LECTURE 24

(24.0) Galois theory: a bit of history.– Our next, and last topic of this course is *Galois theory*. While motivated by the problem of "solvability by radicals" of a polynomial equation, Galois theory has since evolved in a significant way and has become crucial in many areas of mathematics. A quick look at the historical developments is provided here (see *Bourbaki, Algebra, Historical notes to Chapter V: Commutative Fields* for a more thorough and fun read).

The following formula has been known since the time of Babylonian mathematics (around 1800 BC).

$$ax^2 + bx + c = 0 \qquad \Rightarrow \qquad x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

After the fall of Babylon (539 BC), Greek mathematicians continued to develop techniques of arithmetic and gave several geometric proofs/interpretations of this formula. Especially Pythagoras (570-495 BC) and his school developed algorithms for extraction of a square-root. Their discovery of *irrational* numbers led philosophers (Plato (428-348 BC) and his academy) to re-think what it means to be a *number*. The general consensus of the time being *numbers have to be constructible* - via ruler and compass, or more sophisticated tools, for instance *spirals, cycloids*. Mathematicians of the time thus concerned themselves with determining which numbers are constructible, focusing on problems of the type *squaring a circle, doubling a cube* and so on. This direction is a bit tangential to our story to which we now return.

The first major breakthrough came in the early sixteenth century. Italian mathematician Scipio del Ferro (1465-1526) succeeded in solving a typical degree 3 polynomial equation. A simple linear change of variables gets rid of the the x^2 term, and for an equation $x^3 = ax + b$, his solution was:

$$x = \left(\frac{b}{2} + \sqrt{\left(\frac{b}{2}\right)^2 + \left(\frac{a}{3}\right)^3}\right)^{\frac{1}{3}} + \left(\frac{b}{2} - \sqrt{\left(\frac{b}{2}\right)^2 + \left(\frac{a}{3}\right)^3}\right)^{\frac{1}{3}}$$

If you would like to derive it for yourself, here is a hint which is very close to how Scipio del Ferro argued. Find two numbers r, s such that

$$rs = -\left(\frac{a}{3}\right)^3, \qquad r + s = b.$$

The trick is that $r^{\frac{1}{3}} + s^{\frac{1}{3}}$ will be a solution to $x^3 = ax + b$. These two equations become one quadratic equation for r, which we know how to solve.

Italian mathematicians of the sixteenth century continued working on such problems. Especially Gerolamo Cardona (1501-1576) and his student Lodovico de Ferrari (1522-1565) obtained a similar formula for a typical degree 4 equation. I am not going to reproduce the result here, but the idea is as follows. Start from a (monic, with no x^3 term) degree 4 equation: $x^4 = ax^2 + bx + c$. Add $2zx^2 + z^2$ to both sides to get (here z is to be determined

later):

$$(x^2+z)^2 = (a+2z)x^2 + bx + (c+z^2)$$

Next, we try to find two numbers A and B such that $(a+2z)x^2+bx+(c+z^2) = (Ax+B)^2$. If this were the case, our problem is solved, as $x^2+z = \pm(Ax+B)$ from which we extract the value of x.

Now the auxiliary equation $(a+2z)x^2+bx+(c+z^2) = (Ax+B)^2$, gives rise to:

$$a+2z = A^2, \qquad b = 2AB, \qquad c+z^2 = B^2,$$

from which we obtain the following cubic equation for z:

$$2z^3 + az^2 + 2cz + ac = \frac{b^2}{4}.$$

We know how to solve this, which gives a value for z, and A, B as above. Substituting it back gives a formula for x.

It was clear at that time what the precise problem is. Given a polynomial equation $x^n = a_{n-1}x^{n-1} + \cdots + a_0$, find a formula for x, in terms of the coefficients $\{a_0, \ldots, a_{n-1}\}$, involving only (i) rational functions, and (ii) k^{th} roots (in other words, *solve it by radicals*).

The list of names of famous mathematicians who contributed (positively) towards this problem is too long to include here (see Bourbaki's historical notes). Niels Henrik Abel (1802-1829) and his contemporary Évariste Galois (1811-1832) are the two main characters who finally finished this story. At a very young age, Abel believed that he had a formula for a degree 5 polynomial equation. However, he soon recognized his error, and became convinced that no such formula could possibly exist. Abel developed a general (algebraic) theory of elliptic functions (whose independent analytic treatment was discovered by Jacobi) to attack this problem. Abel's idea was to characterize all polynomial equations which can be solved by radicals. However, he passed away before he could finish his program. In his honour, certain algebraic extensions are called *abelian extensions*, whose groups of symmetries became known as *abelian groups*. It turns out that these could be any group where the group operation is commutative, which is why commutative groups are also called abelian groups.

Galois approached the problem of solvability by radicals, via considering the group of symmetries of the (not yet found) roots of a given polynomial equation (which we now call *Galois group*). He also had a very short life, but he succeeded in proving that polynomial equations of degree ≥ 5 cannot be solved by radicals, because *S_n is not a solvable group, for $n \geq 5$*. Hopefully, by the end of this topic we will see what this last statement precisely means.

(24.1) Fields.– Recall that a field is a (unital, commutative) ring where every non–zero element is invertible. In other words, $\{0\}$ is the only proper ideal of a field.

Since we require our ring homomorphisms to be unital, we have the following.

Lemma. *Let K be a field and A a commutative (unital) ring. Then every ring homomorphism $f : K \to A$ is injective.*

PROOF. As $\mathrm{Ker}(f) \subset K$ is a proper ideal ($1 \notin \mathrm{Ker}(f)$), it has to be zero, proving that f is injective. □

In other words, $\mathrm{Hom}_{\mathbf{Rings}}(K, A)$ is either empty, or consists entirely of injective morphisms.

(24.2) Characteristic of a field.– Let K be a field. Consider the natural ring homomorphism $i : \mathbb{Z} \to K$, defined on $n \in \mathbb{Z}_{\geq 1}$ as: $i(n) = \underbrace{1 + \cdots + 1}_{n \text{ terms}}$, and $i(-n) = -\iota(n)$. There are two possibilities for $\mathrm{Ker}(i)$:

- $\mathrm{Ker}(i) = \{0\}$. In this case, i extends to a unique homomorphism (still denoted by i) $\mathbb{Q} \to K$ (since for every $n \in \mathbb{Z}_{\neq 0}$, $i(n) \in K$ is non–zero, hence invertible). Being a homomorphism from a field, it has to be injective, by Lemma 24.1 above.

- $\mathrm{Ker}(i) = (p)$ for some $p \in \mathbb{Z}_{\geq 2}$. In this case, we get an injective ring homomorphism $i : \mathbb{Z}/p\mathbb{Z} \to K$. As K is an integral domain, so will be $\mathbb{Z}/p\mathbb{Z}$ proving that p has to be a prime number.

Let $\mathbb{F}_p$ denote the field $\mathbb{Z}/p\mathbb{Z}$, where $p \in \mathbb{Z}_{\geq 2}$ is a prime number. We summarize our preceding argument as:

Proposition. *Let K be a field. Then either $\mathbb{Q} \hookrightarrow K$, or there exists a prime number $p \in \mathbb{Z}_{\geq 2}$ such that $\mathbb{F}_p \hookrightarrow K$.*

Definition. We say K is of *characteristic zero* if $\mathbb{Q} \hookrightarrow K$. If $\mathbb{F}_p \hookrightarrow K$, we say that the characteristic of K is p (or K is of characteristic p). The characteristic of a field K is denoted by $\mathrm{Char}(K)$.

Note that the inclusions mentioned in this definition are *canonical*, namely i from the discussion above. More precisely, given any field K, we have:

$$\mathrm{Hom}(\mathbb{Q}, K) = \begin{cases} \{i\} & \mathrm{Char}(K) = 0, \\ \emptyset & \mathrm{Char}\, K \neq 0. \end{cases} \qquad \mathrm{Hom}(\mathbb{F}_p, K) = \begin{cases} \{i\} & \mathrm{Char}(K) = p, \\ \emptyset & \mathrm{Char}\, K \neq p. \end{cases}$$

(24.3) Field extensions.– Let K and L be two fields. Recall (Lemma 24.1) that either there are no homomorphisms $K \to L$, or there is an injective homomorphism $K \hookrightarrow L$. Therefore, a necessary condition for the existence of a homomorphism $K \to L$ is that $\mathrm{Char}(K) = \mathrm{Char}(L)$. If such a homomorphism exists, and is clear from the context, we will simply write $K \subset L$, and refer to it as *K is a subfield of L*.

Definition. Assume $K \subset L$ are two fields. Then, L is called an *extension* of K, also denoted by L/K. Degree of the extension L/K, denoted by $[L : K]$, is defined to be the dimension of L, viewed as a K–vector space.

$$\boxed{[L : K] = \dim_K(L)}$$

If $[L : K] < \infty$, we say L is a *finite extension* of K.

Example. Any field of characteristic 0 is an extension of $\mathbb{Q}$. A field of characteristic p is an extension of $\mathbb{F}_p$. The field of complex number $\mathbb{C}$ is a degree 2 extension of $\mathbb{R}$.

(24.4) Adjoining elements.– Let L/K be a field extension. Given a set of element $\{\alpha_i\}_{i\in I} \subset L$, let $K(\alpha_i : i \in I)$ denote the smallest subfield of L containing K and $\{\alpha_i : i \in I\}$. We say $K(\alpha_i : i \in I)$ is *a subextension of L/K obtained by adjoining elements $\{\alpha_i\}$ to K.*

Proof of existence. Consider the set $\mathcal{F}$ of all subfields of L which contain K and the set of elements $\{\alpha_i\}$. This set is non–empty, since $L \in \mathcal{F}$. Moreover, it is easy to see that an arbitrary intersection of subfields is again a subfield, proving that

$$K(\alpha_i : i \in I) = \bigcap_{L' \in \mathcal{F}} L'.$$

A word on notations. $K[\alpha_i : i \in I]$ denotes the smallest K–subalgebra of L, and is in general different from $K(\alpha_i : i \in I)$, as we will see below. A (commutative) K–algebra is any commutative ring which contains K as a subring. A typical element of $K[\alpha_i : i \in I] \subset L$ is thus a polynomial in $\{\alpha_i\}_{i\in I}$ with coefficients from K.

The following proposition will be useful in studying infinite extensions.

Proposition. *Let L/K be a field extension and $\{\alpha_i\}_{i\in I} \subset L$. Consider the right directed partially ordered set $\mathcal{I}$:*

$$\mathcal{I} = \{J \subset I : J \text{ is finite}\},$$

ordered by inclusion. For each $J \in \mathcal{I}$, let $K(J)$ denote the subextension of L/K obtained by adjoining $\{\alpha_j\}_{j\in J}$.

$$K(J) = K(\alpha_j : j \in J) \subset L.$$

Then, $\{K(J)\}_{J\in\mathcal{I}}$ is a direct system of subextensions of L/K, and

$$\boxed{K(\alpha_i : i \in I) = \varinjlim_{J\in\mathcal{I}} K(J) = \bigcup_{J\in\mathcal{I}} K(J)}$$

Proof. Let $\widetilde{K}$ denote the union $\bigcup_{J\in\mathcal{I}} K(J)$. We begin by showing that $\widetilde{K} \subset L$ is a subfield. It is clear that $\widetilde{K}$ contains 0 and 1. Given two elements $a, b \in \widetilde{K}$, there is some $J \in \mathcal{I}$ such that $a, b \in K(J)$. Therefore, $a + b, ab \in K(J) \subset \widetilde{K}$. Moreover, if $a \in \widetilde{K}$ is non–zero, then $a \in K(J)$ for some J and $a^{-1} \in K(J) \subset \widetilde{K}$. This finishes the proof that $\widetilde{K}$ is a field.

As $K \subset \widetilde{K}$ and $\alpha_i \in \widetilde{K}$ for every $i \in I$, we conclude that $K(\alpha_i : i \in I) \subset \widetilde{K}$. Moreover, for every $J \in \mathcal{I}$, $K(J) \subset K(\alpha_i : i \in I)$ which establishes the reverse inclusion and completes the proof. □

(24.5) Algebraic vs transcendental elements.– Let L/K be a field extension and let $\alpha \in L$. There are two possibilities for the set of elements $\{1, \alpha, \alpha^2, \ldots\}$:

- There exists an $N \in \mathbb{Z}_{\geq 0}$ such that the set $\{1, \alpha, \ldots, \alpha^{N+1}\}$ is linearly dependent over K.
- For every $N \in \mathbb{Z}_{\geq 0}$, the set $\{1, \alpha, \ldots, \alpha^{N+1}\}$ is linearly independent over K.

In the first case, we say α is *algebraic* over K, while in the second *transcendental*. Another useful way to think about this, is to consider the ring homomorphism called *evaluation at* α.

$$\mathrm{ev}_\alpha : K[x] \to L, \qquad \mathrm{ev}_\alpha(f(x)) = f(\alpha).$$

The following statement is clear from the definitions.

$$\boxed{\alpha \in L \text{ is transcendental if, and only if } \mathrm{ev}_\alpha \text{ is injective}}$$

Remark. Thus, $\alpha \in L$ is transcendental over $K \iff K[\alpha] \cong K[x]$, which is not a field. This is further equivalent to $K[\alpha] \subsetneq K(\alpha)$. For instance, we know π is transcendental over $\mathbb{Q}$, which implies $\mathbb{Q}[\pi] \subsetneq \mathbb{Q}(\pi)$. The former being the set of all real numbers which are polynomials in π, with coefficients from $\mathbb{Q}$, while the latter rational expressions. Thus, algebraically speaking, there is no conceptual difference between a transcendental element, and a formal variable.

Definition. Let L/K be a field extension, and let $\alpha \in L$ be an element which is *algebraic* over K. The *minimal polynomial* of α, denoted by $\mathsf{m}_\alpha(x) \in K[x]$ is the unique monic polynomial such that $\mathrm{Ker}(\mathrm{ev}_\alpha) = (\mathsf{m}_\alpha(x))$. Note that since ev_α induces an injective ring homomorphism $\mathrm{ev}_\alpha : K[x]/(\mathsf{m}_\alpha(x)) \hookrightarrow L$, the ring $K[x]/(\mathsf{m}_\alpha(x))$ has to be an integral domain, proving that $\mathsf{m}_\alpha(x)$ must be an irreducible polynomial.

Proposition. *Let L/K be a field extension, and $\alpha \in L$ be algebraic over K. Then $K(\alpha) = K[\alpha]$ is a finite extension of K, with*

$$\boxed{[K(\alpha) : K] = \deg(\mathsf{m}_\alpha(x))}$$

Proof. We begin by proving that $K[\alpha] = K(\alpha)$. Note that $\mathrm{ev}_\alpha : K[x]/(\mathsf{m}_\alpha(x)) \xrightarrow{\sim} K[\alpha] \subset L$. The former is a finite–dimensional integral domain, hence a field. This proves that $K[\alpha]$ is a field, and clearly the smallest one containing K and α, so $K[\alpha] = K(\alpha)$.

To recall the proof of *finite–dimensional integral domains are fields*, let A be a commutative algebra over K, which is finite–dimensional as a K–vector space. Assume that A is an integral domain. Then, given any $0 \neq a \in A$, the operation of left multiplication $\mu_a : A \to A$ is an injective K–linear map, hence surjective by dimension reasons. So, there must be $b \in A$ such that $ab = \mu_a(b) = 1$.

Now assume $\mathsf{m}_\alpha(x) = x^n - \sum_{j=0}^{n-1} a_j x^j$, where $a_0, \ldots, a_{n-1} \in K$. We claim that $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a basis of $K[\alpha]$ as a K–vector space.

Span. Note that we have (in L):

$$\alpha^n = \sum_{j=0}^{n-1} a_j \alpha^j.$$

We claim that for every $\ell \in \mathbb{Z}_{\geq 0}$, $\alpha^{n+\ell}$ can be written as a linear combination of $\{1, \alpha, \ldots, \alpha^{n-1}\}$. It is true for $\ell = 0$ by the equation given above. Assuming its validity for $\ell \in \mathbb{Z}_{\geq 1}$, that is,

$$\alpha^{n+\ell} = \sum_{j=0}^{n-1} c_j \alpha^j.$$

Multiply both sides by α to get:

$$\alpha^{n+\ell+1} = \sum_{j=0}^{n-2} c_j \alpha^{j+1} + c_{n-1}\alpha^n = \sum_{j=0}^{n-2} c_j \alpha^{j+1} + \sum_{i=0}^{n-1} a_i \alpha^i$$

which proves that $\{1, \alpha, \ldots, \alpha^{n-1}\}$ spans $K[\alpha]$.

Linear independence. If the set $\{1, \alpha, \ldots, \alpha^{n-1}\}$ were linearly dependent, we will have a (non–zero) polynomial of degree $\leq n-1$, say $g(x) \in K[x]$, such that $g(\alpha) = 0$. That is, $g(x) \in \mathrm{Ker}(\mathrm{ev}_\alpha) = (\mathsf{m}_\alpha(x))$, proving that $g(x) = \mathsf{m}_\alpha(x)h(x)$ for some $h(x)$. But $\deg(g) < \deg(\mathsf{m}_\alpha(x))$, which is absurd.

Thus we conclude that $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a basis of $K(\alpha) \cong K[\alpha] \cong K[x]/(\mathsf{m}_\alpha(x))$ as a K–vector space. This proves the proposition. □