find the remainder on dividing $x_2^2 x_3^2$ by y.

$$\begin{aligned}
f_1 :& x_2^2 x_3^2 \xrightarrow{f_1} x_1 x_3 \xrightarrow{f_3} x_1 x_2 x_3 x_4 \xrightarrow{f_2} x_1^2 x_4^2 \\
f_2 :& x_2^2 x_3^2 \xrightarrow{f_2} x_1 x_2 x_3 x_4 \xrightarrow{f_2} x_1^2 x_4^2 \\
f_3 :& x_2^2 x_3^2 \xrightarrow{f_3} x_2^3 x_4 \xrightarrow{f_1} x_1 x_2 x_3 x_4 \xrightarrow{f_2} x_1^2 x_4^2
\end{aligned}$$

The remainders are the same: this shouldn't surprise us. But we haven't proved it, so why did this work?

3 General commutative ring

Definition 3.0.1. An ideal $I \subseteq R$ is *prime* if it's proper and $f, g \in I \Rightarrow f$ or $g \in I$.

Notation. $\operatorname{Spec}(R) := \{\text{prime ideals in } R\}$.

Example 3.0.2. $R = \mathbb{Z}/6\mathbb{Z}$, $\operatorname{Spec}(R) = \{\langle 2\rangle, \langle 3\rangle\}$. Note that although 5 is prime but $\langle 5\rangle$ is not a prime ideal since $5^2 = 1$ in $\mathbb{Z}/6\mathbb{Z}$ so it's not proper.

Lemma 3.0.3. An ideal $P \subseteq R$ is prime iff R/P is a domain.

Proof. P is prime iff

$$fg \in P \Rightarrow f \text{ or } g \in P. \tag{$*$}$$

R/P is a domain iff $fg + P = 0 + P \Rightarrow f + P$ or $g + P = 0 + P$, which is equivalent to $(*)$. □

Definition 3.0.4. An ideal $I \subseteq R$ is *maximal* if it's proper and there is no ideal $J : I \subsetneqq J \subsetneqq R$.

Do maximal ideals always exist? Yes, if we assume axiom of choice.

Recall: a *partially ordered* set is a set S with transitive, reflexive binary relation $\leq$ (e.g. $\leq$ on $\mathbb{R}$ or power set (inclusion)). Given a subset $U \subseteq S$, an *upper bound* for U is $s \in S$ with $u \leq s\ \forall u \in U$. An element $m \in S$ is *maximal* if $\nexists s \in S$ with $s > m$.

Axiom 3.0.5 (Zorn's lemma)**.** Let S be a nonempty partially ordered set with the property that any totally ordered subset $U \subseteq S$ (a 'chain') has an upper bound. Then S has a maximal element.

This is equivalent to:

1. The axiom of choice: every product $\prod_{a\in A} S_a$ of nonempty sets is nonempty.
2. Well-ordering principle: every set can be well-ordered.

Week 3, lecture 3 starts here

Proposition 3.0.6. Let R be a ring and let I be a proper ideal of R. Then there is a maximal ideal M containing I.

Proof. Let $\mathcal{I}$ be the set of proper ideals in R containing I, ordered by inclusion ($J_1 \leq J_2$ if $J_1 \subseteq J_2$). Note that if $\{J_\alpha : \alpha \in A\}$ is a totally ordered (any two are comparable) subset of $\mathcal{I}$ then $J = \bigcup_{\alpha\in A} J_\alpha$ is an ideal. [$\lightning$ this uses the total order, e.g. in $K[x, y]$, $\langle x\rangle \cup \langle y\rangle$ is not an ideal since $x + y$ is not in there.] Since $J_\alpha \subseteq J\ \forall\alpha$ and $I \subseteq J$, one has $J \in \mathcal{I}$. Hence J is an upper bound for $\{J_\alpha\}$. Thus by Zorn's lemma, $\mathcal{I}$ has a maximal element. □

Lemma 3.0.7. $I \subseteq R$ is maximal iff R/I is a field.

Proof. Exercise (see Algebra II notes). □

Corollary 3.0.8. Maximal ideals are prime.

Proof. If I is maximal then R/I is a field, and in particular a domain. □

3.1 Localisation

Definition 3.1.1. A ring R is *local* if it has a unique maximal ideal M.

Example 3.1.2. Every field is local. $\mathbb{Z}$ is not local since $\langle 2\rangle, \langle 3\rangle$ are both maximal.
Consider

$$\mathbb{Z}_{\langle 2\rangle} := \left\{\frac{a}{b} \in \mathbb{Q} : a, b \in \mathbb{Z},\ 2 \nmid b\right\}.$$

This is a subring of $\mathbb{Q}$. Note that proper ideals are those generated by even integers, but $\langle 6\rangle = \langle 2\rangle$ since $\frac{1}{3} \in \mathbb{Z}_{\langle 2\rangle}$. So in fact they are all generated by powers of 2, and $\langle 2\rangle$ is maximal, so $\mathbb{Z}_{\langle 2\rangle}$ is local.

$\mathbb{C}[x]$ is not local, since we can build (at least two) quotient rings which is a field by first isomorphism theorem, e.g. $\varphi_1 : x \to 1$ and $\varphi_2 : x \to i$.
Now consider

$$\mathbb{C}[x]_{\langle x\rangle} := \left\{\frac{f}{g} : f, g \in \mathbb{C}[x],\ x \nmid g\right\}.$$

This is analogous to $\mathbb{Z}_{\langle x\rangle}$ and its proper ideals are of the form $\langle x^j\rangle$ with $\langle x\rangle$ being maximal.

Definition 3.1.3. A set $U \subseteq R$ is *multiplicatively closed* if $1 \in U$ and $f, g \in U \Rightarrow fg \in U$.

Example 3.1.4. In any R with $f \in R,\ U = \{1, f, f^2, \dots\}$ is multiplicatively closed.
Suppose $P \subseteq R$ is prime. Then $1 \notin P$, i.e. $1 \in R \backslash P$, and $fg \in P \Rightarrow f$ or $g \in P$, so $f, g \in R\backslash P \Rightarrow fg \in R\backslash P$. By definition this means R/P is multiplicatively closed.
$U = \{r \in R : \exists s \in R : rs = 1\} = \{\text{units of } R\}$ is multiplicatively closed. In particular, if R is a domain then $U = R\backslash\{0\}$ is.

Definition 3.1.5. Let R be a ring and let $U \subseteq R$ be multiplicatively closed. Then

$$R\left[U^{-1}\right] := \left\{\frac{r}{u} : r \in R, u \in U\right\}$$

modulo the equivalence relation $\sim$

$$\frac{r}{u} \sim \frac{r'}{u'} \quad \text{if} \quad \exists \widetilde{u} \in U : \widetilde{u}(ru' - r'u) = 0.$$

Example 3.1.6. $R = \mathbb{Z},\ U = \mathbb{Z}\backslash\{0\}$. Then $R\left[U^{-1}\right] = \mathbb{Q}$. We don't have to worry about the $\widetilde{u}$ condition since $\mathbb{Z}$ is a domain.
$R = \mathbb{Z},\ U = \mathbb{Z}\backslash\langle 2\rangle$. Then $R[U^{-1}] = \mathbb{Z}_{\langle 2\rangle}$.
$R = \mathbb{C}[x],\ U = \mathbb{C}[x]\backslash\langle x\rangle$. Then $R[U^{-1}] = \mathbb{C}[x]_{\langle x\rangle}$.

Week 4, lecture 1 starts here

Lemma 3.1.7.

1. The $\sim$ in Definition 3.1.5 is indeed an equivalence relation.
2. $R[U^{-1}]$ is a ring with addition and multiplication defined
$$\frac{r}{u} + \frac{r'}{u'} := \frac{ru' + r'u}{uu'}, \quad \left(\frac{r}{u}\right)\left(\frac{r'}{u'}\right) := \frac{rr'}{uu'}$$
3. The map $\varphi : R \to R[U^{-1}]$ given by $r \mapsto \frac{r}{1}$ is a ring homomorphism.

Proof.

1. It's reflexive since $1(ru - ru) = 0$. It's symmetric since $\widetilde{u}(ru' - r'u) = 0 \Rightarrow -1\widetilde{u}(r'u - ru') = 0$ and $-1\widetilde{u} \in U$ by multiplicative closedness.
Now suppose
$$\frac{r}{u} \sim \frac{r'}{u'}, \quad \frac{r'}{u'} \sim \frac{r''}{u''},$$
then $\exists \widetilde{u} \in U : \widetilde{u}(ru' - r'u) = 0$ and $\exists \widetilde{u}' \in U : \widetilde{u}'(r'u'' - r''u') = 0$. So
$$\widetilde{u}'u''(\widetilde{u}(ru' - r'u)) + \widetilde{u}u(\widetilde{u}'(r'u'' - r''u')) = 0.$$
which is equal to
$$\widetilde{u}\widetilde{u}'(ru'u'' - r'uu'' + r'uu'' - r''uu') = \widetilde{u}\widetilde{u}'u'(ru'' - r''u)$$
where $\widetilde{u}\widetilde{u}'u' \in U$. Therefore it's transitive.
2. (Exercise) One needs to check:
   - The two operations are well-defined, i.e. they don't depend on choice of representatives
   - Ring axioms, in particular $\frac{0}{1}$ is additive identity and $\frac{1}{1}$ is multiplicative identity
3. One has $\varphi(r + r') = \frac{r+r'}{1} = \frac{r}{1} + \frac{r'}{1} = \varphi(r) + \varphi(r')$ and $\varphi(rr') = \frac{rr'}{1} = \left(\frac{r}{1}\right)\left(\frac{r'}{1}\right) = \varphi(r)\varphi(r')$.

□

Remark.

1. If U contains 0 then it's very boring: $R[U^{-1}] = 0$ iff $0 \in U$. Indeed, for $R[U^{-1}] = 0$ one needs $\exists u \in U : u \cdot 1 = 0$, and the only such u is 0, and if $0 \in U$ then $0(r \cdot 1 - 0 \cdot 1) = 0r = 0\ \forall r$ hence $\frac{r}{1} \sim \frac{0}{1}\ \forall r$.
2. φ is not always injective, e.g. $R = \mathbb{Z}/6\mathbb{Z},\ U = \{1, 3, 5\}$. Then $\varphi(2) = \frac{2}{1}$ but $\frac{2}{1} \sim \frac{0}{1}$ since $3(2\times 1 - 0\times 1) = 0$. Furthermore, $\ker\varphi = \left\{r \in R : \frac{r}{1} \sim \frac{0}{1}\right\} = \{r \in R : \exists u \in U : ur = 0\}$.

Notation (Important special case)**.** In the case of $U = R\backslash P$ where P is prime, we write R_P for $R[(R\backslash P)^{-1}]$. An example would be, again, $\mathbb{Z}_{\langle 2\rangle}$.

Why is this important?

Proposition 3.1.8. The set $P_P := \left\{\frac{r}{u} \in R_P : r \in P\right\}$ is an ideal of R_P and is the unique maximal ideal.

Proof. If $\frac{r}{u} \notin P_P$ then $r \notin P$, so $\frac{u}{r} \in R_P$ and hence $\frac{r}{u}$ is a unit. Now suppose there is a maximal ideal I and in particular $\exists \frac{r}{u} \in I \backslash P_P$. But then I would be the whole ring R_P since it contains a unit. This argument also justifies that P_P is maximal itself. $\square$

Corollary 3.1.9 (A fortunate byproduct of the proof)**.** $I \subseteq R$ is the unique maximal ideal iff every $r \notin I$ is a unit.

Week 4, lecture 2 starts here

3.1.1 Effect of localisation on ideals

We want to investigate the relationship between $\mathrm{Spec}(R)$ and $\mathrm{Spec}(R[U^{-1}])$.

We have the ring homomorphism φ, but $I \mapsto \varphi(I) := \{\varphi(r) : r \in I\}$ is not good enough, since if $R = \mathbb{Z},\ U = \mathbb{Z}\backslash\{0\}$ then $R[U^{-1}] = \mathbb{Q}$ is a field, so it has only two ideals, and $\varphi(I) = \left\{\frac{n}{1} : n \text{ even}\right\}$ obviously is not one of them. Rather we need $I \mapsto \varphi(I)R[U^{-1}] := \langle \varphi(r) : r \in I\rangle$. In the above case, $\varphi(I)R[U^{-1}] = \mathbb{Q}$.

For the other way, we can simply consider $J \mapsto \varphi^{-1}(J)$ as a map without the 'generated by'.

Lemma 3.1.10. There is a bijection between ideals $J \subseteq R[U^{-1}]$ and ideals $I \subseteq R$ with property

$$ru \in I \text{ for some } u \in U \Rightarrow r \in I. \tag{$\star$}$$

Example 3.1.11. In the above example, $\langle 6\rangle$ is not such ideal $I \subseteq \mathbb{Z}$ since $6 = 6 \times 1 \in \langle 6\rangle,\ 6 \in U$ but $1 \notin \langle 6\rangle$. Note that this argument works for any $\langle n\rangle$ where $n > 1$. In fact, the only two ideals that satisfy this are $\langle 0\rangle, \langle 1\rangle$ which indeed have a natural bijection to ideals in $\mathbb{Q}$.

Proof. To show $J \mapsto \varphi^{-1}(J)$ is injective, we show $\varphi(\varphi^{-1}(J))R[U^{-1}] = J$.

$\subseteq$ is clear: $\varphi^{-1}(J) = \left\{r : \frac{r}{1} \in J\right\}$, so $\varphi(\varphi^{-1}(J)) = \left\{\frac{r}{1} : \frac{r}{1} \in J\right\}$, and if you take the ideal generated by a subset of J of course you get something contained in J.

To see $\supseteq$, note that

$$\frac{r}{u} \in J \Rightarrow \frac{u}{1}\frac{r}{u} = \frac{r}{1} \in J,$$

so $r \in \varphi^{-1}(J)$ and $\frac{r}{1} \in \varphi(\varphi^{-1}(J))R[U^{-1}]$ and furthermore for any

$$u \in U, \quad \frac{1}{u}\frac{r}{1} = \frac{r}{u} \in \varphi(\varphi^{-1}(J))R[U^{-1}].$$

To show $J \mapsto \varphi^{-1}(J)$ is surjective, fix $I \subseteq R$ satisfying $\star$ and let $J = \varphi(I)R[U^{-1}]$. The proof is then complete if we show $I = \varphi^{-1}(J)$.

$\frac{r}{1} \in \varphi(I)R[U^{-1}]$ means

$$\begin{aligned} \frac{r}{1} &= \sum \frac{h_i}{u_i}\frac{r_i}{1} \text{ where } r_i \in I,\ h_i \in R,\ u_i \in U \\ &= \frac{\widetilde{r}}{u} \text{ for some } \widetilde{r} \in I,\ u \in U. \end{aligned}$$

By definition, this implies $\exists \widetilde{u} \in U : \widetilde{u}(ur - \widetilde{r}) = 0$, i.e. $(\widetilde{u}u)r = \widetilde{u}\widetilde{r} \in I$ since $\widetilde{r} \in I$. By assumption, $r \in I$. This shows $\varphi^{-1}(J) \subseteq I$, and since $\frac{r}{1} \in J\ \forall r \in I,\ I \subseteq \varphi^{-1}(J)$. $\square$

Exercise 3.1.12 ($*$)**.** What ideals $I \subseteq \mathbb{Z}$ satisfy $\star$ when $U = \{\text{odd numbers}\}$ and when $U = \{1, 2, 4, 8, \ldots\}$?

For $U = \{\text{odd numbers}\}$, recall Example 3.1.2. $U = \mathbb{Z}\backslash\langle 2\rangle$, so ideals $I \subseteq \mathbb{Z}$ satisfy $\star$ corresponds to ideals of $\mathbb{Z}_{\langle 2\rangle}$, which are generated by powers of 2 (and also the 0 ideal).

Corollary 3.1.13. $J \mapsto \varphi^{-1}(J)$ maps $\mathrm{Spec}(R[U^{-1}])$ to $\{P \in \mathrm{Spec}(R) : P \cap U = \varnothing\}$.

Proof. In Homework 2 it will be proved that for any ring homomorphism $\varphi : R \to S$, if $P \subseteq S$ is prime then $\varphi^{-1}(P) \subseteq R$ is prime. Now if a prime $P \subseteq R$ satisfies $P \cap U = \varnothing$ and if $ru \in P$ for some $u \in U$, then $r \in P$ since P is prime and $u \notin P$, so it's indeed the image. Conversely, if $\star$ holds then $P \cap U = \varnothing$ since if $u \in P \cap U,\ u = u \cdot 1 \in P$ but $1 \notin P$, a contradiction. $\square$

Week 4, lecture 3 starts here

4 Module

Definition 4.0.1. Let R be a ring. An *R-module* is an abelian group M with multiplication $R \times M \to M$ (sometimes called R-action) satisfying

1. $r(m+n) = rm + rn$
2. $(r+r')m = rm + r'm$
3. $(rr')m = r(r'm)$
4. $1_R m = m$

$\forall r, r' \in R,\ m, n \in M$.

Example 4.0.2. If $R = K$ is a field then M is a K-vector space. In fact, the definition should remind you of that of vector spaces.

If $R = \mathbb{Z}$ then R-modules are abelian groups with $R \times M \to M$ given by $n \times g := \underbrace{g + \cdots + g}_{n \text{ times}}$. One is forced to define multiplication like this by definition.

If R is an arbitrary ring and I is an ideal in R, then R itself is a R-module with multiplication the same as ring multiplication in R, and $I,\ R/I$ are also R-modules.

Remark. Much of commutative algebra is generalising linear algebra to modules, and every theorem you see about modules, ask what it says for vector spaces/abelian groups.

Definition 4.0.3. A subset $N \subseteq M$ is a *submodule* if

1. $m, n \in N \Rightarrow m + n \in N$ and
2. $m \in N,\ r \in R \Rightarrow rm \in N$.

Example 4.0.4. A submodule of the R-module R is precisely an ideal.

Like any other algebraic objects, it's important to understand functions between modules. We want a definition that can be generalised to group homomorphisms since modules are abelian groups, and can be specified to linear maps since vector spaces are modules.

Definition 4.0.5. A function $\varphi : M \to N$ where M, N are R-modules is an *R-module homomorphism* if

1. φ is a group homomorphism and
2. $\varphi(rm) = r\varphi(m)$.

Example 4.0.6. As expected, if R is a field then an R-module homomorphism is a linear map, and if $R = \mathbb{Z}$ then it's a group homomorphism. Also $R \to R/I$ and $I \to R$ for I an ideal given by $r \mapsto r$ are R-module homomorphisms.

Definition 4.0.7. The *kernel* of an R-module homomorphism $\varphi : M \to N$ is

$$\ker \varphi := \{m \in M : \varphi(m) = 0_N\},$$

and the *image* of φ is

$$\text{im } \varphi = \{\varphi(m) : m \in M\}.$$

Exercise 4.0.8. Show that these are both submodules of M and N respectively.

Definition 4.0.9. If N is a submodule of an R-module M, then it is also a subgroup of the abelian group M, so we can construct quotient group M/N. This is an R-module with $r(m+N) = rm + N$ and called a *quotient module*.

Theorem 4.0.10 (Isomorphism theorems)**.**

1. If $\varphi : M \to N$ is an R-module homomorphism then $M/\ker\varphi \cong \text{im } \varphi$. (The morally equivalence of this in linear algebra is the rank–nullity theorem.)
2. If $L \subseteq M \subseteq N$ with L a submodule of M and M a submodule of N, then $N/M \cong (N/L)/(M/L)$.
3. If L, M are submodules of N then $(L+M)/L \cong M/(M \cap L)$ where $L + M := \{l + m : l \in L, m \in M\}$. (This is a generalisation of the proposition about dimensions of subspaces in linear algebra.)

Week 5, lecture 1 starts here

4.1 Free module

Recall that every finite dimensional K-vector space is isomorphic to K^n.

Definition 4.1.1. The R-module R^n is defined to be

$$\{(r_1, \dots, r_n) : r_i \in R\}$$

with R-action

$$r(r_1, \dots, r_n) = (rr_1, \dots, rr_n), \qquad (r_1, \dots, r_n) + (r_1', \dots, r_n') = (r_1 + r_1', \dots, r_n + r_n').$$

Remark. 1. More generally, for any index set A (might be uncountable), $M_1 := \{(r_\alpha : \alpha \in A) : r_\alpha \in R\}$ (functions $A \to R$) and $M_2 := \{(r_\alpha : \alpha \in A) : r_\alpha \in R,$ only finitely many $r_\alpha \neq 0\}$ are R-modules.

2. Note that every element of R^n can be written as an R-linear combination of the standard basis e_i as expected.

Definition 4.1.2. Let M be an R-module and $\mathcal{G} = \{m_\beta : \beta \in B\} \subseteq M$. Then $\mathcal{G}$ *generates* M (as an R-module) if every element $m \in M$ can be written as

$$m = \sum_{i=1}^{s} r_i m_{\beta_i} \text{ for some } \beta_1, \dots, \beta_s \in B, \quad r_1, \dots, r_s \in R.$$

Note that B might be infinite but the sum must be finite.

Example 4.1.3. 1. If R is a field then the verb generate is the same as 'span' as in linear algebra.

2. If $R = \mathbb{Z}$ then $\mathcal{G}$ generates M iff it generates M as an abelian group.

3. If $M = I \subseteq R$ is an ideal, then $\mathcal{G}$ generates M as an R-module iff g generates I as an ideal.

Exercise 4.1.4. 1. Give an example of an R-module M with $g \subseteq M$ that generates M as an R-module but not as an abelian group.

   Consider $M = R = \mathbb{R}$. Then $\mathcal{G} = \{1\}$ generates M as an R-module, but the abelian group it generates is $\mathbb{Z} \subsetneq \mathbb{R}$.

2. Generators for M_1, M_2 in above remark?

Definition 4.1.5. A set $\mathcal{G} \subseteq M$ is a *basis* for M if $\mathcal{G}$ generates M as an R-module and every element of M can be written uniquely as an R-linear combination of finitely many elements of $\mathcal{G}$. Equivalently, if $\sum_{i=1}^{s} r_i g_i = 0_M$ for $g_i \in \mathcal{G},\ r_i \in R$ then $r_i = 0\ \forall i = 0$.

Example 4.1.6. 1. If R is a field then a basis for M as an R-module is a basis for M as a R-vector space.

2. A basis for R^2 is $\{(1, 0), (0, 1)\}$.

3. $\{e_\alpha\}$ is a basis for M_2. It's not a basis for M_1 since the sum could be infinite. $\lightning$ There are modules with no basis (that's kind of the point of this section), e.g. $R = \mathbb{C}[x, y],\ M = \langle x, y \rangle$. Suppose M has a basis $\mathcal{G}$. First of all $|\mathcal{G}| > 1$ since M is not a principal ideal. Now pick $f, g \in \mathcal{G}$. Then $fg \in M$, but $fg = fg = gf$, so not uniquely expressed, a contradiction.

Week 5, lecture 2 starts here

Definition 4.1.7. A R-module is *free* if it has a basis.

Example 4.1.8. R^n and M_2 are free. $\langle x, y \rangle \subseteq \mathbb{C}[x, y]$ is not a free $\mathbb{C}[x, y]$-module, but it's a free $\mathbb{C}$-module since $\mathbb{C}$ is a field so it's a vector space, which always has a basis.

$\mathbb{Q}$ is not a free $\mathbb{Z}$-module. First a basis would have to be infinite, but $bc\left(\frac{a}{b}\right) - ad\left(\frac{c}{d}\right) = 0$, a nontrivial linear dependence relation.

4.2 Cayley–Hamilton theorem

Remark. Matrices make sense over an arbitrary ring and give a R-module homomorphism $\varphi : R^n \to R^m$. Determinants still make sense (as a indicator of whether φ is invertible).

Definition 4.2.1. Let M be an R-module. The set of all R-module homomorphisms $\varphi : M \to M$ forms a noncommutative ring with identity and $(\varphi+\varphi)(m) = \varphi(m)+\varphi(m)$ and $(\varphi\psi)(m) = \varphi(\psi(m))$, denoted $\operatorname{End}(M)$.

Example 4.2.2. If R is a field and $M = R^n$ then $\operatorname{End}(M) = n \times n$ matrices.

Week 5, lecture 3 starts here

Notation. $\{\varphi_s : s \in R\}$ where $\varphi_s(m) := sm$.

Definition 4.2.3. Given an $n \times n$ matrix A, the subring $R[A]$ of $\operatorname{End}(R^n)$ is the smallest subring of $\operatorname{End}(R^n)$ containing A and all $\{\varphi_s : s \in R\}$. Explicitly,

$$R[A] = \left\{ \sum_{i=0} a_i A^i : a_i \in R \right\}$$

and set $A^0 = I$.

Remark. Note that $R[A]$ is commutative, and (suggestive by notation) we have a ring homomorphism

$$\begin{aligned} \psi : R[x] &\to R[A] \\ x &\mapsto A. \end{aligned}$$

This is of course not an isomorphism by Cayley–Hamilton theorem.
Also, R^n is an $R[A]$ module with action given by

$$\left(\sum_{i=0} a_i A^i \right) \underline{v} = \sum_{i=0} a_i \left(A^i \underline{v} \right)$$

where $\underline{v} = (r_1, \ldots, r_n) \in R^n$.

Definition 4.2.4. The *characteristic polynomial* of $A \in \operatorname{End}(R^n)$ is $\det(xI - A) \in R[x]$.

Example 4.2.5. 1. $A = \begin{pmatrix} x & x^2 \\ x^3 & x^4 \end{pmatrix}$ and $R = \mathbb{C}[x]$. Then

$$\begin{aligned} \det \begin{pmatrix} t-x & x^2 \\ x^3 & t-x^4 \end{pmatrix} &= (t-x)(t-x^4) - x^5 \\ &= t^2 - (x+x^4)t + x^5 - x^5 \\ &= t^2 - (x+x^4)t. \end{aligned}$$

2. $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ and $R = \mathbb{Z}/6\mathbb{Z}$. Then

$$\det \begin{pmatrix} x-1 & 2 \\ 3 & x-4 \end{pmatrix} = (x-1)(x-4) - 6 = x^2 - 5x - 2 = x^2 + x + 4.$$

Remark. Recall the adjoint of an $n \times n$ matrix B is the matrix C with

$$C_{ij} = (-1)^{i+j} \det \left(B \backslash i\text{th column and } j\text{th row} \right),$$

which makes sense over any ring. We claim $BC = CB = \det B I_n$ (which implies if $\det B$ is a unit then B is invertible). Indeed,

$$\begin{aligned} (BC)_{ij} &= \sum_{k=1}^{n} B_{ik} C_{kj} \\ &= \sum_{k=1}^{n} (-1)^{k+j} B_{ik} \det \left(B \backslash k\text{th column and } j\text{th row} \right) \\ &= \det \left(B \text{ with } j\text{th row replaced by } i\text{th row} \right) \\ &= \begin{cases} 0 \text{ if } i \neq j \\ \det B \text{ if } i = j \end{cases} \\ &= \left(\det B I_n \right)_{ij}. \end{aligned}$$

Theorem 4.2.6 (Cayley–Hamilton)**.** Let R be a ring and let A be an $n \times n$ matrix with entries in R. Set $p_A(x) = \det(xI - A) \in R[x]$, then $p_A(A) = 0$, i.e. $p_A \in \ker \psi$ where ψ is as in remark after Definition 4.2.3.

Definition 4.2.7. An R-module M is *finitely generated* if it has a finite generating set.

Theorem 4.2.8. Let M be a finitely generated R-module with n generators and $\varphi : M \to M$ an R-module homomorphism. Suppose I is an ideal of R with $\varphi(M) \subseteq IM := \langle rm : r \in I, m \in M \rangle$. Then φ satisfies a relation of the form

$$\varphi^n + a_1\varphi^{n-1} + \cdots + a_{n-1}\varphi + a_n = 0 \in \operatorname{End}(M) \text{ where } a_i \in I^i.$$

Week 6, lecture 1 starts here

Proof of Cayley–Hamilton theorem. Write $e_1, \ldots, e_n$ for the standard basis for R^n and one has $Ae_k = \sum_{j=1}^n a_{jk}e_j$ (the kth column of A). Write δ_{jk} for the Kronecker delta. Then

$$\sum_{j=1}^{n} (A\delta_{jk} - a_{jk}I)\, e_j = \sum_{j=1}^{n} A\delta_{jk}e_j - \sum_{j=1}^{n} a_{jk}Ie_j = Ae_k - Ae_k = 0.$$

Let $B = (B_{jk})$ be the $n \times n$ matrix with entries in $R[A]$ with $B_{jk} = A\delta_{jk} - a_{jk}I$ and C the adjoint of B. Then

$$\begin{aligned} 0 &= \sum_{k=1}^{n} C_{kj} \left(\sum_{i=1}^{n} A\delta_{ik} - a_{ik}I \right) e_i = \sum_{i=1}^{n} \left(\sum_{k=1}^{n} C_{kj}(A\delta_{ik} - a_{ik}I)e_i \right) \\ &= \sum_{i=1}^{n}\sum_{k=1}^{n} B_{ik}C_{kj}e_i = \sum_{i=1}^{n} (BC)_{ij}e_i = (\det B)e_j = \begin{pmatrix} 0 \\ \vdots \\ \det B \\ \vdots \\ 0 \end{pmatrix} \leftarrow \text{the } j\text{th position,} \end{aligned}$$

so $\det B = 0$.

Now $p_A(x) \in R[x]$. Then

$$\psi(p_A(x)) = p_A(A) = \det \left(\begin{pmatrix} A & & & 0 \\ & A & & \\ & & \ddots & \\ 0 & & & A \end{pmatrix} - A \right) = \det B = 0.$$

$\square$

Exercise 4.2.9. Let

$$D = \begin{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \\ \begin{pmatrix} 3 & 0 \\ 0 & 4 \end{pmatrix} & \begin{pmatrix} 5 & 6 \\ 7 & 8 \end{pmatrix} \end{pmatrix}.$$

Then

$$\begin{aligned} \det D &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 5 & 6 \\ 7 & 8 \end{pmatrix} - \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}\begin{pmatrix} 3 & 0 \\ 0 & 4 \end{pmatrix} \\ &= \begin{pmatrix} 5 & 6 \\ 7 & 8 \end{pmatrix} - \begin{pmatrix} 3 & 8 \\ 9 & 16 \end{pmatrix} \\ &= \begin{pmatrix} 2 & -2 \\ -2 & -28 \end{pmatrix}. \end{aligned}$$

Proof of Theorem 4.2.8. Let $\{m_1, \ldots, m_n\}$ be a generating set for M. Since $\varphi(M) \in IM$, one can write

$$\varphi(m_i) = \sum_{i=1}^{n} a_{ji}m_j \text{ with } a_{ji} \in I.$$

So $\sum_{j=1}^n(\delta_{ji}\varphi - a_{ji})m_j = 0$ where $\delta_{ji}\varphi - a_{ji}$ can be analogously be viewed as an element of $R[\varphi]$, which is a commutative ring. Write B for the $n\times n$ matrices with entries in $R[\varphi]$ and $B_{ij} = \delta_{ji}\varphi - a_{ij}$. Let C be the adjoint of B. Then

$$0 = \sum_{i=1}^n C_{ki}\left(\sum_{j=1}^n B_{ij}m_j\right) = \sum_{j=1}^n\left(\sum_{i=1}^n C_{ki}B_{ij}\right)m_j = \sum_{j=1}^n (CB)_{kj}m_j = (\det B)m_k,$$

so $(\det B)m = 0\ \forall m\in M$, hence $\det B = 0 \in \mathrm{End}(M)$. Expanding $\det B$ as a polynomial in φ gives us the desired. □

Week 6, lecture 2 starts here

4.2.1 Corollaries of C–H theorem: Nakayama's lemma(s)

Corollary 4.2.10. If M is a finitely generated R-module and I an ideal of R with $IM = M$, then $\exists r\in R$: $r-1\in I,\ rM = 0$.

Proof. Let $\varphi = \mathrm{id}$. Then $\varphi(M)\subset M\subset IM$. So by Theorem 4.2.8, one has

$$\varphi^n + \sum_{i=1}^{n-1} a_i\varphi^{n-1} + a_n = \left(1+\sum_{i=1}^n a_i\right)\varphi = 0 \text{ where } a_i\in I^i.$$

Set $r := 1+\sum_{i=1}^n a_i$. Then $r-1\in I$ and $rm = 0\ \forall m\in M$. □

Corollary 4.2.11. Let R be a local ring with maximal ideal $\mathfrak{m}$ and M a finitely generated R-module. If $\mathfrak{m}M = M$, then $M = 0$.

Proof. By corollary above, $\exists r\in R : r-1\in\mathfrak{m}$ and $rm = 0\ \forall m\in M$. But then $r\notin\mathfrak{m}$ since otherwise $r-(r-1) = 1\in\mathfrak{m}$ hence not maximal. So r is a unit. But then

$$m = 1m = \left(r^{-1}r\right)m = r^{-1}(rm) = r^{-1}0 = 0 \quad \forall m\in M$$

and thus $M = 0$. □

Corollary 4.2.12. Let R be a local ring with maximal ideal $\mathfrak{m}$. If M is a finitely generated R-module and $m_1,\dots,m_n\in M$ are elements whose images span the (*residue field*) $k = R/\mathfrak{m}$-vector space $\overline{M} = M/\mathfrak{m}M$, then m_i generate M.

Remark (Sanity check before the proof)**.** Verify that this is well-defined, i.e. $r+\mathfrak{m} = r'+\mathfrak{m},\ m+\mathfrak{m}M = m'+\mathfrak{m}M \Rightarrow rm+\mathfrak{m}M = r'm'+\mathfrak{m}M$. Indeed, if $r-r'\in\mathfrak{m}$ and $m-m'\in\mathfrak{m}M$, then $rm-r'm' = (r-r')m+(m-m')r'\in\mathfrak{m}M$.

Proof. Let N be the submodule of M generated by m_i. Since $m_i+\mathfrak{m}M$ span $M/\mathfrak{m}M$, each element of M can be written as

$$m = \sum_{i=1}^n r_i m_u + rm' \text{ where } r_i\in R,\ r\in\mathfrak{m},\ m'\in M.$$

Thus $m = n+rm'$ for $n\in N$, i.e. $M/N = \mathfrak{m}M/N$. So by corollary above $M/N = 0$, so $M = N$ and one has the desired. □

Remark ($\lightning$)**.** These all needed M to be finitely generated. If (recall Example 3.1.2) $R = \mathbb{Z}_{\langle 2\rangle}$ and $M = \mathbb{Q}$, then $\langle 2\rangle\,\mathbb{Q} = \mathbb{Q}$, but clearly $\mathbb{Q}\neq 0$. This is not a counterexample since $\mathbb{Q}$ is not finitely generated.

Also, the last two needed R to be local. Consider $\mathbb{Z}$ as a $\mathbb{Z}$-module. $2\mathbb{Z}$ is maximal and the image of 5 (which is 1) generates $\mathbb{Z}/2\mathbb{Z}$, but 5 clearly does not generate $\mathbb{Z}$.

Week 6, lecture 3 starts here

4.3 Localisation of modules

Definition 4.3.1. Let M be an R-module and $U \subseteq R$ a multiplicatively closed set. Then

$$M\left[U^{-1}\right] := \left\{\frac{m}{u} : m \in M, u \in U\right\}$$

modulo the equivalence relation

$$\frac{m}{u} \sim \frac{m'}{u'} \text{ if } \exists \widetilde{u} \in U : \widetilde{u}(u'm - um') = 0.$$

This is an $R\left[U^{-1}\right]$-module.

Readers should verify that the $R\left[U^{-1}\right]$-action $\frac{r}{u} \cdot \frac{m}{u'} = \frac{rm}{uu'}$ is well-defined and $M\left[U^{-1}\right]$ obeys the module axioms.

Lemma 4.3.2. Let R be a ring and M an R-module.

1. If $m \in M,\ m = 0 \Leftrightarrow \frac{m}{1} = \frac{0}{1}$ in every localisation $M_{\mathfrak{m}} = M[U^{-1}]$ at a maximal ideal $\mathfrak{m}$ where $U = R \backslash \mathfrak{m}$.
2. $M = 0 \Leftrightarrow M_{\mathfrak{m}} = 0$ for every maximal ideal $\mathfrak{m}$ of R.

Definition 4.3.3. The *annihilator* of an element $m \in M$ is $\operatorname{ann}(m) := \{r \in R : rm = 0_M\}$.

Example 4.3.4. $R = \mathbb{Z},\ M = \mathbb{Z}/6\mathbb{Z}$. Then $\operatorname{ann}(1) = \langle 6 \rangle,\ \operatorname{ann}(2) = \langle 3 \rangle$. In general, $\operatorname{ann}(m)$ would be an ideal.

Proof.
1. $\frac{m}{1} = \frac{0}{1} \Leftrightarrow \exists u \notin \mathfrak{m} : um = 0 \Rightarrow \operatorname{ann}(m) \not\subseteq \mathfrak{m}$. If $m \neq 0$ then $\operatorname{ann}(m) \neq R$ since $1m = m \neq 0$. So by definition $\exists$ a maximal ideal $\mathfrak{m}$ with $\operatorname{ann}(m) \subseteq \mathfrak{m}$, so $\frac{m}{1} \neq \frac{0}{1}$ in $M_{\mathfrak{m}}$. The other direction is clear.
2. $M = 0 \Leftrightarrow m = 0\ \forall m \in M \Leftrightarrow \forall m \in M, \frac{m}{1} = \frac{0}{1} \in M_{\mathfrak{m}}\ \forall \mathfrak{m} \Leftrightarrow M_{\mathfrak{m}} = 0\ \forall \mathfrak{m}$.

$\square$

Week 7, lecture 1 starts here

Definition 4.3.5 (/Lemma)**.** Let $\varphi : M \to N$ be an R-module homomorphism and P a prime ideal of R. Define $\varphi_P : M_P \to N_P$ (where again M_P denotes $M[U^{-1}]$ where $U = R \backslash P$) by $\dfrac{m}{u} \mapsto \dfrac{\varphi(m)}{u}$.

Check this is well defined: if $\frac{m}{u} = \frac{m'}{u'}$ then $\exists \widetilde{u} \in U : \widetilde{u}(u'm - um') = 0$, so $0_N = \varphi(0_M) = \varphi(\widetilde{u}(u'm - um')) = \widetilde{u}(u'\varphi(m) - u\varphi(m'))$, i.e. $\frac{\varphi(m)}{u} = \frac{\varphi(m')}{u}$. Readers should also check it's a homomorphism.

Corollary 4.3.6. If $\varphi : M \to N$ is an R-module homomorphism, then φ is injective (or surjective, or bijective) iff for every maximal $\mathfrak{m}$ of R, $\varphi_{\mathfrak{m}} : M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is injective (or surjective, or bijective).

Proof. One has

$$\begin{aligned}\ker \varphi_{\mathfrak{m}} &= \left\{\frac{m}{u} : \frac{\varphi(m)}{u} = \frac{0}{1}\right\} = \left\{\frac{m}{u} : \exists \widetilde{u} \notin \mathfrak{m} : \widetilde{u}(\varphi(m)) = 0\right\} \\ &= \left\{\frac{m}{u} : \exists \widetilde{u} \notin \mathfrak{m} : \varphi(\widetilde{u}m) = 0\right\} \subseteq (\ker \varphi)_{\mathfrak{m}}\end{aligned}$$

since $\dfrac{m}{u} = \dfrac{\widetilde{u}m}{\widetilde{u}u}$. Now if $\dfrac{m}{u} \in (\ker \varphi)_{\mathfrak{m}}$ then $\varphi_m\left(\dfrac{m}{u}\right) = \dfrac{\varphi(m)}{u} = 0$, so $\dfrac{m}{u} \in \ker \varphi_m$. Hence

$$\begin{aligned}\varphi \text{ injective} &\Leftrightarrow \ker \varphi = 0 \Leftrightarrow (\ker \varphi)_{\mathfrak{m}} = 0\ \forall \mathfrak{m} \Leftrightarrow \ker \varphi_{\mathfrak{m}} = 0\ \forall \mathfrak{m} \\ &\Leftrightarrow \varphi_{\mathfrak{m}} \text{ injective } \forall \mathfrak{m}.\end{aligned}$$

Now consider cokernel $N/\operatorname{im} \varphi$, which is 0 iff φ is surjective. We claim $(N/\operatorname{im} \varphi)_{\mathfrak{m}} \cong N_{\mathfrak{m}}/\operatorname{im} \varphi_{\mathfrak{m}}$ by the map $\dfrac{n + \operatorname{im} \varphi}{u} \mapsto \dfrac{n}{u} + \operatorname{im} \varphi$. Rest of proof is left as an exercise. $\square$

5 Integral closure

Definition 5.0.1. Let R be a ring. A ring S is an *R-algebra* if $\exists$ a homomorphism $\varphi : R \to S$. This implies S is a R-module with R-action given by $r \cdot s := \varphi(r)s$.

Example 5.0.2. $\mathbb{C}[x_1, x_2]$ is a $\mathbb{C}$-algebra, $\mathbb{Q}\left(\sqrt{3}\right)$ is a $\mathbb{Q}$-algebra, $\mathbb{Z}/6\mathbb{Z}$ is a $\mathbb{Z}$ algebra.

Definition 5.0.3. S is *finite* over R if S is a finitely generated R-module.

Definition 5.0.4. $s \in S$ is *integral* over R if there is a monic polynomial $f(y) = y^n + a_1 y^{n-1} + \cdots + a_n \in R[y]$ with $f(s) = 0$. If every element of S is integral over R, we say S is *integral* over R.

Example 5.0.5 (Why 'integral'?)**.** $\mathbb{Q}$ is a $\mathbb{Z}$-algebra, and $q \in \mathbb{Q}$ is integral iff $q \in \mathbb{Z}$.
$\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ is a $\mathbb{Z}$-algebra, and $\varphi = \frac{1+\sqrt{5}}{2}$ is integral since $\varphi^2 - \varphi - 1 = 0$.
$\mathbb{Z}\left[\frac{1}{3}\right] = \mathbb{Z}_{\langle 3\rangle}$ is a $\mathbb{Z}$-algebra. Let's prove $\frac{1}{3}$ is not integral. Suppose

$$f\left(\frac{1}{3}\right) = \left(\frac{1}{3}\right)^n + \sum_{i=0}^{n-1} a_{n-i}\left(\frac{1}{3}\right)^i = 0.$$

Then

$$1 + \sum_{i=0}^{n-1} a_{n-i} 3^{n-i} = 0,$$

which is impossible since LHS $= 1 \bmod 3$ and RHS $= 0 \bmod 3$.

Notation. For a R-algebra S with $R \subseteq S$ and $s_1, \ldots, s_m$ elements of S, write $R[s_1, \ldots, s_m]$ for the smallest subring of S containing R and $s_1, \ldots, s_m$.

Week 7, lecture 2 starts here

Lemma 5.0.6. We can explicitly write

$$R[s_1, \ldots, s_m] = \left\{ \sum_{u \in \mathbb{N}^n}^{k} a_u s^u : a_u \in R \text{ and only finitely many } a_u \neq 0 \right\}.$$

Definition 5.0.7. $S' \subseteq S$ is an *R-subalgebra* if S' is a subring and $\varphi : R \to S$ has image in S'.

Proposition 5.0.8. Let S be an R-algebra with $R \subseteq S$ and fix $s \in S$. The following are equivalent:

1. s is integral over R.
2. Subring $R[s] \subseteq S$ is finite over R.
3. There is an R-subalgebra $R' \subseteq S : R[s] \subseteq R'$ and R' is finite over R.

Proof.

$1 \Rightarrow 2$: If s satisfies a relation $s^n + a_1 s^{n-1} + \cdots + a_n = 0$ with $a_i \in R$, then $R[s]$ is generated by $1, s, \ldots, s^{n-1}$ as an R-module. Indeed, if $f \in R[s]$ is a polynomial in s of degree $\geq n$, then we can use the relation to lower the degree.

$2 \Rightarrow 3$: Take $R' = R[s]$.

$3 \Rightarrow 1$: Consider the R-module homomorphism $\varphi : R' \to R'$ given by $r \mapsto sr$. Since R' is a finitely generated R-module, φ satisfies a relation $\varphi^n + a_1\varphi^{n-1} + \cdots + a_n = 0$ where $a_i \in R$ by Theorem 4.2.8 and taking $I = R$. Applying this to 1_R gives $s^n + a_1 s^{n-1} + \cdots + a_n = 0$, so s is integral.

□

Theorem 5.0.9. Let S be a R-algebra with $R \subseteq S$.

1. If $R \subseteq S \subseteq S'$, S' is finite over S and S is finite over R, then S' is finite over R.
2. If $s_1, \ldots, s_m \in S$ are integral, then $R[s_1, \ldots, s_m]$ is finite over R and in particular integral over R.

3. If $R \subseteq S \subseteq S'$, S' is integral over S and S is integral over R, then S' is integral over R.
4. The subset
$$\widetilde{R} := \{s \in S : s \text{ integral over } R\} \subseteq S,$$
is a subring of S with $\widetilde{\widetilde{R}} = \widetilde{R}$, i.e. if $s \in S$ is integral over $\widetilde{R}$, it is integral over R.

Week 7, lecture 3 starts here

Proof. 1. If $s_1, \ldots, s_m$ generate S as an R-module and $s'_1, \ldots, s'_n$ generate S' as an S-module, then $\{s_i s'_j : 1 \leq i \leq m,\ 1 \leq j \leq n\}$ generates S' as an R-module. Indeed, if $s \in S'$ then $s = \sum_{i=1}^n a_i s'_i$ where $a_i \in S$, and $a_i = \sum_{j=1}^m r_{ij} s_j$ where $r_{ij} \in R$, so
$$s = \sum_{i=1}^n \left(\sum_{j=1}^m r_{ij} s_j \right) s'_i = \sum_{i=1}^n \sum_{j=1}^m r_{ij}(s'_i s_j).$$

2. We prove by induction on m and Proposition 5.0.8 provides the base case. Suppose the claim is true for $m' < m$. One has $R[s_1, \ldots, s_m] = R[s_1, \ldots, s_{m-1}][s_m]$, $R[s_1, \ldots, s_{m-1}]$ is finite over R and s_m is integral over $R[s_1, \ldots, s_{m-1}]$, so again by Proposition 5.0.8, $R[s_1, \ldots, s_m]$ is finite over $R[s_1, \ldots, s_{m-1}]$. Hence by part 1, $R[s_1, \ldots, s_m]$ is finite over R. To see it is integral, one uses part 3 of Proposition 5.0.8.

3. Let $s' \in S'$. One has s' satisfies a relation $s'^n + b_1 s'^{n-1} + \cdots + b_n = 0$ where $b_i \in S$, so each b_i is integral over R. By part 2, $R[b_1, \ldots, b_n]$ is finite over R, so by Proposition 5.0.8, $R[b_1, \ldots, b_n, s']$ is finite over $R[b_1, \ldots, b_n]$ and so $R[b_1, \ldots, b_n, s']$ is finite over R. Therefore again by part 3 of Proposition 5.0.8, s' is integral over R.

4. To see $\widetilde{R}$ is a ring, consider $s_1, s_2 \in \widetilde{R}$. Then by part 2, $R[s_1, s_2]$ is integral over R, so $-s_1, s_1 + s_2, s_1 s_2 \in R[s_1, s_2]$ are integral over R, i.e. in $\widetilde{R}$. The fact that $\widetilde{\widetilde{R}} = \widetilde{R}$ follows from part 3 with $S = \widetilde{R}$, $S' = \widetilde{R}[s]$.

□

Definition 5.0.10. $\widetilde{R}$ is called *integral closure* of R in S.
If $\widetilde{R} = R$ then R is *integrally closed* in S.
If R is a domain and is integrally closed in its field of fractions $R_{\langle 0 \rangle}$, then R is *integrally closed* (or *normal*).

Example 5.0.11. For $R = \mathbb{Z}$ and $S = \mathbb{Q}\left(\sqrt{d}\right)$ where d is a squarefree integer, $\widetilde{R} = \mathbb{Z}[d]$ if $d \equiv 2, 3 \bmod 4$ and $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ if $d \equiv 1 \bmod 4$. When one sees this, one should recall definition of *ring of integers* in algebraic number theory.
The integral closure of $\mathbb{C}[t^2, t^3] \subseteq \mathbb{C}[t]$ is all of $\mathbb{C}[t]$ since t is integral ($x^2 - t^2 = 0$).

6 Variety

Definition 6.0.1. Let $I \subseteq K[x_1, \ldots, x_n]$ be an ideal where K is a field. The *variety* of I is $V(I) := \{(a_1, \ldots, a_n) \in K^n : f(a_1, \ldots, a_n) = 0\ \forall f \in I\}$.

Example 6.0.2. $V(\langle x^2 + y^2 - 1 \rangle) \subseteq \mathbb{R}^2$ is a circle, $V(\langle y^2 - x^3 + x - 1 \rangle) \subseteq \mathbb{C}^2$ is an elliptic curve, $V(\langle xy, xz \rangle) \subseteq \mathbb{C}^2$ is y-z-plane and x-axis.
By Fermat's last theorem, $V(\langle x^4 + y^4 - 1 \rangle) \subseteq \mathbb{Q}^2$ is $\{(0, \pm 1), (\pm 1, 0)\}$.
$V(\langle xz - y^2, xw - yz, yw - z^2 \rangle)$ is ...

Week 8, lecture 1 starts here

Note that $(a, b, c, d) \in X \Rightarrow (\lambda a, \lambda b, \lambda c, \lambda d) \in X\ \forall \lambda \in K$. So we look at 2 cases:

1° $w = 0$, then solutions are $\{(a, 0, 0, 0) : a \in K\}$.

2° $w = 1$, then solutions are $\{(wz^3, wz^2, wz, w) : w, z \in K\}$, which is equivalent to $\{(a^3, a^2 b, ab^2, b^3) : a, b \in K\}$.

Remark. Note that by the way we define $V(I)$, $I = \langle f_1, \dots, f_r \rangle$ is finitely generated by Hilbert. In particular,

$$V(I) = \{(a_1, \dots, a_n) \in K^n : f_1(a_1, \dots, a_n) = \dots = f_r(a_1, \dots, a_n)\}.$$

Definition 6.0.3. A field K is *algebraically closed* if $\forall f \in K[x],\ \exists a \in K : f(a) = 0$.

Within context of this module, we assume K to be algebraically closed when talking about varieties.

Definition 6.0.4. Let $X \subseteq K^n$ be a set. The *ideal* of X is

$$I(X) = \{f \in K[x_1, \dots, x_n] : f(a_1, \dots, a_n) = 0\ \forall (a_1, \dots, a_n) \in X\}.$$

Remark. One has $X \subseteq V(I(X))$ and $I \subseteq I(V(I))$. Both can be proper, e.g.

1. $X = \mathbb{Z} \subseteq \mathbb{C}$. Then $V(I(X)) = V(\langle 0 \rangle) = \mathbb{C}$.
2. $I = \langle x^2 \rangle \subseteq \mathbb{C}[x]$. Then $I(V(I)) = I(\{0\}) = \langle x \rangle$.

Theorem 6.0.5 (Nullstellensatz)**.** Let K be algebraically closed and $I \subseteq K[x_1, \dots, x_n]$.

1. $V(I) = \varnothing \Leftrightarrow I = \langle 1 \rangle = K[x_1, \dots, x_n]$. weak form
2. $I(V(I)) = \sqrt{I} := \{f : f^m \in I \text{ for some } m \geq 1\}$. strong form

Remark.
1. 2 implies 1, but we will prove it first anyway since it's in fact harder.
2. K must be algebraically closed, e.g. $V(\langle x^2 + 1 \rangle) \subseteq \mathbb{R}$ is empty.
3. $\sqrt{I}$, called the *radical* of I, is an ideal. Indeed, if $f, g \in \sqrt{I}$, then $f^m, g^r \in I$ so

$$(f+g)^{m+r} = \sum_{k=0}^{m+r} \binom{m+r}{k} f^k g^{m+r-k} \in I,$$

so $f + g \in \sqrt{I}$. It's also clear that $\sqrt{I}$ is multiplicatively closed.

Week 8, lecture 2 starts here

Lemma 6.0.6. $I(X)$ is an ideal.

Proof. If $f(a), g(a) = 0\ \forall a \in X$, then $(f+g)(a) = f(a) + g(a) = 0 + 0 = 0\ \forall a \in X$, and $(hf)(a) = h(a)f(a) = h(a)0 = 0$. □

Proposition 6.0.7. If $R \subseteq S$ are domains with S integral over R, then R is a field iff S is a field.

Proof. $\Rightarrow$: Fix $s \in S$ with $s \neq 0$. Then one can write

$$s^n + a_1 s^{n-1} + \dots + a_{n-1} s + a_n = 0 \quad \text{where } a_i \in R$$

Since S is domain, $a_n \neq 0$, and since R is a field,

$$1 = -a_n^{-1} s \left(s^{n-1} + a_1 s^{n-2} + \dots + a_{n-2} s + a_{n-1}\right),$$

i.e. s has an inverse, so S is a field.

$\Leftarrow$: Fix $r \in R$ with $r \neq 0$. Then since S is a field, $r^{-1} \in S$, so one can write

$$\left(r^{-1}\right)^n + a_1 \left(r^{-1}\right)^{n-1} + \dots + a_{n-1} r^{-1} + a_n = 0 \quad \text{where } a_i \in R.$$

Multiplying by r^{n-1} gives

$$r^{-1} + a_1 + \dots + a_{n-1} r^{n-2} + a_n r^{n-1} = 0,$$

so $r^{-1} \in R$.

□

Definition 6.0.8. An R-algebra S is *finitely generated* if $\exists s_1, \dots, s_n \in S : S$ the smallest R-subalgebra containing $s_1, \dots, s_n$.

Remark. Finitely generated as an R-algebra is <u>weaker</u> than finite over R (i.e. finitely generated as an R-module), e.g. $K[x_1, \dots, x_n]$ as a K-algebra/module.

Theorem 6.0.9. Let K be a field and L a finitely generated K-algebra which is also a field. Then L is finite over K (in particular integral over K).

Proof. Write

$$L = K[x_1, \dots, x_n]/I \cong K[\overline{x_1}, \dots, \overline{x_n}] \quad \text{where } \overline{x_i} = x_i + I \text{ is the image of } x_i \text{ in } L.$$

We will prove (by induction) that each $\overline{x_i}$ is integral over K, so that by Theorem 5.0.9.2 we would have the desired.

When $n = 1$, $L = K[\overline{x_1}]$. Since $\overline{x_1}^{-1} \in L$, it's a polynomial p in $\overline{x_1}$, so $*(\overline{x_1}) = \overline{x_1}p(\overline{x_1}) - 1 = 0$. Since K is a field, we can make $*$ monic and $\overline{x_1}$ is hence integral over K, so L is finite over K.

Now suppose the statement is true for $n-1$. Since L is a field, it contains the field $K(\overline{x_1})$, so we can really think of L as $K(\overline{x_1})[\overline{x_2}, \dots, \overline{x_{n-1}}]$. By induction hypothesis, L is finite over $K(\overline{x_1})$, so each $\overline{x_j}$ where $2 \leq j \leq n$ is integral over $K(\overline{x_1})$, i.e. one has a monic polynomial $p_j \in K(\overline{x_1})[x] : p_j(\overline{x_j}) = 0$. Let $f \in K[\overline{x_1}]$ be a common denominator of coefficients of all p_j. Then one can see p_j as monic with coefficients in $K[\overline{x_1}][f^{-1}]$, and L is integral over $K[\overline{x_1}][f^{-1}]$. By Proposition 6.0.7, $K[\overline{x_1}][f^{-1}] \subseteq K(\overline{x_1})$ is a field. By minimality of $K(\overline{x_1})$, $K[\overline{x_1}][f^{-1}] \cong K(\overline{x_1})$.

Week 8, lecture 3 starts here

Consider the ring homomorphism $\varphi : K[t] \to K[\overline{x_1}] : t \mapsto \overline{x_1}$. This is surjective by construction. If φ is injective (hence an isomorphism), then $K(t) \cong K(\overline{x_1})$. Let $p(t) = \varphi^{-1}(f)$ and choose $g \in K[t]$ with $p \nmid g$. Then

$$\frac{1}{q} \notin K[t][p^{-1}] \cong K[\overline{x_1}][f^{-1}] \cong K(\overline{x_1}) \cong K(t),$$

a contradiction, so φ is not injective, i.e. $\exists p \in K[t] : p(\overline{x_1}) = 0$. Again, since K is a field, one can make p monic and see that $\overline{x_1}$ is integral over K, so $K[\overline{x_1}]$ is finite over K. Now by 6.0.7, $K[\overline{x_1}]$ is a field and so $K[\overline{x_1}] \cong K(\overline{x_1})$, hence $K(\overline{x_1})$ is finite over K. We conclude that L is finite over K. $\square$

Corollary 6.0.10. The maximal ideals of $K[x_1, \dots, x_n]$ where K is an algebraically closed field are of the form $\langle x_1 - a_1, \dots, x_n - a_n \rangle$ where $a_i \in K$.

Remark.
1. Again we do need the assumption of K being algebraically closed. Consider $\langle x^2 + 1 \rangle \subseteq \mathbb{R}[x]$, which is maximal since any ideal strictly containing it would be generated by something that strictly divides $x^2 + 1$, which is however irreducible over $\mathbb{R}$.
2. If K is algebraically closed then there are no fields $L \supsetneq K$ with L finite over K, since if there is such L then $l \in L \backslash K$ would satisfy a monic polynomial with coefficients in K and minimal degree, but then by definition $l \in K$.

Proof. Let $\mathfrak{m}$ be a maximal ideal. Then $L = K[x_1, \dots, x_n]/\mathfrak{m}$, a finitely generated K-algebra, is a field, so by theorem above L is finite over K. Since K is algebraically closed, by remark above $L \cong K$, i.e. $\exists \varphi : K[x_1, \dots, x_n]/\mathfrak{m} \to K$ with $\varphi(a) = a \ \forall a \in K$. Set $a_i = \varphi(x_i)$, then $\varphi(x_i - a_i) = \varphi(x_i) - a_i = 0$, i.e. $x_i - a_i \in \ker \varphi = \mathfrak{m}$, so $\mathfrak{m} \supseteq \langle x_1 - a_1, \dots, x_n - a_n \rangle$. We claim

$$f \in \mathfrak{m} \backslash \langle x_1 - a_1, \dots, x_n - a_n \rangle \Rightarrow f(a_1, \dots, a_n) \in \mathfrak{m},$$

proof of which is left as an exercise. This completes the proof. $\square$

We are now ready to prove the **Nullstellensatz**.

Proof of 6.0.5.
1. Suppose $I \subsetneq K[x_1, \dots, x_n]$. Then $I \subseteq \mathfrak{m}$ for some maximal ideal $\mathfrak{m} = \langle x_1 - a_1, \dots, x_n - a_n \rangle$. One has $I \subseteq J \Rightarrow V(J) \subseteq V(I)$, so since $(a_1, \dots, a_n) \in V(\mathfrak{m})$, $V(I) \neq \varnothing$.
2. (by Rabinowitch trick) Note that if $f^m \in I$ then $f^m(a) = 0 \ \forall a \in V(I)$, so $(f(a))^m = 0$ and so $f(a) = 0 \ \forall a \in V(I)$, so $f \in I(V(I))$. We have just proved that $\sqrt{I} \subseteq I(V(I))$.

   Now fix $f \in I(V(I))$ and set $J = \langle f_1, \dots, f_r, yf - 1 \rangle \subseteq K[x_1, \dots, x_n, y]$ where f_i are generators of I (one can write down this since $K[x_1, \dots, x_n]$ is Noetherian). One has $V(J) = \varnothing$ since f and $fy - 1$ cannot be zero at the same time. By weak Nullstellensatz, $1 \in J$, i.e.

$$1 = \sum_{i=1}^{r} h_i(x, y) f_i(x) + h(x, y)(yf - 1) \in K[x_1, \dots, x_n, y] \subseteq K(x_1, \dots, x_n, y).$$

Now if one just lets $y = \frac{1}{f}$ then

$$1 = \sum_{i=1}^{r} h_i\left(x, \frac{1}{f}\right) f_i(x)$$

and for some m one can clear the denominators and have

$$f^m = \sum_{i=1}^{r} \underbrace{h_i\left(x, \frac{1}{f}\right) f^m}_{\text{polynomial in } x} f_i(x) \in I,$$

i.e. $I(V(I)) \subseteq \sqrt{I}$.

$\square$

Week 9, lecture 1 starts here

Example 6.0.11. $\sqrt{I}$ where $I = \langle n \rangle \subseteq \mathbb{Z}$ is $\langle m \rangle$ where m is the 'squarefree part of n', i.e. if $n = 72 = 2^3 \times 3^2$ then $m = 2 \times 3 = 6$, and if $n = 8 = 2^3$ then $m = 2$.

7 Primary decomposition

Remark. Recall

1. Any positive integer has a unique prime factorisation $n = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}$ where p_i are prime and $m_i \in \mathbb{N}$.
2. If R is a UFD then every $f \in R$ can be written uniquely as a product of powers of irreducible elements

$$f = \prod_{i=1}^{s} f_i^{m_i} \qquad \text{(meaning)} \;\; \langle f \rangle = \bigcap_{i=1}^{s} \langle f_i^{m_i} \rangle$$

   where f_i are irreducible and $m_i \in \mathbb{N}$, up to unit.

   Note that in this case,

3. $$V(\langle f \rangle) = \bigcup_{i=1}^{s} V(f_i^{m_i}) = \bigcup_{i=1}^{s} V(f_i).$$

   In general, $I = J_1 \cap J_2 \Rightarrow V(I) = V(J_1) \cup V(J_2)$.

   Proof. One has $J_1 \cap J_2 \subseteq J_1$ and so by definition $V(J_1) \subseteq V(J_1 \cap J_2) = V(I)$ and similarly $V(J_2) \subseteq V(J_1 \cap J_2) = V(I)$ and one has $V(J_1) \cup V(J_2) \subseteq V(I)$.

   Conversely, $J_1 \cap J_2 \supseteq J_1 J_2 = \langle fg : f \in J_1, g \in J_2 \rangle$, so $V(I) = V(J_1 \cap J_2) \subseteq V(J_1 J_2)$. If $x \in V(J_1 J_2) \backslash V(J_1)$ then $(fg)(x) = 0 \; \forall g \in J_2$ and $\exists f \in J_1 : f(x) \neq 0$, but then $x \in V(J_2)$, so $V(J_1 J_2) \subseteq V(J_1) \cup V(J_2)$. $\square$

   We want to do things like this in more generality in this chapter.

Definition 7.0.1. Let Q be a proper ideal in a ring R. Q is *primary* if $fg \in Q \Rightarrow f \in Q$ or $g^m \in Q$ for some $m \in \mathbb{N}$.

Example 7.0.2. $\langle 27 \rangle \subseteq \mathbb{Z}$ is primary since if $nm \in \langle 27 \rangle$ then $27 \mid nm$ so either $27 \mid n$ or $3 \mid m$ (so $27 \mid m^3$). In fact, primary ideals in $\mathbb{Z}$ are generated by powers of primes.

Note that if Q is primary then $\sqrt{Q}$ is prime. Indeed, if $fg \in \sqrt{Q}$ then $(fg)^n = f^n g^n \in Q$ for some $n > 0$, so either $f^n \in Q$ (so $f \in \sqrt{Q}$) or $g^{nm} \in Q$ (so $g \in \sqrt{Q}$).

Week 9, lecture 2 starts here

Remark ($\lightning$). There are ideals Q with $\sqrt{Q} = P$ prime, but Q not primary, e.g. $Q = \left\langle x^2, xy \right\rangle \subseteq \mathbb{C}[x, y]$ is not primary since $xy \in Q$ but $x \notin Q$ since x is not divisible by x^2 or xy and $y^m \notin Q$ (note this argument only works for monomial ideals). But $\sqrt{Q} = \langle x \rangle$ is prime, since $\mathbb{C}[x, y] / \langle x \rangle \cong \mathbb{C}[y]$, a domain.

For the rest of this topic, we will assume R is Noetherian.

Definition 7.0.3. Let I be a proper ideal in ring R. A *primary decomposition* of I is an expression

$$I = Q_1 \cap \cdots \cap Q_r \quad \text{where each } Q_i \text{ is primary.}$$

The decomposition is *irredundant* if we can't remove any Q_i, i.e.

$$I \subsetneq \bigcap_{i \neq j} Q_i.$$

The decomposition is *minimal* if there's no decomposition with fewer terms, i.e. r is minimal.

Example 7.0.4. 1. $\langle 12 \rangle = \langle 3 \rangle \cap \langle 4 \rangle$. This is a primary decomposition that's irredundant and minimal (since $\langle 12 \rangle$ is no primary).

2. $I = \left\langle x^2, xy, x^2z^2, yz^2 \right\rangle = \left\langle x^2, y \right\rangle \cap \left\langle x, z^2 \right\rangle$. Note that the radicals

$$\sqrt{\langle x^2, y \rangle} = \langle x, y \rangle, \quad \sqrt{\langle x, z^2 \rangle} = \langle x, z \rangle$$

are prime. We claim they are actually primary, so we've got a primary decomposition. Again this is irredundant and minimal since $xy \in I$ but $x \notin I$ and $y^m \notin I \; \forall m \in \mathbb{N}$.

Exercise 7.0.5. 1. Is $\left\langle x^2 \right\rangle \cap \left\langle y^3 \right\rangle \cap \langle x, y \rangle = \left\langle x^2y^3 \right\rangle$ a primary decomposition? Irredundant? Minimal?

Indeed $\left\langle x^2 \right\rangle$ is primary (since $x^2 \mid fg \Rightarrow x^2 \mid f$ or $x \mid g$ so $x^2 \mid g^2$), $\left\langle y^3 \right\rangle$ is primary (similar) and $\langle x, y \rangle$ is maximal so prime so primary. It's not irredundant since one can remove $\langle x, y \rangle$, so as a result it's not minimal.

2. Verify the two ideals in above example are primary.

Definition 7.0.6. A proper ideal $I \subseteq R$ is *irreducible* if it cannot be written as intersection of 2 strictly large ideals, i.e. $I = J \cap K$, J, K ideals of $R \Rightarrow I = J$ or K.

Example 7.0.7. 1. In $\mathbb{Z}$, $\langle 5 \rangle, \langle 25 \rangle$ are irreducible and $\langle 6 \rangle = \langle 2 \rangle \langle 3 \rangle$ is.

2. $\langle xy \rangle = \langle x \rangle \cap \langle y \rangle \subseteq \mathbb{C}[x, y]$ is not irreducible, but $\left\langle x^2, y^2 \right\rangle$ is.

Lemma 7.0.8. Irreducible ideals in ring R are primary.

Proof. Let $I \subseteq R$ be irreducible with $fg \in I$. Consider chain of ideals

$$J_1 \subseteq J_2 \subseteq J_3 \subseteq \cdots$$

where

$$J_m = (I : g^m) := \{h \in R : hg^m \in I \text{ for } m \geq 1\}.$$

This must stabilise since R is Noetherian, i.e. $\exists N : J_m = J_N \; \forall m \geq N$. We claim that

$$I = \left(I + \left\langle g^N \right\rangle\right) \cap (I + \langle f \rangle).$$

The $\subseteq$ inclusion is clear. Now fix $h \in \left(I + \left\langle g^N \right\rangle\right) \cap (I + \langle f \rangle)$. Then $gh \in I$ since $h \in I + \langle f \rangle$ and $fg \in I$. Also one can write $h = i + rg^N$ for some $i \in I$, $r \in R$, so $gh = gi + rg^{N+1} \in I$, hence $rg^{N+1} \in I$, i.e. $r \in (I : g^{N+1}) = (I : g^N)$. Thus $rg^N \in I$ and so $h \in I$.

Since I is irreducible, $I = I + \left\langle g^N \right\rangle$ or $I + \langle f \rangle$, which precisely implies that I is primary. □

Week 9, lecture 3 starts here

Theorem 7.0.9. All proper ideals of a ring R have a primary decomposition.

Proof by Noetherian induction. By lemma above, it suffices to show every proper ideal is intersection of finitely many irreducibles. Let S by the set of proper ideals that is not such intersection and we want to show $S = \varnothing$. Suppose not, then S has a maximal element I since R is Noetherian. Then I is not irreducible, and so one can write $I = J \cap K$ for strictly larger ideals $J, K \notin S$. Hence one has write irreducible decompositions for both J, K and therefore one for I, a contradiction. □

Example 7.0.10 (Primary ideals are not necessarily irreducible)**.** Consider $I = \left\langle x^2, xy, y^2 \right\rangle \subseteq \mathbb{C}[x, y]$. If $fg \in I$ and f, g are homogeneous, then $\deg fg \geq 2$ so either $\deg f \geq 2$ which means $f \in I$ or $\deg g \geq 1$ so $g^2 \in I$, so I is primary, so it is a irredundant primary decomposition of itself. But also $I = \left\langle x^2, y \right\rangle \cap \left\langle x, y^2 \right\rangle$ is also a irredundant decomposition. Note that radicals of both are $\langle x, y \rangle$, which is not an accident.

Lemma 7.0.11. If Q_1, Q_2 are primary ideals in R with $\sqrt{Q_1} = \sqrt{Q_2} = P$ then $Q_1 \cap Q_2$ is P-primary.

Proof. Let $fg \in Q_1 \cap Q_2$. Then either $f \in Q_1 \cap Q_2$ or WLOG $f \notin Q_1$. Since Q_1 is primary, $g^m \in Q_1$ for some $m > 0$, so $g \in \sqrt{Q_1} = \sqrt{Q_2}$ and so $g^l \in Q_2$ for some $l > 0$, thus $g^{\max(m,l)} \in Q_1 \cap Q_2$, hence $Q_1 \cap Q_2$ is primary. Now $Q_1 \cap Q_2 \subseteq Q_1 \Rightarrow \sqrt{Q_1 \cap Q_2} \subseteq \sqrt{Q_1} = P$. If $f \in P$ then $f^m \in Q_1$ and $f^l \in Q_2$ for some $m, l > 0$, so $f^{\max(m,l)} \in Q_1 \cap Q_2$, thus $P \subseteq \sqrt{Q_1 \cap Q_2}$. One concludes $\sqrt{Q_1 \cap Q_2} = P$. $\square$

This means we can just take intersection of two primary ideals with same radical in our decomposition to get a shorter one. The next goal is to show that after this 'shortening', the $\sqrt{Q_i}$ are determined.

Definition 7.0.12. Let M be an R-module. An ideal P is an *associated prime* of M if P is prime and $P = \operatorname{ann}(m)$ for some $m \in M$. We write $\operatorname{ass}(M)$ for set of associated primes of M.

Example 7.0.13. $\langle 3 \rangle$ is an associated prime of the $\mathbb{Z}$-module $\mathbb{Z}/27\mathbb{Z}$; in fact it's the only one, i.e. $\operatorname{ass}(M) = \{\langle 3 \rangle\}$.

Week 10, lecture 1 starts here

Lemma 7.0.14. If R is Noetherian and $M \neq 0$, then $\operatorname{ass}(M) \neq \varnothing$.

Proof. Let $S = \{\operatorname{ann}(m) : m \in M, m \neq 0\}$. Then S is nonempty since $M \neq 0$. Every element of S is proper, since $1 \notin \operatorname{ann}(m)$ if $m \neq 0$. S therefore has a maximal element $I = \operatorname{ann}(m')$ since R is Noetherian. We claim I is prime. Indeed, if $fg \in I$ then $fgm' = 0$. If $gm' = 0$ then $g \in I$. Otherwise, $gm' \neq 0$ and $f \in \operatorname{ann}(gm') \in S$. It's clear that $\operatorname{ann}(m') \subseteq \operatorname{ann}(gm')$, but since $\operatorname{ann}(m')$ is maximal, it must be $\operatorname{ann}(m') = \operatorname{ann}(gm')$ and $f \in \operatorname{ann}(m')$, so I is prime, hence an associated prime. $\square$

Proposition 7.0.15. If Q is P-primary in a Noetherian ring R, then $\operatorname{ass}(R/Q) = \{P\}$.

Proof. We have $\sqrt{Q} = P$. If $r \in R \backslash Q$ and $s \in R$ with $rs \in Q$, then $s^l \in Q$ for some $l > 0$, so $s \in P$. Thus for any $0 \neq m = r + Q \in R/Q$, one has $\operatorname{ann}(m) \subseteq P$. Since $Q \subseteq \operatorname{ann}(m)$, one has $P = \sqrt{Q} \subseteq \sqrt{\operatorname{ann}(m)} \subseteq \sqrt{P} = P$, so $\sqrt{\operatorname{ann}(m)} = P$. This means if $\operatorname{ann}(m)$ is prime then it's P, i.e. $\operatorname{ass}(R/Q) \subseteq \{P\}$. The other inclusion is clear, so $\operatorname{ass}(R/Q) = \{P\}$. $\square$

Example 7.0.16. $\operatorname{ass}\left(\dfrac{\mathbb{C}[x,y]}{\langle x^2, y \rangle}\right) = \{\langle x, y \rangle\}$ since $\langle x^2, y \rangle$ is $\langle x, y \rangle$-primary.

Lemma 7.0.17. If $\varphi : M \to N$ is injective then $\operatorname{ass}(M) \subseteq \operatorname{ass}(N)$.

Proof. $\operatorname{ann}(m) = \operatorname{ann}(\varphi(m))$, since if $rm = 0_M$ then $0_N = \varphi(rm) = r\varphi(m)$ so $\operatorname{ann}(m) \subseteq \operatorname{ann}(\varphi(m))$ and if $r\varphi(m) = 0_N$ then $\varphi(rm) = 0_N$, so since φ is injective $rm = 0_M$, i.e. $r \in \operatorname{ann}(m)$, so $\operatorname{ann}(m) \supseteq \operatorname{ann}(\varphi(m))$. $\square$

Example 7.0.18. One can indeed has proper inclusion, e.g. $R = \mathbb{Z},\ N = \mathbb{Z}/6\mathbb{Z},\ M = \mathbb{Z}/3\mathbb{Z}$ with $\varphi : M \to N : m \mapsto 2m$. Then $\operatorname{ass}(N) = \{\langle 2 \rangle, \langle 3 \rangle\}$ and $\operatorname{ass}(M) = \{\langle 3 \rangle\}$.

Week 10, lecture 2 starts here

Definition 7.0.19. If $M_1, \ldots, M_s$ are R-modules, then $\bigoplus_{i=1}^s R_i$ is an R-module with elements $(m_1, \ldots, m_s)$ where $m_i \in M_i$, coordinatewise addition and multiplication defined $r(m_1, \ldots, m_s) = (rm_1, \ldots, rm_s)$.

Example 7.0.20. $R^n = \bigoplus_{i=1}^n R$

$R = \mathbb{Z},\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} = \mathbb{Z}/6\mathbb{Z}$.

Lemma 7.0.21. If $M = \bigoplus_{i=1}^s M_i$ then $\operatorname{ass}(M) = \bigcup_{i=1}^s \operatorname{ass}(M_i)$.

Proof. We have injective homomorphisms

$$\begin{aligned} \varphi_i : M_i &\to M \\ m_i &\mapsto (0, \ldots, \underset{i\text{th position}}{m_i}, \ldots, 0) \end{aligned}$$

Thus by 7.0.17, $\operatorname{ass}(M_i) \subseteq \operatorname{ass}(M)\ \forall i$, i.e. $\bigcup_{i=1}^s \operatorname{ass}(M_i) \subseteq \operatorname{ass}(M)$.

For the other inclusion, we prove by induction on s. The base case is a tautology, now suppose the statement is true for $s-1$, and let $P = \operatorname{ann}((m_1, \ldots, m_s)) \in \operatorname{ass}(M)$. Suppose for contradiction $P \notin \operatorname{ass}(M_i)$ for any i. Note that for all $r \in P,\ rm_s = 0_{M_s}$. Since $P \neq \operatorname{ann}(m_s)$by assumption, there is an $r' \in \operatorname{ann}(m_s) \backslash P$. By induction, $P \notin \operatorname{ass}\left(\bigoplus_{i=1}^{s-1} M_i\right)$, so $P \neq \operatorname{ann}((m_1, \ldots, m_{s-1}))$. Thus there is an $r'' \in R \backslash P$ with $r''(m_1, \ldots, m_{s-1}) = 0_{\bigoplus_{i=1}^{s-1} M_i}$. Then $r'r''(m_1, \ldots, m_s) = 0$, i.e. $r'r'' \in P$. But P is prime, a contradiction. $\square$

Example 7.0.22. By lemma above and Proposition 7.0.15,

$$\begin{aligned}\operatorname{ass}(\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}) &= \operatorname{ass}(\mathbb{Z}/2\mathbb{Z}) \cup \operatorname{ass}(\mathbb{Z}/4\mathbb{Z}) \cup \operatorname{ass}(\mathbb{Z}/3\mathbb{Z}) \\ &= \{\langle 2\rangle\} \cup \{\langle 2\rangle\} \cup \{\langle 3\rangle\} \\ &= \{\langle 2\rangle, \langle 3\rangle\}.\end{aligned}$$

Theorem 7.0.23. Let R be Noetherian and $I = Q_1 \cap \cdots \cap Q_s$ a primary decomposition with Q_i P-primary. Then

$$\operatorname{ass}(R/I) \subseteq \{P_1, \ldots, P_s\}$$

and if the decomposition is irredundant then one has equality.

This gives us a way to get a minimal primary decomposition from any decomposition.

Proof. Each R/Q_i is an R-module, so we can form the direct sum $M = \bigoplus_{i=1}^s R/Q_i$. Consider the R-module homomorphism

$$\begin{aligned}\varphi : R/I &\to M \\ r + I &\mapsto (r + Q_1, \ldots, r + Q_s)\end{aligned}$$

This is well defined, since if $r + I = r' + I$ then $r - r' \in I \subseteq Q_i$ for all i, so $r + Q_i = r' + Q_i$ for all i. This is injective, since $\varphi(r + I) = 0$ implies $r \in Q_i$ for all i, i.e. $r \in \bigcap_{i=1}^s Q_i = I$. Thus by lemmas above,

$$\operatorname{ass}(R/I) \subseteq \operatorname{ass}(M) = \bigcup_{i=1}^s \operatorname{ass}(R/Q_i) = \{P_1, \ldots, P_s\}.$$

If the decomposition is irredundant, then for all i, $I \subsetneqq \bigcap_{j\neq i} Q_j$. Consider $0 \neq \bigcap_{j\neq i} Q_j + I \subseteq R/I$ and $\varphi\left(\bigcap_{j\neq i} Q_j + I\right)$. Since φ is injective, this is nonzero, but the jth coordinates are zero where $j \neq i$. So $\varphi|_{\bigcap_{j\neq i} Q_j + I}$ is an injective homomorphism to R/Q_i. Thus

$$\operatorname{ass}\left(\bigcap_{j\neq i} Q_j + I\right) \subseteq \operatorname{ass}(R/Q_i) = \{P_i\}.$$

Since $\operatorname{ass}\left(\bigcap_{j\neq i} Q_j + I\right)$ is nonempty by 7.0.14, it's $\{P_i\}$. Now since

$$\begin{aligned}\bigcap_{j\neq i} Q_j + I &\hookrightarrow R/I \\ r + I &\mapsto r + I\end{aligned}$$

is injective,

$$\operatorname{ass}\left(\bigcap_{j\neq i} Q_j + I\right) \subseteq \operatorname{ass}(R/I),$$

so $P_i \in \operatorname{ass}(R/I)$ for all i, i.e. $\{P_1, \ldots, P_s\} \subseteq \operatorname{ass}(R/I)$. ∎

Week 10, lecture 3 starts here

Definition 7.0.24. An associated prime P of an R-module M is *minimal* if there is no $P' \subsetneq P$ with $P' \in \operatorname{ass}(M)$.

Example 7.0.25. $\langle x\rangle \cap \langle x^2, y\rangle = I = \langle x^2, xy\rangle \subseteq \mathbb{C}[x, y] = R$. Then $\operatorname{ass}(R/I) = \{\langle x\rangle, \langle x, y\rangle\}$ where $\langle x\rangle$ is minimal and $\langle x, y\rangle$ is not.

Definition 7.0.26. If $I = \bigcap Q_j$ is an irredundant primary decomposition with $\sqrt{Q_i} \neq \sqrt{Q_j}$ for $i \neq j$, then Q_i is called the *primary component* of I corresponding to $P_i = \sqrt{Q_i}$.

Proposition 7.0.27. Let P be a minimal associated prime of an ideal I in a Noetherian ring R. Then the P-primary component of I does not depend on the choice of primary decomposition.

Proof. Let $I = \bigcap_{i=1}^s Q_i$ be an irredundant primary decomposition with $\sqrt{Q_i} \neq \sqrt{Q_j}$ for $i \neq j$, and $\sqrt{Q_s} = P$. Since $\bigcap_{i=1}^{s-1} Q_i \neq I$, there is $f \in \bigcap_{i=1}^{s-1} Q_i \backslash Q_s$. We may also assume $f \notin P$ since if $\bigcap_{i=1}^{s-1} Q_i \subseteq P$, then $Q_i \subseteq P$ for some i, so $\sqrt{Q_i} \subseteq P$ for some i, contradicting minimality. Then $(I : f^\infty) = \bigcap_{i=1}^s (Q_i : f^\infty)$. If $f \in Q_i$ then $(Q_i : f^\infty) = R$ since $1f \in Q_i$, so $(I : f^\infty) = (Q_s : f^\infty)$. If $g \in (Q_s : f^\infty)$ then $gf^m \in Q_s$ for some $m \geq 0$. Since Q_s is primary, either $g \in Q_s$ or $(f^m)^l \in Q_s \subseteq P$ for some l, but then $f \in P$, so $g \in Q_s$, thus $(I : f^\infty) = (Q_s : f^\infty) = Q_s$. ∎

Remark. The minimality assumption was essential. Consider $I = \langle x^2 \rangle \cap \langle x^3, y^2 \rangle = \langle x^2 \rangle \cap \langle x^3, x^2y^2, y^3 \rangle = \langle x^3, x^2y^2 \rangle \subseteq \mathbb{C}[x, y]$.