23. Main theorem

We have developed all the ideas we need. We now place them together, in an intellectual jigsaw puzzle.

(23.1) Theorem: Let $f(X) \in F[X]$ be solvable by radicals over F. Let E be the splitting field of f(X) over F. Then G(E/F) is a solvable group.

Remark: Actually, we are only stating half of the theorem, for in fact, the converse is also true. (We will not deal with the converse in these notes.) In full form, the theorem says that f(X) is solvable by radicals over F if and only if G(E/F) is a solvable group. This beautiful relationship between polynomials and groups demonstrates the awesome power of mathematics to find and exploit subtle connections between seemingly disparate ideas.

Proof: Since f(X) is solvable by radicals over F, there is, by Theorem (13.1), a root tower $F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \ldots \subseteq F_n$ such that $E \subseteq F_n$. By Theorem (22.2), there is a field L with $F_n \subseteq L$, L/F Galois, and G(L/F) solvable. Note that $E \subseteq F_n \subseteq L$. Thus, we have $F \subseteq E \subseteq L$, with both E/F and L/F Galois, and G(L/F) solvable. By Theorem (20.5), G(E/F) is solvable.

Suppose that f(X) is a polynomial in F[X] having k distinct roots, and that E is the splitting field of f(X) over F. Then in Theorem (18.5), we saw that G(E/F) can be thought of as a subgroup of S_k in a natural way. We will be particularly interested in the case that G(E/F) is not only a subgroup of S_k, but in fact is all of S_k. The next corollary shows why.

(23.2) Corollary: If the Galois group of f(X) over F equals S_k with $k \geq 5$, then f(X) is not solvable by radicals over F.

Proof: Suppose that the splitting field of f(X) over F is E. Were f(X) solvable by radicals over F, then Theorem (23.1) shows that G(E/F) would be solvable. However, by assumption we have $G(E/F) = S_k$, which we know is not solvable, by Theorem (17.3).

Remark: It can be shown that any subgroup of a solvable group is solvable. Since S_1, S_2, S_3, and S_4 are all solvable, any subgroup of these groups is solvable. Now let f(X) be a polynomial of degree at most four in $\mathbf{Q}[X]$. Then f(X) has at most four roots, and by Theorem (18.5), its Galois group over $\mathbf{Q}$ is a subgroup of one of S_1, S_2, S_3, or S_4, and so is solvable. As the unproven converse of Theorem (23.1) states, this means that f(X) is solvable by radicals. In section 2, we mentioned that in fact it was known how to solve any such polynomial by the middle of the sixteenth century. We will now produce an example of a quintic polynomial which is not solvable by radicals over $\mathbf{Q}$.

(23.3) Theorem: Let $k \geq 5$ be a prime integer, and let $f(X)$ be an irreducible polynomial in $\mathbf{Q}[X]$ with degree k. Suppose that exactly $k - 2$ of the roots of $f(X)$ are real. Then $f(X)$ is not solvable by radicals over $\mathbf{Q}$.

Proof: Let K be the splitting field of $f(X)$ over $\mathbf{Q}$. Let $\alpha_1, \ldots, \alpha_k$ be the roots of $f(X)$. By Theorem (7.10), we know these roots are distinct. Let us also assume that the ordering is such that α_1 and α_2 are not real, while $\alpha_3, \ldots, \alpha_k$ are real. By Theorem (18.5), we know that $G(K/\mathbf{Q})$ is a subgroup of S_k. We will in fact show that $G(K/\mathbf{Q}) = S_k$. By Lemma (18.6), we know that conjugation restricted to K is in $G(K/\mathbf{Q})$, and thinking of $G(K/\mathbf{Q})$ as a subgroup of S_k, that lemma shows that conjugation identifies with the permutation $(1, 2)$ of S_k. Thus, $G(K/\mathbf{Q})$ contains a transposition. Next, pick any integers c and d with $1 \leq c,d \leq k$. Since α_c and α_d are both roots of the irreducible polynomial $f(X)$ in $\mathbf{Q}[X]$, Corollary (12.3) tells us that there is a $\Theta \in G(K/\mathbf{Q})$ with $\Theta(\alpha_d) = \alpha_c$. Thought of as a permutation in S_k, Θ sends d to c. As there is such a Θ for any choice of c and d, Theorem (16.5) tells us that $G(K/\mathbf{Q}) = S_k$, as desired. By Corollary (23.2), $f(X)$ is not solvable by radicals over $\mathbf{Q}$.

We leave as a set of exercises, the proof that $X^5 - 6X + 2$ is not solvable by radicals over $\mathbf{Q}$.

(23.4) Exercises: a) Show that $X^5 - 6X + 2$ is irreducible in $\mathbf{Q}[X]$.
b) Show that exactly 3 of the roots of $X^5 - 6X + 2$ are real.
(Hint: Sketch the graph of this polynomial, and then prove that the sketch is not misleading.)
c) Conclude that $X^5 - 6X + 2$ is not solvable by radicals over $\mathbf{Q}$.

24. Dimension

In this section we introduce a new and very powerful concept, one which is quite useful in actually calculating Galois groups and minimal polynomials. We will describe the useful properties of this concept, and give some examples.

Let $F \subseteq K$ be fields. We will associate to this pair of fields, a number called the dimension of K over F, and denoted $[K : F]$. This number will always be either a positive integer, or infinity. In fact, in all of the cases we are interested in, it will be a positive integer. We will now state a theorem describing the properties of $[K : F]$. We will not prove the various parts of the theorem until later sections.

(24.1) Theorem: i) If α is algebraic over F, and the minimal polynomial of α over F is $g(X)$, then $[F[\alpha] : F] = \deg g(X)$.
ii) If $F \subseteq K \subseteq L$, then $[L : F] = [L : K][K : F]$.
iii) If K/F is Galois, then $[K : F] = |G(K/F)|$ (the size of $G(K/F)$).

Let us give some examples.

Example: Since $\mathbf{C} = \mathbf{R}[i]$, and since the minimal polynomial of i over R is $X^2 + 1$, Theorem (24.1)(i) tells us that $[\mathbf{C} : \mathbf{R}] = 2$.

Example. Since $X^3 - 2$ is the minimal polynomial of $\sqrt[3]{2}$ over $\mathbf{Q}$, Theorem (24.1)(i) tells us that $[\mathbf{Q}[\sqrt[3]{2}] : \mathbf{Q}] = 3$.

Example: Let F be a field. Since the minimal polynomial of 1 over F is $X - 1$, and since $F[1] = F$, Theorem (24.1)(i) tells us that $[F : F] = 1$.

Example: Let K be the splitting field of $X^3 - 1$ over $\mathbf{Q}$, so that $K = \mathbf{Q}[\omega]$, where $\omega = -\frac{1}{2} + (\frac{\sqrt{3}}{2})\, i$ is a primitive cube root of unity. Since the minimal polynomial of ω over $\mathbf{Q}$ is $X^2 + X + 1$, Theorem (24.1)(i) tells us that $[K : \mathbf{Q}] = 2$. By Theorem (24.1)(iii), we see that $|G(K/\mathbf{Q})| = 2$. The agrees with what Exercise (18.4) tells us.

Example. Let K be the splitting field of $X^3 - 2$ over $\mathbf{Q}$. We already saw one way of deducing that $G(K/\mathbf{Q}) = S_3$, using Theorem (18.7). We will now determining that same fact using Theorem (24.1). We know that the roots of $X^3 - 2$ are

$\sqrt[3]{2}$, $\sqrt[3]{2}\,\omega$, and $\sqrt[3]{2}\,\omega^2$, where $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}\,i$, and $\sqrt[3]{2}$ is real. We know that $G(K/\mathbb{Q})$ is a subgroup of S_3, and so to show that $G(K/\mathbb{Q}) = S_3$, it will suffice to show that $|G(K/\mathbb{Q})| = |S_3| = 6$. By Theorem (24.1)(iii), it will suffice to show that $[K : \mathbb{Q}] = 6$. Clearly $K = \mathbb{Q}[\sqrt[3]{2}, \omega]$. Since $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt[3]{2}] \subseteq K$, by Theorem (24.1)(ii) we have $[K : \mathbb{Q}] = [K : \mathbb{Q}[\sqrt[3]{2}]][\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}]$. Now the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ is $X^3 - 2$, so by Theorem (24.1)(i), $[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = 3$. Also, the minimal polynomial of ω over $\mathbb{Q}[\sqrt[3]{2}]$ is $X^2 + X + 1$, (since $\omega \notin \mathbb{Q}[\sqrt[3]{2}]$, because ω is not real). Thus Theorem (24.1)(i) shows that $[K : \mathbb{Q}[\sqrt[3]{2}] = [\mathbb{Q}[\sqrt[3]{2}][\omega] : \mathbb{Q}[\sqrt[3]{2}]] = 2$. It follows that $[K : \mathbb{Q}] = (2)(3) = 6$, as desired.

We can say more about this example. Since $\mathbb{Q} \subseteq \mathbb{Q}[\omega] \subseteq K$, Theorem (24.1)(ii) tells us that $6 = [K : \mathbb{Q}] = [K : \mathbb{Q}[\omega]][\mathbb{Q}[\omega] : \mathbb{Q}]$. Now the minimal polynomial of ω over $\mathbb{Q}$ is $X^2 + X + 1$, so that by Theorem (24.1)(i), $[\mathbb{Q}[\omega] : \mathbb{Q}] = 2$. Therefore, we deduce that $[K : \mathbb{Q}[\omega]] = 3$. Since $K = \mathbb{Q}[\omega][\sqrt[3]{2}]$, by Theorem (24.1)(i) we see that the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}[\omega]$ has degree three. Since $\sqrt[3]{2}$ is a root of $X^3 - 2 \in \mathbb{Q}[\omega][X]$, clearly $X^3 - 2$ is the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}[\omega]$. In particular, this means that $X^3 - 2$ is irreducible in $\mathbb{Q}[\omega][X]$.

(24.2) Exercise: For k = 4, 5, and 6, let K_k be the splitting field of $X^k - 1$ over Q. What is $[K_k : Q]$? What is $G(K_k/Q)$? Also, determine how $X^k - 1$ factors in $Q[X]$.

Remark: Let k be a positive integer, and let $\omega_1, \ldots, \omega_m$ be all of the primitive k-th roots of unity. Also let K be the splitting field of $X^k - 1$ over Q, so that $K = Q[\omega_1]$. A remark at the end of section 21 mentioned that the polynomial $(X - \omega_1)(X - \omega_2) \ldots (X - \omega_m)$ is the minimal polynomial of ω_1 over Q. Since $K = Q[\omega_1]$, it follows that $[K : Q]$ equals the degree of $(X - \omega_1)(X - \omega_2) \ldots (X - \omega_m)$, which obviously equals m, the number of primitive k-th roots of unity. By exercise (9.2), this equals the number of integers n with $0 \leq n \leq k$ and n relatively prime to k. (This last number is called $\varphi(k)$, where φ is the Euler phi-function.)

(24.3) Exercise: Let ω be a primitive cube root of unity, and let γ be a primitive 6-th root of unity. Show that $Q[\omega] = Q[\gamma]$ two ways; first by showing that $Q[\omega] \subseteq Q[\gamma]$ and $Q[\gamma] \subseteq Q[\omega]$, and then by showing $Q[\omega] \subseteq Q[\gamma]$, and $[Q[\gamma] : Q] = [Q[\omega] : Q]$. (Use the previous remark.)

(24.4) Exercises: $X^4 - 2 = (X - \sqrt[4]{2})(X + \sqrt[4]{2})(X - \sqrt[4]{2}\, i)(X + \sqrt[4]{2}\, i)$.

a) Show that $X^4 - 2$ is irreducible in $Q[X]$.

b) What is the minimal polynomial of $\sqrt[4]{2}$ over $Q[\sqrt{2}]$? What is $[Q[\sqrt[4]{2}] : Q[\sqrt{2}]]$?

c) What is the minimal polynomial of $\sqrt[4]{2}$ over $Q[\sqrt[4]{2}\, i]$? What is $[Q[\sqrt[4]{2}, \sqrt[4]{2}\, i] : Q\sqrt[4]{2}\, i]$?

d) What is $[Q[\sqrt[4]{2}, \sqrt[4]{2}\, i] : Q]$?

e) Show that $Q[\sqrt[4]{2}, \sqrt[4]{2}\, i] = Q[i, \sqrt[4]{2}]$, and that this field is the splitting field of $X^4 - 2$ over Q.

f) What is $[Q[i, \sqrt[4]{2}] : Q[i]]$? What is the minimal polynomial of $\sqrt[4]{2}$ over $Q[i]$?

(24.5) Exercise: For $k = 5$ and 6, let K_k be the splitting field of $X^k - 2$ over Q. What is $[K_k : Q]$? What is $G(K_k/Q)$?

(24.6) Exercises: a) Let $f(X) \in Q[X]$, and suppose that the Galois group of $f(X)$ over Q is S_4. Let the roots of $f(X)$ be α_1, α_2, α_3, and α_4. Show that $[Q[\alpha_1] : Q] = 4$, $[Q[\alpha_1, \alpha_2] : Q[\alpha_1]] = 3$, $[Q[\alpha_1, \alpha_2, \alpha_3] : Q[\alpha_1, \alpha_2]] = 2$, and $[Q[\alpha_1, \alpha_2, \alpha_3, \alpha_4] : Q[\alpha_1, \alpha_2, \alpha_3]] = 1$.

b) With notation as in part (a), for each $1 \leq i \leq 4$, show that the minimal polynomial of α_i over $Q[\alpha_1, \ldots, \alpha_{i-1}]$ is $(X - \alpha_i)(X - \alpha_{i+1}) \ldots ((X - \alpha_4)$.

(24.7) Exercise: Derive Theorem (18.7) as a corollary of Theorem (24.1).

25. Dimension II

In this section, we will prove Theorem (24.1)(i) and a special case of Theorem (24.1)(ii). (Part (iii) takes considerably more work, and will be done in the next section.)

Definition: Let $F \subseteq K$ be fields. If $\alpha_1, \ldots, \alpha_n$ are elements in K, then these elements are called a basis of K over F if every element β in K can be written as a unique way as $\beta = a_1\alpha_1 + a_2\alpha_2 + \ldots + a_n\alpha_n$, where the coefficients $a_1, \ldots, a_n$ come from F.

(25.1) Exercise: Show that if $\alpha_1, \ldots, \alpha_n$ are a basis of K over F, then none of the α_i can be zero.

Example: The elements 1 and i together form a basis of $\mathbf{C}$ over $\mathbf{R}$. This simply says that every complex number β can be written in a unique way as $\beta = a(1) + b(i)$, with a and b in $\mathbf{R}$.

Example: The elements $2 + 3i$ and $4 - i$ together form a basis of $\mathbf{C}$ over $\mathbf{R}$. To show this, we must show that any complex number β can be written in a unique way as $\beta = a(2 + 3i) + b(4 - i)$, with a and b in $\mathbf{R}$. For example, suppose that $\beta = -8 + 9i$. Then we want there to be a unique solution (in $\mathbf{R}$) for the equation $a(2 + 3i) + b(4 - i) = -8 + 9i$. Since $a(2 + 3i) + b(4 - i) = (2a + 4b) + (3a - b)i$, we are trying to solve $(2a + 4b) + (3a - b)i = -8 + 9i$. Therefore, we have

$$2a + 4b = -8$$

and $3a - b = 9$.

Solving this simultaneous system of equations shows that $a = 2$ and $b = -3$. This shows that $-8 + 9i = (2)(2 + 3i) + (-3)(4 - i)$, and that no coefficients other than 2 and -3 make this true.

Having just looked at a specific example, let us now work with an arbitrary $\beta \in \mathbf{C}$. Suppose that β is the complex number $c + di$. (Here, c and d are given numbers in $\mathbf{R}$.) Then we want $c + di = \beta = a(2 + 3i) + b(4 - i) = (2a + 4b) + (3a - b)i$. Therefore, we want

$$2a + 4b = c$$

and $3a - b = d$.

Solving this system of simultaneous equations shows that we must have $a = \frac{c + 4d}{14}$ and $b = \frac{3c - 2d}{14}$. Note that a and b are in $\mathbf{R}$, and are the only solution in $\mathbf{R}$ to $\beta = a(2 + 3i) + b(4 - i)$. This shows that a $2 + 3i$ and $4 - i$ are a basis of $\mathbf{C}$ over $\mathbf{R}$.

Example: $5 + 2i$ does not by itself form a basis of $\mathbf{C}$ over $\mathbf{R}$. If it did form a basis, then for any $\beta \in \mathbf{C}$, the equation $\beta = a(5 + 2i)$ would have a unique solution $a \in \mathbf{R}$. However, if we let $\beta = 1 + i$, we see that $1 + i = a(5 + 2i)$ is false for any choice of $a \in \mathbf{R}$. (It is true for some $a \in \mathbf{C}$, but that is not enough. We insist that a be in $\mathbf{R}$.)

Example: $4 - 2i$, $3 + 5i$, and $10 + 8i$ together do not form a basis of C over R. If they did form a basis, then for any $\beta \in \mathbf{C}$, the equation $\beta = a(4 - 2i) + b(3 + 5i) + c(10 + 8i)$ would have a <u>unique</u> solution $a,b,c \in \mathbf{R}$. Now in fact, there will always be a solution $a,b,c \in R$, but the problem is that there will be more than just one solution. For example, if $\beta = 20 + 16i$, then $a = 2$, $b = 4$, $c = 0$ is a solution, but $a = 0$, $b = 0$, $c = 2$ is another solution. This one example is enough to show that $4 - 2i$, $3 + 5i$, and $10 + 8i$ do not form a basis of **C** over **R**.

(25.2) Exercises: a) Show that $5 - 2i$ and $3 + 4i$ together form a basis of **C** over **R**.

b) Show that $10 - 4i$ and $-15 + 6i$ together do <u>not</u> form a basis of **C** over **R**.

c) Show that no one complex number $c + di$ by itself can form a basis of **C** over **R**.

d) Show that if $5 - 4i$, $3 + i$, and $-2 + 7i$ together do <u>not</u> form a basis of **C** over **R**.

Looking at the previous examples and doing the above exercises, you might be tempted to guess that any basis of **C** over **R** must contain exactly 2 elements. That is correct. In fact, we have a general theorem.

(25.3) Theorem: Let $F \subseteq K$ be fields, and suppose that $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots \beta_m$ are both bases of K over F. Then $n = m$. We will not prove this theorem here, as it is really a special case of a basic fact from linear algebra. (Those readers who know linear algebra will see that K can be thought of as a vector space over F, and we are simply saying that any two bases of a given vector space have the same size.)

Definition: Let $F \subseteq K$ be fields, and suppose that there is a basis of K over F consisting of n elements, (here assuming that n is finite). Then we call n the dimension of K over F, writing $[K : F] = n$. We also say that K is n-dimensional over F, or less specifically, K/F is finite.

Example: $[\mathbf{C} : \mathbf{R}] = 2$, since 1, i is a basis of $\mathbf{C}$ over $\mathbf{R}$.

(25.4) Exercise: Explain why we would not be allowed to make this definition until after stating Theorem (25.3).

(25.5) Exercise: Show that if F is any field, then 1 is a basis of F over F, so that $[F : F] = 1$.

Definition: Let $F \subseteq K$ be fields. Suppose that for all finite positive integers n, there is no basis of K over F consisting of n elements. Then we will say that K is infinite dimensional over F (or K/F is infinite), and will say that $[K : F]$ equals infinity.

In our work, we will not need to study infinite dimensional extensions, and so will say little about them. In particular, we will not bother to define what it means to say that an infinite set of elements of K is a basis of K over F. We do mention, by way of example, that $\mathbf{R}$ is infinite dimensional over $\mathbf{Q}$. Thus, no finite set of elements in $\mathbf{R}$ forms a basis of $\mathbf{R}$ over $\mathbf{Q}$. The proof of this fact is a bit challanging. The easiest proof uses the fact (which we will not prove here) that if K is finite dimensional over F, then every element in K is algebraic over F.

We now prove part (i) of Theorem (24.1).

Proof of Theorem (24.1)(i): Let α be algebraic over F, and let g(X) be the minimal polynomial of α over F. Suppose that g(X) has degree n. We must show that $[F[\alpha] : F] = n$. It will suffice to show that $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ is a basis of $F[\alpha]$ over F. This means that we must show that every element of $F[\alpha]$ can be written as a linear combination of $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ (with coefficients in F) in a unique way. However, Theorem (8.7) tells us that this is so.

Next, we prove part (ii) of Theorem (24.1). However, since in our applications we will only be concerned with the case in which $[L : K]$ and $[K : F]$ are finite, we will restrict our proof to that case.

Proof of Theorem (24.1)(ii), in the finite dimensional case: Suppose that $F \subseteq K \subseteq L$ are fields, with $[L : K]$ and $[K : F]$ finite. We must show that $[L : F] = [L : K][K : F]$. Say that $\alpha_1, \ldots, \alpha_n$ is a basis of L over K, and $\beta_1, \ldots, \beta_m$ is a basis of K over F.

We leave it to the reader to show that

$\alpha_1\beta_1, \ldots \alpha_1\beta_m, \alpha_2\beta_1, \ldots, \alpha_2\beta_m, \ldots\ldots\ldots, \alpha_n\beta_1, \ldots, \alpha_n\beta_m$ is a basis of L over F. Since this basis has $nm = [L : K][K : F]$ elements, we are done.

(25.6) Exercise: Fill in the details of the above proof.

26. Dimension III

In this section, we will prove part (iii) of Theorem (24.1). We begin by recalling an basic fact proved in linear algebra.

(26.1) Lemma: Let

$$\begin{aligned} a_{11}X_1 + a_{12}X_2 + \ldots + a_{1k}X_k &= 0 \\ a_{21}X_1 + a_{22}X_2 + \ldots + a_{2k}X_k &= 0 \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot & \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot & \\ a_{m1}X_1 + a_{m2}X_2 + \ldots + a_{mk}X_k &= 0 \end{aligned}$$

be a system of m simultaneous homogeneous linear equations in k unknowns. Suppose that the coefficients a_{ih} all come from some field F. Suppose also that $k > m$. Then there is a nontrivial solution in F. (That is, there is a solution for $X_1, \ldots, X_k$, in which all the values for the X_h come from F, and not all the X_h are zero.)

Suppose that K/F is a Galois extension. Say that $K = F[\alpha_1, \ldots, \alpha_n]$, where $\alpha_1, \ldots, \alpha_n$ are all the roots of the polynomial $f(X) \in F[X]$. The next exercise asks you to show that K/F is finite.

(26.2) Exercise: Show that if K/F is Galois, then [K : F] is finite. (Hint: Make repeated use of Theorem (24.1), parts (i) and (ii).)

Proof of Theorem (24.1)(iii): Suppose that K/F is Galois. By Exercise (26.2), we know that [K : F] is finite. Say [K : F] = n. We must show that $|G(K/F)| = n$. We will first show that $n \geq |G(K/F)|$. We will assume this statement is false, and derive a contradiction. Thus, suppose that $\Theta_1, \ldots, \Theta_{n+1}$ are distinct members of G(K/F). Let $\alpha_1, \ldots, \alpha_n$ be a basis of K over F. Consider the following system of n homogeneous equations with n + 1 unknowns $\beta_1, \ldots, \beta_{n+1}$.

$$\beta_1\Theta_1(\alpha_1) + \ldots + \beta_{n+1}\Theta_{n+1}(\alpha_1) = 0$$

$$\beta_1\Theta_1(\alpha_2) + \ldots + \beta_{n+1}\Theta_{n+1}(\alpha_2) = 0$$

$$\beta_1\Theta_1(\alpha_n) + \ldots + \beta_{n+1}\Theta_{n+1}(\alpha_n) = 0$$

Since we have n+1 unknowns but only n equations, and since all of the coeficients $\Theta_i(\alpha_h)$ come from K, Lemma (26.1) tells us that there is a nontrivial solution in K (i.e., a solution in which all the β_i come from K, but not all the β_i are zero). Therefore, we may now assume that $\beta_1, \ldots, \beta_{n+1}$ are all in K, are not all zero, and make the above system of equations true.

Now consider the function $\beta_1\Theta_1 + \ldots + \beta_{n+1}\Theta_{n+1}$. If this is applied to any α_h, $1 \leq h \leq n$, we get $\beta_1\Theta_1(\alpha_h) + \ldots + \beta_{n+1}\Theta_{n+1}(\alpha_h) = 0$. Now if $\gamma \in F$, then for each Θ_i, $\Theta_i(\gamma\alpha_h) = \Theta_i(\gamma)\Theta_i(\alpha_h) = \gamma\Theta_i(\alpha_h)$, so that $\beta_1\Theta_1(\gamma\alpha_h) + \ldots + \beta_{n+1}\Theta_{n+1}(\gamma\alpha_h) = \gamma(\beta_1\Theta_1(\alpha_h) + \ldots + \beta_{n+1}\Theta_{n+1}(\alpha_h)) = 0$. It follows that if we apply this function to any linear combination of the α_h's (with coefficients in F), the result will be zero. However, everything in K can be written as such a linear combination. Thus, the function $\beta_1\Theta_1 + \ldots + \beta_{n+1}\Theta_{n+1}$ is indentically zero on all of K.

We have just seen that it is possible to express the zero function on K in the form $\sigma_1\phi_1 + \ldots + \sigma_r\phi_r$ with the ϕ_i's distinct elements in G(K/F), the σ_i's in K, and not all the σ_i's equal to zero. Let us suppose that $\sigma_1\phi_1 + \ldots + \sigma_r\phi_r = 0$ is such an expression with r as small as possible. (Note that this means each σ_i is nonzero, or else the i-th term could be deleted, giving a smaller sum. Note also that r must be at least 2, since otherwise $\sigma_1\phi_1 = 0$ and $\sigma_1 \neq 0$ would imply that ϕ_1 was indentically zero, which is false.) Since $\phi_1 \neq \phi_2$, there is some $\omega \in K$ with $\phi_1(\omega) \neq \phi_2(\omega)$. Let ρ be any element of K.

We know that $\sigma_1\phi_1(\rho) + \sigma_2\phi_2(\rho) + \ldots + \sigma_r\phi_r(\rho) = 0$. Multiplying through by $\phi_1(\omega)$, we get

$$(*)\ \sigma_1\phi_1(\omega)\phi_1(\rho) + \sigma_2\phi_1(\omega)\phi_2(\rho) + \ldots + \sigma_r\phi_1(\omega)\phi_r(\rho) = 0.$$

Now we also know that $\sigma_1\phi_1(\omega\rho) + \sigma_2\phi_2(\omega\rho) + \ldots + \sigma_r\phi_r(\omega\rho) = 0$. Since $\phi_i(\omega\rho) = \phi_i(\omega)\phi_i(\rho)$, we get
$\sigma_1\phi_1(\omega)\phi_1(\rho) + \sigma_2\phi_2(\omega)\phi_2(\rho) + \ldots + \sigma_r\phi_r(\omega)\phi_r(\rho) = 0$.
If we subtract this last equation from equation $(*)$, we get
$\sigma_2(\phi_1(\omega) - \phi_2(\omega))\phi_2(\rho) + \ldots + \sigma_r(\phi_1(\omega) - \phi_r(\omega))\phi_r(\rho) = 0$.
This is true for any $\rho \in K$, and so the function
$\sigma_2(\phi_1(\omega) - \phi_2(\omega))\phi_2 + \ldots + \sigma_r(\phi_1(\omega) - \phi_r(\omega))\phi_r$ is identically zero on K. Since $\sigma_2 \neq 0$, and $\phi_1(\omega) - \phi_2(\omega) \neq 0$, the first coefficient is nonzero. As there are r - 1 terms in this sum, the minimality of r shows that we have a contradiction. This completes the argument that $[K : F] = n \geq |G(K/F)|$.

We will now show that $[K : F] = n \leq |G(K/F)|$. In fact, since it will be useful later, we will prove a bit more. Namely, if K/F is finite, and if $H < G(K/F)$ with $F(H) = F$, then we will show that $[K : F] \leq |H|$. Since our K/F is finite, and since $F(G(K/F)) = F$ (by Theorem (21.2), our desired goal follows from this fact. Therefore, we now turn to proving the next lemma.

(26.3) Lemma: Let K/F be finite, and let $H < G(K/F)$ with $F(H) = F$. Then $[K : F] \leq |H|$.

Proof: Suppose not (and we will derive a contradiction). Thus, suppose that $H = \{\Theta_1, \ldots, \Theta_m\}$ with $m < n = [K : F]$. Say that $\alpha_1, \ldots, \alpha_n$ is a basis of K over F. Consider the following system of m homogeneous equations in n unknowns $b_1, \ldots, b_n$.

$$b_1\Theta_1(\alpha_1) + \ldots + b_n\Theta_1(\alpha_n) = 0$$

$$b_1\Theta_2(\alpha_1) + \ldots + b_n\Theta_2(\alpha_n) = 0$$

$$\vdots$$

$$b_1\Theta_m(\alpha_1) + \ldots + b_n\Theta_m(\alpha_n) = 0$$

Since the coefficients $\Theta_i(\alpha_h)$ come from K, and since there are more unknowns then equations, Lemma (26.1) tells us we can find a nontrivial solution $b_1, \ldots, b_n$ in K. Of all the nontrivial solutions in K, let us suppose that $b_1, \ldots, b_n$ is a nontrivial solution in which a maximal number of the b_i are zero. By renumbering if necessary, we can assume that $b_1, \ldots, b_s$ are nonzero while $b_{s+1}, \ldots, b_n$ are zero. (Note that $s \geq 2$, since if $s = 1$, we would have $\Theta_1(\alpha_1) = 0$, so that $\alpha_1 = 0$, which contradicts Exercise (25.1). Also, if $b_1', \ldots, b_n'$ is another nontrivial solution in K, then at least s of the b_i' are nonzero). Since dividing everything by b_1 does no harm, we may also assume that $b_1 = 1$. Ignoring zero terms, the above system becomes

$$b_1\Theta_1(\alpha_1) + \ldots + b_s\Theta_1(\alpha_s) = 0$$

$$b_1\Theta_2(\alpha_1) + \ldots + b_s\Theta_2(\alpha_s) = 0$$

$$\vdots$$

$$b_1\Theta_m(\alpha_1) + \ldots + b_s\Theta_m(\alpha_s) = 0.$$

For any $\Theta_i \in \{\Theta_1, \ldots, \Theta_m\} = H$, $b_1\Theta_i(\alpha_1) + \ldots + b_s\Theta_i(\alpha_s) = 0$. If we pick any $\Theta \in H$ and apply Θ to this equation, we get $\Theta(b_1)\Theta(\Theta_i(\alpha_1)) + \ldots + \Theta(b_s)\Theta(\Theta_i(\alpha_s)) = 0$. However, (as explained in the paragraph preceding (21.4)), as Θ_i varies through $\{\Theta_1, \ldots, \Theta_m\} = H$, so does $\Theta\Theta_i$. Therefore, we see that $\Theta(b_1)$, $\Theta(b_2)$, ..., $\Theta(b_s)$ is another solution to our previous system of equations. That is, we have (after rearranging the rows)

$$\Theta(b_1)\Theta_1(\alpha_1) + \ldots + \Theta(b_s)\Theta_1(\alpha_s) = 0$$

$$\Theta(b_1)\Theta_2(\alpha_1) + \ldots + \Theta(b_s)\Theta_2(\alpha_s) = 0$$

$$\vdots \qquad\qquad \vdots$$

$$\Theta(b_1)\Theta_m(\alpha_1) + \ldots + \Theta(b_s)\Theta_m(\alpha_s) = 0.$$

If we subtract this system from the previous system, we get

$$(b_1 - \Theta(b_1))\Theta_1(\alpha_1) + \ldots + (b_s - \Theta(b_s))\Theta_1(\alpha_s) = 0$$

$$(b_1 - \Theta(b_1))\Theta_2(\alpha_1) + \ldots + (b_s - \Theta(b_s))\Theta_2(\alpha_s) = 0$$

$$\vdots$$

$$(b_1 - \Theta(b_1))\Theta_m(\alpha_1) + \ldots + (b_s - \Theta(b_s))\Theta_m(s_n) = 0.$$

However, since $b_1 = 1$, $\Theta(b_1) = 1$, and so this gives a solution $b_1', \ldots, b_n'$ to our original system with $b_1' = 0$, $b_2' = b_2 - \Theta(b_2)$, $\ldots b_s' = b_s - \Theta(b_s)$, $b_{s+1}' = 0, \ldots b_n' = 0$. In this solution, less then s of the coefficients are nonzero. By our choice of s this cannot happen in a nontrivial solution. Therefore, we must have the trivial solution. That is, all the $b_k' = 0$. In particular, we have $\Theta(b_2) = b_2, \ldots \Theta(b_s) = b_s$. This argument holds for all $\Theta \in G(K/F)$. Thus each of $b_2, \ldots, b_s$ is in $F(H) = F$. Of course $b_1 = 1 \in F$, and $b_{s+1}, \ldots, b_n$ are all zero, and so in F. That is, all of the b_k are in F. Howver, we already have $b_1\Theta_i(\alpha_1) + \ldots + b_n\Theta_i(\alpha_n) = 0$ for each $\Theta_i \in G(K/F)$. Since one of those Θ_i is just the identity automorphism, we get $b_1\alpha_1 + \ldots + b_n\alpha_n = 0$. Since all the b_k are in F but not all the b_k are zero, we have contradicted that $\alpha_1, \ldots, \alpha_n$ are a basis of K over F, (since $0\alpha_1 + \ldots + 0\alpha_n = 0$ is a different way of writting 0 as a linear combination of $\alpha_1, \ldots, \alpha_n$).

27. Fixed fields II

We now give the converse to the theorem in the section fixed fields I.

(27.1) Theorem: Let $F \subseteq E$ be fields, where $E = F[\gamma_1, \ldots, \gamma_k]$ with each γ_i algebraic over F. Then $F(G(E/F)) = F$ if and only if E/F is Galois.

Proof: One direction is by Theorem (21.2). Thus, suppose that $F(G(E/F)) = F$. Let $g_i(X)$ be the minimal polynomial of γ_i over F. We will show that E is the splitting field of $p(X) = g_1(X) \ldots g_k(X)$ over F, which will show that E/F is Galois. Since $\gamma_1, \ldots, \gamma_k$ are roots of p(X), and since we already have $E = F[\gamma_1, \ldots, \gamma_k]$, in order to show that E is the splitting field of p(X) over F, it will clearly suffice to show that every root of p(X) is in E. Therefore, we need only show that any root of any $g_i(X)$, $i = 1, \ldots, k$, is in E. Since we already know that each $g_i(X)$ has at least one root in E, namely γ_i, what we need is provided by the following lemma.

(27.2) Lemma: Suppose that $F(G(E/F)) = F$, and let g(X) be irreducible in F[X]. If any root of g(X) is in E, then all the roots of g(X) are in E.

Proof: Let $\rho \in E$ be a root of $g(X)$. Let $\Theta \in G(E/F)$. Since $g(X) \in F[X]$, we see that $\Theta(g(X)) = g(X)$. Thus $\Theta(\rho)$ is also a root of $g(X)$. Thus we see that the set $\{\Theta(\rho) \mid \Theta \in G(E/F)\}$ is finite, since it consists of roots of $g(X)$. Let $\{\Theta(\rho) \mid \Theta \in G(E/F)\} = \{\rho_1, \ldots, \rho_m\}$. Note that if $\Lambda \in G(E/F)$, then $\{\Lambda(\rho_1), \ldots, \Lambda(\rho_m)\} = \{\Lambda(\Theta(\rho)) \mid \Theta \in G(E/F)\}$. However, as Θ varies throughout $G(E/F)$, so does $\Lambda\Theta$, and therefore, this last set is just $\{\Theta(\rho) \mid \Theta \in G(E/F)\} = \{\rho_1, \ldots, \rho_m\}$. That is to say, $\{\Lambda(\rho_1), \ldots, \Lambda(\rho_m)\} = \{\rho_1, \ldots, \rho_m\}$. Now let $q(X) = (X - \rho_1) \ldots (X - \rho_m)$. Then for any $\Lambda \in G(E/F)$, $\Lambda(q(X)) = (X - \Lambda(\rho_1)) \ldots (X - \Lambda(\rho_m)) = (X - \rho_1) \ldots (X - \rho_m) = q(X)$. Thus, we see that Λ fixes $q(X)$, and so fixes each coefficient of $q(X)$. As this is true for all $\Lambda \in G(E/F)$, and as $F(G(E/F)) = F$, we see that $q(X) \in F[X]$. As noted earlier, each ρ_i is a root of $g(X)$, and so deg $q(X) = m$ is equal to or less than the number of roots of $g(X)$, which in turn equals deg $g(X)$ (since $g(X)$ is irreducible). That is, deg $q(X) \leq$ deg $g(X)$. Furthermore, since $g(X)$ is irreducible in $F[X]$, and has ρ_1 for a root, $g(X)$ is the minimal polynomial of ρ_1 over F, by Exercise (8.2)(d). However, ρ_1 is a root of $q(X)$, and so $g(X)$ must divide $q(X)$, by Exercise (8.2)(c). Since deg $q(X) \leq$ deg $g(X)$, we must have that $q(X) = g(X)$. Thus the roots of $g(X)$ are just $\rho_1, \ldots, \rho_m$, and by construction, these are all in E. This completes the proof.

Remark: Some people take $F(G(K/F)) = F$ to be the definition of what it means to say K/F is Galois.

(27.3) Exercise: Let $E = F[\gamma_1, \ldots, \gamma_m]$ with each γ_i algebraic over F. Show that the following two statements are equivalent.

a) E/F is Galois.

b) For any irreducible $g(X) \in F[X]$, if g(X) has any root in E, then all of the roots of g(X) are in E.

28. Fundamental Theorem

Let K/F be Galois, and consider the two sets $\{L \mid L \text{ is a field with } F \subseteq L \subseteq K\}$ and $\{H \mid H < G(K/F)\}$. Given a field L in the first set, we know by exercise (18.2) that $H = G(K/L)$ is in the second set. Furthermore, given any H in the second set, we easily see that $L = F(H)$ is in the first set. We will now show that these two operations, sending L to G(K/L), and sending H to F(H) are the inverses of each other.

(28.1) Lemma: Let K/F be Galois.

a) For any field L with $F \subseteq L \subseteq K$, $F(G(K/L)) = L$.

b) For any subgroup H of G(K/F), $G(K/F(H)) = H$.

Proof: a) Since K/F is Galois, Exercise (12.1)(a) tells us that K/L is also Galois. Thus Theorem (21.2) tells us that (a) is true.

b) We have $H < G(K/F)$, and want $G(K/F(H)) = H$. Note that the definitions of F(H) and G(K/F(H)) show that $H < G(K/F(H))$. Since

$F \subseteq F(H) \subseteq K$, and K/F is Galois, by Exercise (12.1)(a) we have $K/F(H)$ Galois. We apply Lemma (26.3) to $K/F(H)$, and the subgroup H of $G(K/F(H))$. That lemma tells us that $[K : F(H)] \leq |H|$. Also, Theorem (24.1)(iii) tells us that $[K : F(H)] = |G(K/F(H))|$. Thus, $|G(K/F(H))| \leq |H|$. However, as H is a subgroup of $G(K/F(H))$, and as these two groups have the same (finite) size, they must be equal.

(28.2) Theorem: Let K/F be Galois. There is a one-to-one correspondence between $\{L \mid L$ is a field with $F \subseteq L \subseteq K\}$ and $\{H \mid H < G(K/F)\}$, given by $L \rightarrow G(K/L)$.

Proof: We first show that the operation $L \rightarrow G(K/L)$ is one-to-one. Thus, suppose that L_1 and L_2 are both field between F and K, and that $G(K/L_1) = G(K/L_2)$. We must show that $L_1 = L_2$. However, by Lemma (28.1)(a), $L_1 = F(G(K/L_1)) = F(G(K/L_2)) = L_2$, as desired. Next, we must show that the operation $L \rightarrow G(K/L)$ is onto the set $\{H \mid H < G(K/L)\}$. Therefore, let H be a subgroup of $G(K/L)$. We must find a field L between F and K such that $L \rightarrow H$. In other words, we need L such that $L \rightarrow G(K/L) = H$. We simply let L be $F(H)$. By Lemma (28.1)(b), $G(K/F(H)) = H$, and so we are done.

Theorem (28.2) is part of what is called the Fundamental Theorem of Galois Theory. This famous theorem summarizes the heart of Galois' beautiful work. Essentially, it says that information concerning a field L between F and K (with K/F

Galois), coresponds to information concerning G(K/L). For instance, since K/L is automatically Galois (by Exercise (12.1)(a)), we have already seen that $[K : L] = |G(K/L)|$, illustrating that information about L corresponds to information about G(K/L).

Remark: For the sake of reader's familiar with group theory, we will now mention another part of the Fundamental Theorem. If $F \subseteq L \subseteq K$, with K/F Galois, then we know that K/L is Galois. However, it may or may not happen that L/F is Galois. Part of the Fundamental Theorem says that L/F is Galois if and only if G(K/L) is a normal subgroup of G(K/F), and in that case, G(L/F) is isomorphic to the quotient group of G(K/F) modulo G(K/L).

The brilliance of Galois' work was in showing that information about field extensions can often be made to correspond to information about groups. The usefulness of this was amply illustrated when we employed it to produce an example of a polynomial which was not solvable by radicals over $\mathbf{Q}$. We now present a much smaller but still pleasant use of this technique, called the Theorem of the Primitive Element.

(28.3) Theorem: (E. Artin) Let $L = F[\alpha_1, \ldots, \alpha_n]$, where $\alpha_1, \ldots, \alpha_n$ are all algebraic over F. Then there is an element $\gamma \in K$ such that $L = F[\gamma]$.

Proof: Let $f_i(X)$ be the minimal polynomial of α_i over F. Let K be the splitting field of the product $f_1(X)f_2(X) \ldots f_n(X)$ over F. Clearly K/F is Galois, and $F \subseteq L \subseteq K$ (since each α_i is in K). By Theorem (28.2), there is a one-to-one correspondence between the set of all fields between F and K, and the set of all subsets of G(K/F). However, as G(K/F) is finite, that group can only have finitely many subgroups. Thus, there are only finitely many fields between F and K.

Since $L = F[\alpha_1, \ldots, \alpha_n]$, we see that L can be generated over F by n elements. Possibly a smaller set of elements might also generate L over F. Let us assume that the smallest number of elements needed to generate L over F is m. We will show that $m = 1$ (thus proving the theorem). We will proceed by contradiction, assuming that $m \geq 2$. Therefore, assume that $\beta_1, \ldots, \beta_m$ (with $m \geq 2$) are elements in L such that $L = F[\beta_1, \ldots, \beta_m]$. We now consider the field $F[\beta_1, \beta_2]$. Also, for each element $a \in F$, let $L_a = F[\beta_1 + a\beta_2] \subseteq F[\beta_1, \beta_2] \subseteq L \subseteq K$. Thus, $F \subseteq L_a \subseteq K$. However, in the previous paragraph, we saw that there are only finitely many fields between F and K. Thus, there are only finitely many choices for L_a. On the other hand, since F contains infinitely many elements, there are infinitely many choices for a. This shows that there are two distinct elements $b \neq c$ in F, such that $L_b = L_c$. In particular, we have $\beta_1 + b\beta_2 \in L_b = L_c$. Since also $\beta_1 + c\beta_2 \in L_c$, we see that L_c contains $(\beta_1 + b\beta_2) - (\beta_1 + c\beta_2) = (b - c)\beta_2$. As $b - c \neq 0$, we may divide by it, and so we see that $\beta_2 \in L_c$. Since also

$\beta_1 + c\beta_2 \in L_c$, and $c \in F \in L_c$, we see that L_c contains β_1. That is, L_c contains both β_1 and β_2, and so contains $F[\beta_1, \beta_2]$. However, we already have $L_c \subseteq F[\beta_1, \beta_2]$, and so we have $F[\beta_1, \beta_2] = L_c = F[\beta_1 + c\beta_2]$. Now we have $L = F[\beta_1, \beta_2, \beta_3, \ldots, \beta_m] = F[\beta_1 + c\beta_2, \beta_3, \ldots, \beta_m]$. That is, we have generated L over F using only m - 1 elements. This is a contradiction, and so completes the proof.

This completes our journey. Although it has only looked at Galois theory in the special setting of fields contained within the complex numbers, nonetheless, we have seen much of the beauty of this magnificent subject. I hope the reader is inspired to learn more about the many applications of Galois theory.