LECTURE 28

(28.0) Review.– Last time we stated and proved the main theorem about symmetric polynomials (Theorem 27.3). We saw two of its applications (Corollaries 27.5 and 27.6) which stated the following.

- For a field K and a non–negative integer n, the field extension:
$$F(S) = K(T_1, \ldots, T_n)^{\mathfrak{S}_n} \subset F(R) = K(T_1, \ldots, T_n)$$
is of degree $n!$.
- Let $p(x) \in K[x]$ be monic of degree n. Let $r_1, \ldots, r_n \in L$ be its roots in an extension L/K. Then every symmetric polynomial in $r_1, \ldots, r_n$ is a polynomial in the coefficients of $p(x)$, hence an element of K.

(28.1) Application III: Existence of splitting extensions.– We can use Theorem 27.3 to give another proof of the existence of splitting extensions.

Proposition. *Let K be a field and let $p(x) \in K[x]$ be a monic polynomial of degree n. Then there exists a field extension L/K and $r_1, \ldots, r_n \in L$ such that*

(1) $p(x) = \displaystyle\prod_{i=1}^{n}(x - r_i)$ *in* $L[x]$.
(2) $L = K(r_1, \ldots, r_n)$.

PROOF. Let $R = K[x_1, \ldots, x_n]$ and $S = R^{\mathfrak{S}_n} = K[e_1, \ldots, e_n]$, where e_k is the degree k elementary symmetric polynomial in $x_1, \ldots, x_n$. Write $p(x) = x^n + \sum_{j=1}^n a_j x^{n-j} \in K[x]$, and define the ideal $\mathfrak{a} = (e_k - (-1)^k a_k : 1 \leq k \leq n) \subset R$. Set $\overline{R} := R/\mathfrak{a}$.

Claim. $\mathfrak{a} \subsetneq R$. Hence, $\overline{R} \neq \{0\}$.

Given the claim, we can choose a maximal ideal $\mathfrak{m} \subsetneq \overline{R}$ and define $L = \overline{R}/\mathfrak{m}$. Let $\pi : R \to L$ be the natural quotient homomorphism. Composing the ring homomorphisms $K \hookrightarrow R \twoheadrightarrow L$, we obtain $K \to L$ which is necessarily injective, showing that L is a field extension of K. Let $r_i = \pi(x_i) \in L$ $(1 \leq i \leq n)$. As $p(x) = \prod(x - \overline{x_i})$ in $\overline{R}[x]$, we get the following in $L[x]$.
$$p(x) = \prod_{i=1}^{n}(x - r_i), \quad \text{in } L[x].$$
Similarly, since R is generated as an K–algebra by $x_1, \ldots, x_n$, $L = K(r_1, \ldots, r_n)$.

Proof of the claim. Note that $\mathfrak{a} = R \iff \overline{R} = \{0\}$. We will show that $\overline{R}$ is $n!$–dimensional K vector space, which will prove the claim. For this, recall that (Theorem 27.3) $S = R^{\mathfrak{S}}$ if a polynomial ring $S = K[e_1, \ldots, e_n]$. Hence there exists a ring homomorphism

$\psi : S \to K$ such that $\psi(e_k) = (-1)^k a_k$. This allows us to view $K \cong S/\operatorname{Ker}(\psi)$ as an S–module, and by definition $\mathfrak{a} = \operatorname{Ker}(\psi)R \subset R$. Viewing R as $S^{\oplus n!}$, we get:

$$\overline{R} = R/\mathfrak{a} = R \otimes_S (S/\operatorname{Ker}(\psi)) \cong (S \otimes_S S/\operatorname{Ker}(\psi))^{\oplus n!} = K^{n!} \text{ as a } K--\text{vector space.}$$

This finishes the proof of the claim. □

(28.2) Application III continued.– Now let $P \subset K[x]$ consist of monic polynomials. For every $p(x) \in P$, let L_p/K be the field extension constructed above. Define:

$$\mathcal{R} = \bigotimes_{p \in P} L_p,$$

as an infinite tensor product of finite–dimensional K–vector spaces. Note that we have $\phi : K \to \mathcal{R}$, given by sending $1 \in K$ to $\otimes_p 1_p$, where $1_p \in L_p$ is the unit element. We consider componenet–wise multiplication on $\mathcal{R}$ which gives it a structure of a (unital, commutative) K–algebra. Moreover, $\mathcal{R} \neq \{0\}$, since upon choosing a basis $\{\xi_1^{(p)}, \dots, \xi_{\ell_p}^{(p)}\}$ of L_p as a K–vector space, we get a basis of $\mathcal{R}$:

$$\left\{ \otimes_{p \in P} \xi_{j_p}^{(p)} : 1 \leq j_p \leq \ell_p \right\}.$$

Now we proceed as before. Choose a maximal ideal $M \subsetneq \mathcal{R}$, and define $L = \mathcal{R}/M$, which is easily seen to be a splitting extension of $P \subset K[x]$.

(28.3) Fundamental theorem of algebra.– We can now give a proof of the fundamental theorem of algebra. We view $\mathbb{C} \cong \mathbb{R}[x]/(x^2+1)$ as a degree 2 extension of $\mathbb{R}$. Let $\iota := \overline{x} \in \mathbb{C}$ so that $\iota^2 = -1$.

The following proof was sketched by Euler in 1749, and completed by Lagrange in 1776. At the time of its appearance, this proof was considered *incomplete* but these objections were superficial in nature, and the underlying idea is definitely flawless.

Theorem. $\mathbb{C}$ *is the algebraic closure of* $\mathbb{R}$.

Proof. Note that it is sufficient to show that every $f(x) \in \mathbb{R}[x]$ has a root in $\mathbb{C}$. If the root α lies in $\mathbb{R}$, then $f(x) = (x-\alpha)g(x)$ with $g(x) \in \mathbb{R}[x]$ of smaller degree. If $\alpha \in \mathbb{C} \setminus \mathbb{R}$ is a root, then so is $\overline{\alpha}$ and we get

$$f(x) = (x-\alpha)(x-\overline{\alpha})h(x) = (x^2 - 2\operatorname{Re}(\alpha)x + |\alpha|^2)h(x),$$

so $h(x) \in \mathbb{R}[x]$ and it has smaller degree than $f(x)$.

The proof is split into three claims.

Claim 1. Every odd degree polynomial in $\mathbb{R}[x]$ has a real root.

Proof. This is the only topological step and requires the intemediate value theorem[1]. Namely, if $p(x) \in \mathbb{R}[x]$ is of odd degree, then $\lim\limits_{x\to\pm\infty} p(x) = \pm\infty$, hence we can find two real numbers $a < b \in \mathbb{R}$ such that $p(a) < 0$ and $p(b) > 0$. Therefore, there must be some real number $c \in (a, b)$ such that $p(c) = 0$.

Claim 2. Every quadratic polynomial with coefficients from $\mathbb{C}$ splits in $\mathbb{C}$.

Proof. This is easily shown by the well–known formula for quadratic polynomials. For $b, c \in \mathbb{C}$, we have:

$$x^2 + bx + c = 0, \qquad \Rightarrow \qquad x = \frac{-b + \sqrt{b^2 - 4c}}{2} \in \mathbb{C}.$$

Claim 3. Every $p(x) \in \mathbb{R}[x]$ has a root in $\mathbb{C}$.

Proof. Without loss of generality, we may assume that $p(x)$ is monic. Note that the claim is true for linear and quadratic polynomials. Let us write $\deg(p) = 2^n m$ where m is odd. Our argument is going to be by induction on n. The base case, $n = 0$ is settled in the first claim.

Let $L/\mathbb{C}$ be an extension where $p(x)$ splits[2]. Let $r_1, \ldots, r_N \in L$ be roots of $p(x)$ in L ($N = 2^n m = \deg(p)$). For every $b \in \mathbb{R}$, define:

$$y_{ij}(b) = r_i + r_j + br_ir_j \in L, \qquad P^{(b)}(x) = \prod_{1\le i<j\le N} (x - y_{ij}(b))$$

Note that coefficients of $P^{(b)}(x) \in L[x]$ are symmetric under permutation of $r_1, \ldots, r_N$. Therefore, by Corollary 27.6, $P^{(b)}(x) \in \mathbb{R}[x]$, and

$$\deg(P^{(b)}(x)) = 2^{n-1}m(2^n m - 1),$$

has smaller exponent of 2 dividing its degree. By induction hypothesis, it has a root in $\mathbb{C}$, that is, there is a pair $i < j$ such that $y_{ij}(b) \in \mathbb{C}$.

Since there are infinitely many real numbers, and for each $b \in \mathbb{R}$ there is a pair $i < j$ with $y_{ij}(b) \in \mathbb{C}$, we can find two different $b \neq c \in \mathbb{R}$ which have the same pair (i, j), that is, there exists $i < j$ such that $y_{ij}(b), y_{ij}(c) \in \mathbb{C}$. Solving the linear system, we conclude that

$$r_i + r_j + br_ir_j \ \text{ and } \ r_i + r_j + cr_ir_j \in \mathbb{C} \qquad \Rightarrow \qquad r_i + r_j, r_ir_j \in \mathbb{C}.$$

Now $x^2 - (r_i + r_j)x + r_ir_j \in \mathbb{C}[x]$ is a quadratic polynomial. By Claim 2, its roots lie in $\mathbb{C}$. But its roots are r_i and r_j. So, $r_i, r_j \in \mathbb{C}$. Hence, $p(x) = 0$ has a root in $\mathbb{C}$. $\square$

Corollary.

(1) *If* $p(x) \in \mathbb{R}[x]$ *is irreducible, then* $\deg(p) = 1$ *or* 2.

[1]Intermediate value theorem was proved by Bolzano in 1817. Bolzano's argument rested on the fact that every bounded infinite set of real numbers has a cluster point, which was rigorously proved by Weierstrass in 1872 (now called Bolzano–Weierstrass theorem).

[2]This is the part of Euler–Lagrange's proof that was heavily criticized by, for instance, Gauss, to whom the first *complete* proof is often attributed. Gauss objected that the proof requires the existence of roots in order to show existence of the roots.

(2) $\overline{\mathbb{Q}} := \{z \in \mathbb{C} : z$ *is algebraic over* $\mathbb{Q}\} \subset \mathbb{C}$ *is the algebraic closure of* $\mathbb{Q}$.

(28.4) Group of automorphisms: Galois group.– Let L/K be an arbitrary field extension.

Definition. The *group of automorphisms of* L over K, denoted by $\mathsf{G}(L/K)$, also called the *Galois group* of L/K, is defined as:

$$\mathsf{G}(L/K) = \left\{\sigma : L \xrightarrow{\sim} L \text{ field automorphism such that } \sigma|_K = \mathrm{Id}_K\right\}$$

Remark. Note that $\mathsf{G}(L/K)$ acts on L via field automorphisms. As usual, we denote by $F = L^{\mathsf{G}(L/K)} \subset L$ the subfield of elements fixed by $\mathsf{G}(L/K)$:

$$F = L^{\mathsf{G}(L/K)} = \{r \in L : \sigma(r) = r,\ \forall\ \sigma \in \mathsf{G}(L/K)\}.$$

It is clear that $K \subset F$, however the reverse inclusion is false in general. For instance, let $K = \mathbb{Q}$ and $L = \mathbb{Q}(2^{\frac{1}{3}}) \subset \mathbb{R}$. It is not hard to show that $\mathsf{G}(L/K) = \{\mathrm{Id}\}$. Therefore $K \subsetneq L^{\mathsf{G}(L/K)} = L$.

(28.5) Galois extensions.– Next week we will discuss two results (due to Dedekind and Artin), which will help us find inequalities relating $|\mathsf{G}(L/K)|$ and the degree of the extension $[L : K]$. For now, we can give a definition.

Definition. A field extension L/K is called a *Galois* extension, if

$$\boxed{K = L^{\mathsf{G}(L/K)}}$$

As we saw in the last paragraph, $\mathbb{Q}(2^{1/3})/\mathbb{Q}$ is not a Galois extension.

Example. $\mathbb{C}/\mathbb{R}$ is a Galois extension. Note that $\mathsf{G}(\mathbb{C}/\mathbb{R})$ contains complex conjugation $\sigma : \mathbb{C} \to \mathbb{C}$, given by $\sigma(z) = \overline{z}$. It is a very easy exercise to show that:

$$\mathsf{G}(\mathbb{C}/\mathbb{R}) = \{\mathrm{Id}, \sigma\} \cong \mathbb{Z}/2\mathbb{Z}.$$

We know that $z = \overline{z}$ if and only if the imaginary part of z is 0, i.e, $z \in \mathbb{R}$. Hence $\mathbb{C}^{\mathsf{G}(\mathbb{C}/\mathbb{R})} = \mathbb{R}$.

(28.6) Example: n^{th} roots of unity.– Let $n \in \mathbb{Z}_{\geq 2}$. The roots of $x^n - 1$ in $\mathbb{C}$ are often called n^{th} roots of unity, and are easy to list. Let

$$\omega_n = e^{\frac{2\pi}{n}\iota} \in \mathbb{C},$$

then we have:

$$x^n - 1 = \prod_{k=0}^{n-1} \left(x - \omega_n^k\right).$$

Thus $\mu_n = \{1, \omega_n, \omega_n^2, \ldots, \omega_n^{n-1}\} \subset \mathbb{C}$ is the set of n^{th} roots of unity. As a subgroup of $\mathbb{C}^{\times}$, we have $\mu_n \cong \mathbb{Z}/n\mathbb{Z}$.

Consider the field extension $\mathbb{Q}(\mu_n)$ of $\mathbb{Q}$. It is clear that $\mathbb{Q}(\mu_n)$ is the splitting extension of $x^n - 1$ over $\mathbb{Q}$. Note that, for every field automorphism $\sigma : \mathbb{Q}(\mu_n) \to \mathbb{Q}(\mu_n)$, $\sigma(\omega_n)$ is another root of $x^n - 1$, hence given by $\sigma(\omega_n) = \omega_n^k$ for some $0 \leq k \leq n-1$. Moreover, in order to be surjective, it is necessary and sufficient that $\gcd(k, n) = 1$. Thus we conclude:

$$\mathsf{G}\left(\mathbb{Q}(\mu_n)/\mathbb{Q}\right) = \mathrm{Aut}_{\mathrm{gp}}\left(\mathbb{Z}/n\mathbb{Z}\right)$$

The complex conjugation is still an element of $\mathsf{G}\left(\mathbb{Q}(\mu_n)/\mathbb{Q}\right)$ and can be used to conclude that $\mathbb{Q}(\mu_n)/\mathbb{Q}$ is a Galois extension.