Lecture 11

Domenico Valloni

1 Noether normalization

Recall that from last section we defined a ring extension $R \subset S$ to be finite if S is a finitely generated R-module. We shall see later in the course that the induced map $\mathrm{Spec}(S) \to \mathrm{Spec}(R)$ sends maximal ideals to maximal ideals. Now, if both R and S are finitely-generated K-algebras, for K an algebraically closed field, we get a map of algebraic varieties $\mathrm{mSpec}(S) \to \mathrm{mSpec}(R)$. Fact: this map is surjective and has finite fibres. We shall explain why in the last lectures, but you will also see this if you will follow the course on algebraic geometry next year.

In this lecture, we shall prove the following:

Theorem 1 (Noether's normalization lemma)**.** *Let K be any field, and let*

$$R = K[x_1, \cdots, x_n]/I$$

be a finitely generated K-algebra. There is a polynomial algebra $S = K[t_1, \cdots, t_d]$ and a ring extension $S \subset R$ such that R is finite over S. Moreover, if R is a domain, then $d = \mathrm{tr.deg}_K(\mathrm{Frac}(R))$.

The geometric interpretation of this comes from the discussion made at the beginning. Assume that R is a domain and K is algebraically closed. So $\mathrm{mSpec}(R) = V(I) \subset K^n$ is an irreducible algebraic variety. The finite ring extension $S \subset R$ then induces a map $V(I) \to K^d$, where d is the dimension of $V(I)$. Then this map is surjective and has finite pre-images. One can also add more conditions on the ring extension, e.g., flatness (this will imply that all the pre-images have the same cardinality, when counted in the right way) or unramified (this will result in something that looks like a covering space in topology).

The theorem above is true for any field K. We shall give a proof in the case that K is infinite (e.g., algebraically closed or of characteristic 0). The proof for finite field follows the same ideas, but it is slighlty more complicated, and can be found in Patakfalvi's notes. We begin with a lemma:

Lemma 2. *Let K be an infinite field. Let $f(x_1, \cdots, x_{n-1}, y) \in K[x_1, \cdots, x_{n-1}, y]$ be a polynomial of degree d. Then, there are elements $c_1, \cdots, c_{n-1} \in K$ and $\lambda \in K \setminus 0$ such that*

$$\lambda^{-1} f(x_1 + c_1 y, x_2 + c_2 y, \cdots, x_{n-1} + c_{n-1} y, y) \in K[x_1, x_2, \cdots, x_{n-1}, y]$$

has the form

$$y^d + g_{d-1}(x_1, \cdots, x_{n-1})y^{d-1} + \cdots + g_1(x_1, \cdots, x_{n-1})y + g_0(x_1, \cdots, x_{n-1})$$

where each $g_i \in K[x_1, \cdots, x_{n-1}]$.

Proof. Write

$$f = \sum_{i_1, i_2, \ldots, i_{n-1}, j \geq 0} (a_{i_1, \cdots, i_{n-1}, j}) x_1^{i_1} \cdots x_{n-1}^{i_{n-1}} y^j,$$

with $a_{i_1, \cdots, i_{n-1}, j} \in K$. Note that by definition

$$d = \max\{i_1 + i_2 + \cdots + i_{n-1} + j \colon a_{i_1, \cdots, i_{n-1}, j} \neq 0\}.$$

Let f_d be the homogeneous part of f of degree d:

$$f_d = \sum_{i_1 + \cdots + i_{n-1} + j = d} (a_{i_1, \cdots, i_{n-1}, j}) x_1^{i_1} \cdots x_{n-1}^{i_{n-1}} y^j,$$

which is non-zero because f has degree d. Now, we consider

$$f_d(x_1 + c_1 y, \cdots, x_{n-1} + c_{n-1} y, y);$$

a simple computation shows that the coefficient of y^d of this polynomial is given by $f_d(c_1, c_2, \cdots, c_{n-1}, 1)$. Since K is infinite, there we can find $c_1, c_2, \cdots, c_{n-1} \in K$ such that $\lambda := f_d(c_1, c_2, \cdots, c_{n-1}, 1) \neq 0$. From this it follows that

$$\lambda^{-1} f(x_1 + c_1 y, \cdots, x_{n-1} + c_{n-1} y, y)$$

has the prescribed form. □

Proof of Noether normalization. We prove this by induction on n. Let us look at the case $n = 1$ first. Now, $I \subset K[x]$ can either be the zero ideal, in which case we put $t_1 = x$, or $I = (f)$ for some $f \neq 0$, since $K[x]$ is a PID. We can also assume that f is monic without modifying the ideal I. In this case, let $\bar{x} \in R$ be the image of x. Then $\bar{x}$ generates R and satisfies the monic equation $f(\bar{x})$ over K, i.e., it is integral over K. So we put $S = K$ and the result follows.

Now we do the induction step. Let again $\bar{x}_i \in R$ be the image of x_i in R. They generate R as a K-algebra. We reorder them and assume that $\bar{x}_1, \cdots, \bar{x}_r$ are algebraically independent over K and that $\bar{x}_{r+1}, \cdots, \bar{x}_n$ are algebraic over $K[\bar{x}_1, \cdots, \bar{x}_r] \subset R$. If $r = n$ then $R = K[x_1, \cdots, x_n]$ necessarily, and we can simply put $t_i = x_i$. So we can assume $r < n$. In this case, $\bar{x}_n$ is algebraic over $K[\bar{x}_1, \cdots, \bar{x}_{n-1}] \subset R$, so we can find a polynomial $0 \neq f(y) \in K[\bar{x}_1, \cdots, \bar{x}_{n-1}][y]$ such that $f(\bar{x}_n) = 0$. Since the natural map $K[x_1, \cdots, x_{n-1}] \to K[\bar{x}_1, \cdots, \bar{x}_{n-1}]$ is surjective, we can find a polynomial $F \in K[x_1, \cdots, x_{n-1}][y]$ such that $F(\bar{x}_1, \cdots, \bar{x}_n, y) = f(y)$ (why?). Now we apply the previous lemma, and we find $c_i, \lambda \in K$ such that

$$\lambda^{-1} F(x_1 + c_1 y, \cdots, x_{n-1} + c_{n-1} y, y) \in K[x_1, \cdots, x_{n-1}][y]$$

is monic in y. Let us denote $\tilde{x}_i = \bar{x}_i + c_i\bar{x}_n \in R$ for $1 \leq i \leq n-1$. Note that $R = K[\bar{x}_1, \cdots, \bar{x}_{n-1}, \bar{x}_m] = K[\tilde{x}_1, \cdots, \tilde{x}_{n-1}, \bar{x}_m]$. Finally, the ring extension $K[\tilde{x}_1, \cdots, \tilde{x}_{n-1}] \subset R$ is finite, because R is generated over $K[\tilde{x}_1, \cdots, \tilde{x}_{n-1}]$ by the element $\bar{x}_n$ which satisfies the monic equation $\lambda^{-1}F(\tilde{x}_1, \cdots, \tilde{x}_{n-1}, y) = 0$. But now $K[\tilde{x}_1, \cdots, \tilde{x}_{n-1}]$ is a quotient of $K[x_1, \cdots, x_{n-1}]$. So by induction we can find $t_1, \cdots, t_d \in K[\tilde{x}_1, \cdots, \tilde{x}_{n-1}]$ which are algebraically independent and such that $S[t_1, \cdots, t_d] \subset K[\tilde{x}_1, \cdots, \tilde{x}_{n-1}]$ is finite. From this it follows that also $S[t_1, \cdots, t_d] \subset R$ is finite. □

Before showing that if R is a domain then d is the transcendental degree of $\mathrm{Frac}(R)$, we prove the following useful proposition:

Proposition 3. *Let $S \subset R$ be an integral extensions of domains. Then R is a field if and only if S is a field.*

Proof. Let us assume that S is a field, and pick $r \in R \setminus 0$. Since r is integral over S it satisfies a monic equation of the form

$$r^n + s_{n-1}r^{n-1} + \cdots + s_1 r + s_0 = 0.$$

Let $i = \min\{j \colon s_j \neq 0\}$, so the equation above is

$$r^n + s_{n-1}r^{n-1} + \cdots + s_i r^i = 0$$

with $s_i \neq 0$. But then $r^i(r^{n-1} + s_{n-1}r^{n-1-i} + \cdots + s_i) = 0$ and since R is a domain by assumption and $r \neq 0$, this shows that $r^{n-1} + s_{n-1}r^{n-1-i} + \cdots + s_i = 0$. So we can assume that $i = 0$. Now, $s_0 \in S \setminus 0$ and since S is a field by assumption we can invert s_0 in S. Then we compute

$$r \cdot \frac{r^{n-1} + s_{n-1}r^{n-2} + \cdots + s_1}{-s_0} = 1,$$

which shows that r is invertible in R.

Assume now that R is a field, and let $s \in S \setminus 0$. Then $r := s^{-1}$ exists in R. Since R is integral over S, we find again a monic polynomial with coefficients in S such that

$$r^n + s_{n-1}r^{n-1} + \cdots + s_1 r + s_0 = 0;$$

we multiply now both sides by s^{n-1} and find

$$r + s_{n-1} + \cdots + s_1 s^{n-2} + s_0 s^{n-1} = 0$$

hence

$$r = -s_{n-1} - \cdots - s_1 s^{n-2} - s_0 s^{n-1} \in S.$$

□

Let us now prove the last statement in in the Noether's normalization lemma. So we assume that R is a domain, and let $S = K[t_1, \cdots, t_d]$ be a polynomial algebra such that $S \subset R$ is finite. This means that there are integral elements $r_1, \cdots, r_k \in R$ such that $R = S[r_1, \cdots, r_k]$. Now consider the field extension $\mathrm{Frac}(S) \subset F = \mathrm{Frac}(R)$. The ring extension $\mathrm{Frac}(S) \subset \mathrm{Frac}(S)[r_1, \cdots, r_k]$ is finite and hence integral. Moreover, $\mathrm{Frac}(S)[r_1, \cdots, r_k] \subset F$ is necessarily a domain. By the previous proposition we deduce that $\mathrm{Frac}(S)[r_1, \cdots, r_k]$ if a field, which must necessarily be equal to F. Hence, the field extension $\mathrm{Frac}(S) \subset F$ is algebraic (i.e., it has finite degree), from which we deduce that $d = \mathrm{tr.deg}_K(\mathrm{Frac}(S)) = \mathrm{tr.deg}_K(F)$.

Let us gather some interesting consequences:

Corollary 4. *Let $R = K[x_1, \cdots, x_n]/I$ be a domain. Then*

$$\mathrm{tr.deg}_K(\mathrm{Frac}(R)) = 0 \iff R \text{ is a field.}$$

Proof. By Noether normalization, we can find a polynomial algebra $S = K[t_1, \cdots, t_d]$ such that $S \subset R$ is finite. Now, if R is a field, S must be a field too, because the extension is integral, and hence $d = 0$ necessarily. Similarly, if $\mathrm{tr.deg}_K(\mathrm{Frac}(R)) = 0$ then $K \subset R$ must be integral, and henc R is a field. □

Lemma 5. *Let R be a domain and let $\dim(R)$ be its Krull dimension. Then $\dim(R) = 0$ if and only if R is a field.*

Proof. Clearly, if R is a field, then its Krull dimension is zero. Now, assume that R has Krull dimension zero and take $r \in R \setminus 0$. Note that r is invertible if and only if the ideal it generates $(r) \subset R$ is the whole ring. But if $(r) \neq R$ then there is a maximal ideal $(r) \subset m$ which contains it. Since R is a domain (0) is a prime ideal, hence the chain $(0) \subset m$ shows that the Krull dimension of R is at least one. □

In particular, recall that one of our goals is to prove that if R is a finitely generated K-algebra which is also a domain, then $\dim(R) = \mathrm{tr.deg}_K(\mathrm{Frac}(R))$. The results above show this particular case:

Corollary 6. *In the notation above, $\dim(R) = 0$ if and only if $\mathrm{tr.deg}_K(\mathrm{Frac}(R)) = 0$.*

2 Tensor products

We now introduce tensor products of modules, which is one of the most basic tools in commutative algebra. Let R be a ring, and let N, M, P be R-modules.

Definition 7. A map $\phi\colon M \oplus N \to P$ is bilinear (over R) if

1. $\phi(m_1 + m_2, n) = \phi(m_1, n) + \phi(m_2, n)$ for every $m_1, m_2 \in M$ and $n \in N$;
2. $\phi(m, n_1 + n_2) = \phi(m, n_1) + \phi(m, n_2)$ for every $m \in M$ and $n_1, n_2 \in N$;
3. $r \cdot \phi(n, m) = \phi(rn, m) = \phi(n, rm)$ for $r \in R$ and $n \in N$ and $m \in M$.

Bilinear maps appear everywhere, let us make some examples:

Example.

1. Let K be a field, and let $A \in M_{n\times n}(K)$ be a matrix. Then $K^n \times K^n \to K$ given by $(v, w) \mapsto v^t \cdot A \cdot w$ is bilinear.

2. Let R, T, S be rings, and let $f: R \to S$ and $g: T \to S$ be ring homomorphisms. Note that every ring can be seen in a natural way as a $\mathbb{Z}$-module. Then, the map $R \oplus T \to S$ given by $(r, t) \mapsto f(r)g(t)$ is $\mathbb{Z}$-bilinear.

3. Let $I, J \subset R$ be ideals such that $I + J = (1)$. Now consider a R-bilinear map $\phi: R/I \oplus R/J \to P$ where P is any R-module. We want to show that ϕ is identically zero. By assumption, we can write $1 = i + j$ for $i \in I$ and $j \in J$. For any $x \in R/I$ and $y \in R/J$ we have $\phi(x, y) = (i + j) \cdot \phi(x, y) = i \cdot \phi(x, y) + j \cdot \phi(x, y) = \phi(ix, y) + \phi(x, jy) = 0 + 0$.

The tensor product is the universal object for bilinear maps, in the following sense:

Theorem 8. *Let R be a ring and let N, M be R-modules. Then, there is an R-module $N \otimes_R M$ together with a bilinear map $u: N \oplus M \to N \otimes_R M$ which satisfies the following universal property: for any other R-module P and bilinear map $b: N \oplus M \to P$, there is a unique R-module morphism $\tilde{b}: N \otimes_R M \to P$ such that b factorizes as*

$$b: N \oplus M \xrightarrow{u} N \otimes_R M \xrightarrow{\tilde{b}} P.$$

The module $N \otimes_R M$ is called the tensor product of N and M, and one denotes $n \otimes m := u(n, m)$.

Proof. The universal property says that if such a pair exists, then it is unique up to unique isomorphism (why?). So we only need to show that it exists, i.e., we need to construct it. Consider the free module $R^{N\oplus M}$. This is the free R-module generated by the elements of the set $N \oplus M$. So an R-basis of $R^{N\oplus M}$ is given by the elements $e_{n,m}$ where $(n, m) \in N \oplus M$ and every element of $R^{N\oplus M}$ if a finite sum of the form $\sum r_i e_{n_i,m_i}$.

We let now $K \subset R^{N\oplus M}$ be the submodule generated by the following elements:

- $e_{n_1+n_2,m} - e_{n_1,m} - e_{n_2,m}$ for $n_1, n_2 \in N$ and $m \in M$;
- $e_{n,m_1+m_2} - e_{n,m_1} - e_{n,m_2}$ for $n \in N$ and $m_1, m_2 \in M$;
- $e_{rn,m} - re_{n,m}$ for $r \in R$, $n \in N$ and $m \in M$;
- $e_{n,rm} - re_{n,m}$ for $r \in R$, $n \in N$ and $m \in M$.

Finally, we put $N \otimes_R M := R^{N\oplus M}/K$ and we let $u: N \oplus M \to N \otimes_R M$ be the map which sends $(n, m) \mapsto [e_{n,m}]$ where here the square brackets simply mean the equivalence class in the quotient $R^{N\oplus M}/K$. We claim that u is bilinear (infact, we have forced this to happen). For instance, we have $u(n_1 + n_2, m) = [e_{n_1+n_2,m}]$ but since $e_{n_1+n_2,m} - e_{n_1,m} - e_{n_2,m} \in K$ we have $[e_{n_1+n_2,m}] = [e_{n_1,m}] + [e_{n_2,m}]$. The other verifications are done in the same way, and we leave them to the reader.

Now we show that this satifies the universal property. Pick any R-bilinear map $b: N \oplus M \to P$. Note that if $\tilde{b}: N \otimes_R M \to P$ it necessarily sends $n \otimes m$ to $b(n, m)$. So, if it exists, it is once again unique. To show existence, we consider the unique map of R-module $\hat{b}\colon R^{N\oplus M} \to P$ which sends $e_{n,m} \mapsto b(n,m)$. This exists by the universal property of direct sums. So we only need to check that $K \subset \ker(\hat{b})$. This is again easily done, we verify it only for one of the defyining relations above (all the others are analogue): we have $\hat{b}(e_{n_1+n_2,m} - e_{n_1,m} - e_{n_2,m}) = \hat{b}(e_{n_1+n_2,m}) - \hat{b}(e_{n_1,m}) - \hat{b}(e_{n_2,m}) = b(n_1+n_2,m) - b(n_1,m) - b(n_2,m) = 0$ because b is bilinear. □

We won't say much more about tensor product in this course, although we will use it in some of the proofs in the next lectures. I will gather here some important facts to keep in mind (others can be found in the exercise sheets):

1. One has natural isomorphisms $N \otimes_R M \cong M \otimes N$ and $(N_1 \oplus N_2) \otimes_R M \cong (N_1 \otimes_R M) \oplus (N_2 \otimes_R M)$;

2. If N if a fixed R-module, then one can consider the functor $A \mapsto A \otimes_R N$. This is right exact, in the sense that if $0 \to A \to B \to C \to 0$ is a short exact sequence of R-modules, then $A \otimes_R N \to B \otimes_R N \to C \otimes_R N \to 0$ is exact. As for the Ext modules, we can extend the sequence above on the left and obtain a long exact sequence:

   $$\cdots \operatorname{Tor}^1_R(A,N) \to \operatorname{Tor}^1_R(B,N) \to \operatorname{Tor}^1_R(C,N) \to A \otimes_R N \to B \otimes_R N \to C \otimes_R N \to 0$$

   using the Tor functors.

3. A module N is said to be flat if $A \mapsto A \otimes_R N$ is exact. A ring morphism $R \xrightarrow{f} S$ is said to be flat if S is flat seen as a R-module (the R-module structure on S is given by $(r,s) \mapsto f(r)s$ for $r \in R$ and $s \in S$.)

4. If N, M are finitely generated R-modules, then also $N \otimes_R M$ is finitely generated.

5. Finally, if $R \to S$ and $R \to T$ are ring morphisms, then $S \otimes_R T$ is a ring in a natural way. This is a fundamental construction which will be used in algebraic geometry to construct fibre products of schemes.