LECTURE 27

(27.0) Splitting extensions.– Recall that last time we proved the existence and uniqueness (up to a non–unique isomorphism) of splitting extension of a set of polynomials. More precisely, for a field K and a set of polynomials $P \subset K[x]$, there exists a unique field extension L/K such that (i) every polynomial $p(x) \in P$ splits completely in $L[x]$ and (ii) the smallest subfield of L containing K and the roots of all the polynomials from P is L itself.

Recall that the argument for its existence had three main steps:

- We can adjoin one root of an irreducible polynomial (Kronecker's theorem).
- By induction, we proved the existence of the splitting extension of a finite set of polynomials.
- Direct limit of the splitting extensions corresponding to finite subsets of P is the splitting extension for P.

In this lecture we will go over the theory of *symmetric polynomials*, and see two of its applications. Next time we will use the basic results about symmetric polynomials (Proposition 27.2 and Theorem 27.3) to give a different proof of the existence of splitting extensions.

(27.1) Symmetric polynomials.– Let A be a unital commutative ring and let $n \in \mathbb{Z}_{\geq 0}$. We denote by $\mathfrak{S}_n$ the symmetric group on n letters. Consider the ring of polynomials in n variables, with coefficients from A, and the natural action of $\mathfrak{S}_n$:

$$\mathfrak{S}_n \circlearrowright R = A[x_1, \ldots, x_n]$$

given by $(\sigma \cdot p)(x_1, \ldots, x_n) = p(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$.

Definition. A polynomial $p(x_1, \ldots, x_n) \in R$ is symmetric if $\sigma \cdot p = p$, for every $\sigma \in \mathfrak{S}_n$. The set of all symmetric polynomials is denoted by $S = R^{\mathfrak{S}_n} \subset R$, and is an A–subalgebra of R.

$$S = \{p \in R : \sigma \cdot p = p \ \forall\ \sigma \in \mathfrak{S}_n\}$$

(27.2) Elementary symmetric polynomials.– We keep the notations of the previous paragraph.

Definition. For each $k \in \mathbb{Z}_{\geq 0}$, the k^{th} elementary symmetric polynomial, denoted by $e_k(x_1, \ldots, x_n)$ (or just e_k if the number of variables is clear from the context) is defined as:

$$\boxed{e_k(x_1, \ldots, x_n) = \sum_{1 \leq i_1 < \ldots < i_k \leq n} x_{i_1} \cdots x_{i_k}}$$

Note that $e_0 = 1$ and $e_k = 0$ for every $k > n$. Each e_k is homogeneous of degree k (if we assign degree 1 to each of the variables $x_1, \ldots, x_n$).

It is clear that $e_k \in S = R^{\mathfrak{S}_n}$. For instance,

$$e_1 = x_1 + \cdots + x_n, \qquad e_2 = \sum_{i<j} x_i x_j, \qquad e_n = x_1 \cdots x_n.$$

Proposition.

(1) *We have the following identity:*

$$\boxed{\prod_{i=1}^{n}(x - x_i) = x^n + \sum_{k=1}^{n}(-1)^k e_k(x_1, \ldots, x_n) x^{n-k}}$$

(2) $(-1)^{n+1} e_n = x_n^n + \sum_{k=1}^{n-1}(-1)^k e_k x_n^{n-k}$.

(3) *Let* $e'_k = e_k(x_1, \ldots, x_{n-1})$ *and* $e_k = e_k(x_1, \ldots, x_n)$. *That is,* $e'_k = e_k|_{x_n=0}$. *Then we have:*

$$e_k = e'_k + e'_{k-1} x_n, \qquad e'_k = \sum_{j=0}^{k}(-1)^j x_n^j e_{k-j}.$$

Here, $e'_{-1} = 0$ *(if* $k = 0$ *in the first equation).*

Proof. (1) is obtained by expanding the left–hand side. (2) follows from (1) if we substitute $x = x_n$.

The first identity in (3) is clear from the definition of e_k. The second one is obtained simply by inverting the first one (or an easy induction on k argument). $\square$

(27.3) Main theorem of symmetric polynomials.– Again, we keep the notations as above: A is a unital commutative ring, $R = A[x_1, \ldots, x_n]$, $S = R^{\mathfrak{S}_n}$, and $e_k \in S$ $(1 \leq k \leq n)$.

Theorem.

(1) *S is generated, as an algebra over A, by* $\{e_1, \ldots, e_n\}$.

(2) $\{e_1, \ldots, e_n\}$ *are algebraically independent.*

(3) *As an S–module, R is free of rank $n!$. More precisely, the following set of $n!$ monomials is an S–basis for R:*

$$\{x_1^{k_1} \cdots x_n^{k_n} : 0 \leq k_j < j, \ \forall\ j = 1, \ldots, n\}.$$

Proof. Our proof of this theorem is going to be based on induction. The base case of the induction is when $n = 0$, $R = S = A$ and there is nothing to show. Our induction hypothesis is that the theorem is true for $n - 1$, and we will prove it for n.

Let us prove (1) first. Let $p(x_1, \ldots, x_n) \in S$ be homogeneous of degree m. We want to argue, by (a second) induction on m, that p can be written as a polynomial in $e_1, \ldots, e_n$, with coefficients from A. If $m = 0$, then $p \in A$ and there is nothing to prove. Otherwise, consider:

$$p' = p(x_1, \ldots, x_{n-1}, 0) \in A[x_1, \ldots, x_{n-1}]^{\mathfrak{S}_{n-1}}.$$

By induction hypothesis (on n) there exists a polynomial $P(y_1, \ldots, y_{n-1}) \in A[y_1, \ldots, y_{n-1}]$ such that $p' = P(e'_1, \ldots, e'_{n-1})$. Here, we are using the same notation as in Proposition 27.2 (2) above. Now it is clear that $p(x_1, \ldots, x_n) - P(e_1, \ldots, e_{n-1})$ is divisible by x_n. Since it is symmetric, it must also be divisible by $x_1, x_2, \ldots, x_{n-1}$. That is,

$$p(x_1, \ldots, x_n) - P(e_1, \ldots, e_{n-1}) = q(x_1, \ldots, x_n) \cdot (x_1 \cdots x_n) = q(x_1, \ldots, x_n) \cdot e_n,$$

with $\deg(q) < \deg(p)$. This finishes the proof of (1).

Now we prove (2) and (3). For this, consider

$$\widetilde{S} = R^{\mathfrak{S}_{n-1}} = A[x_1, \ldots, x_n]^{\mathfrak{S}_{n-1}} = (A[x_n])[x_1, \ldots, x_{n-1}]^{\mathfrak{S}_{n-1}}.$$

That is, $\widetilde{S}$ is the ring of symmetric polynomials in $n - 1$ variables $x_1, \ldots, x_{n-1}$ with coefficients from $A[x_n]$. By induction hypothesis (on n), $\widetilde{S}$ is generated (as an $A[x_n]$–algebra) by algebraically independent elements $e'_1, \ldots, e'_{n-1}$:

$$\widetilde{S} = (A[x_n])[e'_1, \ldots, e'_{n-1}].$$

By Proposition 27.2 (3) above, the two sets $\{e'_1, \ldots, e'_{n-1}\}$ and $\{e_1, \ldots, e_{n-1}\}$ are related by invertible linear (over $A[x_n]$) transformations. Hence, we conclude that $e_1, \ldots, e_{n-1}$ are algebraically independent over $A[x_n]$ (in particular, over A), and can write:

$$\widetilde{S} = A[x_n, e_1, \ldots, e_{n-1}] = (A[e_1, \ldots, e_{n-1}])[x_n].$$

Let us pause and recollect what we know by now. We have shown that $\{e_1, \ldots, e_{n-1}, x_n\}$ are algebraically independent over A. We also know that S is generated by $\{e_1, \ldots, e_n\}$ as an A–algebra. That is, if we write $C = A[e_1, \ldots, e_{n-1}]$, then S is the image of $\varphi : C[T] \to \widetilde{S} = C[x_n]$, where:

$$\varphi(T) = e_n = (-1)^{n+1} x_n^n + \sum_{j=1}^{n} (-1)^{n-j+1} e_j x_n^{n-j}, \quad \text{by Prop. 27.2 (2) above.}$$

Note that $\varphi(T)$ is a degree n polynomial in variable x_n, whose leading coefficient ± 1 is invertible. First of all, this implies that φ is injective, since if $p(T) \in C[T]$ is of degree $N \geq 1$ (in T variable), then $\varphi(p(T))$ will have (± 1) same leading coefficient as $p(T)$, in degree Nn in x_n variable. This proves (2), that is, $\{e_1, \ldots, e_n\}$ are algebraically independent over A.

Secondly, Euclidean division algorithm can be performed to divide a given element of $C[x_n]$ by $\varphi(T)$. Thus $\{1, x_n, \ldots, x_n^{n-1}\}$ is an S–basis of $\widetilde{S}$. Combined with induction hypothesis, this proves (3). $\square$

(27.4) Remark.– Note that our proof of (1) of Theorem 27.3 above gives an efficient algorithm to express a given symmetric polynomial $p(x_1, \ldots, x_n)$ as a polynomial in $e_1, \ldots, e_n$. Namely:

- Set $x_n = 0$ and express the resulting polynomial in $n-1$ variables, say p', as a polynomial $P(e'_1, \ldots, e'_{n-1})$.
- Take the difference $p(x_1, \ldots, x_n) - P(e_1, \ldots, e_{n-1})$, divide it by $e_n = x_1 \cdots x_n$ to get another symmetric polynomial $q(x_1, \ldots, x_n)$ of degree $\deg(p) - n$.
- If $\deg(q) = 0$, we are done. Otherwise, repeat the previous two steps for q.

For instance, let $p = x_1^2(x_2 + x_3) + x_2^2(x_3 + x_1) + x_3^2(x_1 + x_2) \in \mathbb{Z}[x_1, x_2, x_3]^{\mathfrak{S}_3}$. Then:

$$p' = x_1^2 x_2 + x_1 x_2^2 = e'_1 e'_2.$$

Now we compute:

$$p - e_1 e_2 = x_1^2(x_2 + x_3) + x_2^2(x_3 + x_1) + x_3^2(x_1 + x_2) - (x_1 + x_2 + x_3)(x_1 x_2 + x_2 x_3 + x_1 x_3)$$

$$= -3x_1 x_2 x_3 = -3e_3.$$

So $p = e_1 e_2 - 3e_3$.

(27.5) Application I.– Let K be any field, and let $T_1, \ldots, T_n$ be variables.

- Let $R = K[T_1, \ldots, T_n]$, $F(R) = K(T_1, \ldots, T_n)$ (field of fractions of R). Note that we have a group homomorphism $\mathfrak{S}_n \to \mathrm{Aut}(F(R))$, the group of field automorphisms of $F(R)$.

- $S = R^{\mathfrak{S}_n} = K[e_1, \ldots, e_n]$, where e_k's are the elementary symmetric polynomials in $T_1, \ldots, T_n$. Let $F(S) = K(e_1, \ldots, e_n)$ denote the field of fractions of S.

Corollary.

(1) $F(S) = F(R)^{\mathfrak{S}_n}$.
(2) $F(R)$ *is* $n!$ *dimensional* $F(S)$*–vector space. That is:*

$$\boxed{[F(R) : F(S)] = n!}$$

PROOF. It is clear that $F(S) \subset F(R)^{\mathfrak{S}_n}$. For the converse, assume that $p/q \in F(R)$ is symmetric (where $p, q \in R = K[T_1, \ldots, T_n]$).

$$\frac{p}{q} = \frac{p \prod_{\substack{\sigma \in \mathfrak{S}_n \\ \sigma \neq \mathrm{Id}}} (\sigma \cdot q)}{\prod_{\sigma \in \mathfrak{S}_n} (\sigma \cdot q)}.$$

Now the denominator of the right–hand side is symmetric. Hence, so must be the numerator since p/q is symmetric. So $p/q \in F(S)$.

(2) follows from Theorem 27.3 (3) and an argument similar to the one above. Consider the basis of R as a rank $n!$ free S–module given in Theorem 27.3 (3). For notational ease, we will write $m(\underline{k})$ for $x_1^{k_1} \cdots x_n^{k_n}$. The indexing set will be denoted by I:

$$I = \{\underline{k} = (k_1, \ldots, k_n) : 0 \leq k_j < j, \ \forall\, j\}, \qquad B = \{m(\underline{k}) : \underline{k} \in I\} \subset R.$$

We will show that B spans $F(R)$ as $F(S)$–vector space, and is linearly independent.

Let $p/q \in F(R)$. Multiplying and dividing this element by $\prod_\sigma (\sigma \cdot q)$, where the product is over all non–identity permutations, we may assume that the denominator is symmetric. By Theorem 27.3 (3), we can write:

$$\frac{p}{q} = \frac{1}{q}\left(\sum_{\underline{k}\in I} c(\underline{k}) m(\underline{k})\right) = \sum_{\underline{k}\in I} \frac{c(\underline{k})}{q} m(\underline{k})$$

where $c(\underline{k}) \in S$ for every $\underline{k} \in I$, hence $c(\underline{k})/q \in F(S)$. Therefore, B spans $F(R)$. For linear independence, if we have a linear dependence relation:

$$\sum_{\underline{k}\in I} a(\underline{k}) m(\underline{k}) = 0, \quad \text{where } a(\underline{k}) \in F(S),$$

then we can clear the denominator to assume that $a(\underline{k}) \in S$. By Theorem 27.3 (3), this implies that each $a(\underline{k}) = 0$. □

(27.6) Application II. Discriminants.– Let K be a field, and assume that $p(x) \in K[x]$ is monic polynomial of degree n. Let L/K be an extension of K. Assume there exist $r_1, \ldots, r_n \in L$ such that $p(x) = (x - r_1) \cdots (x - r_n)$ in $L[x]$. As another application of Theorem 27.3, we have that *every symmetric polynomial in $r_1, \ldots, r_n$ is an element of K, which can be written as a polynomial in the coefficients of $p(x)$.*

Corollary. *Let $P(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]^{\mathfrak{S}_n}$. Then, $P(r_1, \ldots, r_n) \in K$. Moreover, if $p(x) = x^n + \sum_{j=1}^{n} a_j x^{n-j}$, where $a_1, \ldots, a_n \in K$, then $P(r_1, \ldots, r_n)$ is a polynomial in $a_1, \ldots, a_n$.*

Proof. By Theorem 27.3, $P(x_1, \ldots, x_n) = Q[e_1, \ldots, e_n]$ for a unique polynomial Q in $K[y_1, \ldots, y_n]$. By Proposition 27.2 (1), $e_j(r_1, \ldots, r_n) = (-1)^j a_j$. This finishes the proof. □

For instance, let $\mathrm{Disc}(p) = \prod_{i\neq j}(r_i - r_j) \in L$. Since this is symmetric in the roots, we get that $\mathrm{Disc}(p) \in K$ is a polynomial in the coefficients of p, called the *discriminant of* p. By definition, $\mathrm{Disc}(p) = 0$ if, and only if p has *repeated roots* in L.

As an example, if $p(x) = x^2 + bx + c = (x - r)(x - s)$, then $r + s = -b$ and $rs = c$. $\mathrm{Disc}(p)$ is computed as:

$$(r - s)(s - r) = -(r - s)^2 = -((r + s)^2 - 4rs) = -(b^2 - 4c).$$