GALOIS THEORY

M. PAVAMAN MURTHY

K.G. RAMANATHAN C. S. SESHADRI

U. SHUKLA R. SRIDHARAN

Tata Institute of Fundamental Research, Bombay

School of Mathematics

Tata Institute of Fundamental Research, Bombay

1965

All communications pertaining to this series should be addressed to:

School of Mathematics
Tata Institute of Fundamental Research
Bombay 5, India.

Edited and published by K. Chandrasekharan for the Tata Institute of Fundamental Research, Bombay, and printed by R. Subbu at the Commercial Printing Press Limited, 34–38 Bank Street, Fort, Bombay, India.

EDITORIAL NOTE

This little book on Galois Theory is the third in the series of Mathematical pamphlets started in 1963. It represents a revised version of the notes of lectures given by M. Pavaman Murthy, K.G. Ramanathan, C.S. Seshadri, U. Shukla and R. Sridharan, over 4 weeks in the summer of 1964, to an audience consisting of students and teachers, some of them new to algebra. The course evoked enthusiasm as well as interest. Special thanks are due to the authors, and to Professor M.S. Narasimhan who, as Chairman of the Committee on the Summer School, was responsible for organizing it. I owe personal thanks to Professor Raghavan Narasimhan who has done the actual editing of the work.

K. Chandrasekharan

PREFACE

This pamphlet contains the notes of lectures given at a Summer School on Galois Theory at the Tata Institute of Fundamental research in 1964. The audience consisted of teachers and students from Indian Universities who desired to have a general knowledge of the subject. The speakers were M. Pavaman Murthy, K.G. Ramanathan, C.S. Seshadri, U. Shukla and R. Sridharan.

The rudiments of set theory are assumed. Chapters I and II deal with topics concerning groups, rings and vector spaces to the extent necessary for the study of Galois Theory. In Chapter III, field extensions are studied in some detail; the chapter ends with the theorem on the simplicity of a finite separable extension. The fundamental theorem of Galois Theory is proved in Chapter IV. Chapter V deals with applications of Galois Theory to the solution of algebraic equations and geometrical constructions.

Contents

Chapter 1

Groups

1.1 Groups and Homomorphisms

Definition 1.1 A group is a pair (G, ψ), where G is a set and $\psi: G \times G \to G$ is a map ($\psi(x, y)$ being denoted by xy) satisfying.

(a) $(xy)z = x(yz)$, $\forall\, x, y, z \in G$ (associativity)

(b) there exists an element $e \in G$ such that $ex = xe = x$, $\forall\, x \in G$, and

(c) if $x \in G$ there exists an element $x' \in G$ such that

$$x'x = xx' = e.$$

Remark 1.2 The map ψ is called the group operation. We denote the group simply by G when the group operation is clear from the context.

Remark 1.3 The element e is unique. For, if $e_1 \in G$ such that $e_1 x = xe_1 = x$, $\forall\, x \in G$, we have, in particular, $e = ee_1 = e_1$. The element e is called the identity element of G.

Remark 1.4 For $x \in G$ the element x' is unique. For, if $x'' \in G$ such that $x''x = xx'' = e$, then we have

$$x'' = x''e = x''(xx') = (x''x)x' = ex' = x'.$$

The element x' is called the inverse of x and is denoted by x^{-1}.

Remark 1.5 In view of associativity, we define

$$xyz = (xy)z = x(yz), \text{ where } x, y, z \in G.$$

More generally, the product $x_1 x_2 \ldots, x_n$ is well-defined, where $x_1, x_2, \ldots, x_n \in G$ (proof by induction). For $x \in G$ we set

(i) $x^n = xx \ldots x(n \text{ factors})$, for $n > 0$;

(ii) $x^0 = e$;

(iii) $x^n = (x^{-1})^{-n}$, for $n < 0$

A group G is called *abelian* or *commutative*, if

$$xy = yx, \ \forall\ x, y \in G$$

For an abelian group we sometimes write $\psi(x, y) = x + y$ and call the group operation *addition* in the group. We then denote the identity by 0 and the inverse of an element x by $-x$. Also we write

$$\begin{aligned} nx &= x + x \cdots + x \ (n \text{ terms}), \text{ for } n > 0 \\ 0x &= 0 \\ nx &= (-n)(-x), \text{ for } n < 0. \end{aligned}$$

A group G is called a *finite group* if the set G is finite. The number of elements in a finite group is called its *order*.

Example 1.6 The set $\mathbf{Z}$ (resp. $\mathbf{Q}, \mathbf{R}, \mathbf{C}$) is an abelian group under the "usual" addition.

Example 1.7 The set $\mathbf{Q}^*$ (resp. $\mathbf{R}^*$, $\mathbf{C}^*$) of non-zero rational (resp.real, complex) numbers is an abelian group under "usual" multiplication.

Example 1.8 The set $\mathbf{Z}/(m)$ of residue classes modulo m, where m is an integer, is a group under addition given by $\bar{r} + \bar{s} = \overline{r + s}$ where $\bar{r} + \bar{s} \in \mathbf{Z}/(m)$.

Example 1.9 A one-one map of the set $I_n = \{1, 2, \ldots, n\}$ onto itself is called a *permutation*. The set of all permutations of I_n is a group, the group operation being given by the composition of maps. It is called the *symmetric group of degree* n and is denoted by S_n. If $\sigma \in S_n$ we write

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$$

For $n \geq 3$, S_n is *not abelian.* The order of S_n is $n!$

Definition 1.10 Let G and G' be groups. A map $f\colon G \to G'$ is called a homomorphism if $f(xy) = f(x)f(y)$, $\forall\, x, y \in G$.

Remark 1.11 For a group G, the identity map $I_G\colon G \to G$ is a homomorphism.

Remark 1.12 If $f\colon G \to G'$ and $g\colon G' \to G''$ are homomorphisms, then the map $g \circ f\colon G \to G''$ is a homomorphism.

Definition 1.13 A homomorphism $f\colon G \to G'$ is called an isomorphism, if there exists a homomorphism $g\colon G' \to G$ such that $g \circ f = I_G$ and $f \circ g = I_{G'}$. We then write $G \approx G'$. An isomorphism $f\colon G \to G$ is called an automorphism.

Remark 1.14 A homomorphism is an isomorphism if and only if it is one-one and onto.

Remark 1.15 A homomorphism maps the identity into the identity and the inverse of an element into the inverse of its image.

Example 1.16 The natural map $q\colon \mathbf{Z} \to \mathbf{Z}/(m)$ given by $q(r) = \bar{r}$, where $r \in \mathbf{Z}$, is an onto homomorphism. For $m \neq 0$, it is not an isomorphism.

Example 1.17 The map $f\colon \mathbf{Z} \to \mathbf{Z}$ given by $f(n) = 2n$ is a one-one homomorphism, which is not onto.

Example 1.18 The map $f\colon \mathbf{R} \to \mathbf{R}^{*+}$ (the set of non-zero positive real numbers) given by $f(x) = a^x$, where a is a fixed real number greater than 1 and $x \in \mathbf{R}$, is an isomorphism.

Example 1.19 Let G be a group and let $a \in G$. The map $f_a\colon G \to G$ given by $f_a(x) = axa^{-1}$, where $x \in G$ is an automorphism, called the inner automorphism given by a.

1.2 Subgroups and quotient groups

Definition 1.20 A subgroup H of a group G is a non-empty subset H of G such that if $x, y \in H$, then $x^{-1}y \in H$.

Remark 1.21 The identity e of G belongs to H. Also, if $x \in H$, then $x^{-1} \in H$. In fact H becomes a group under the induced group operation.

Remark 1.22 The inclusion map $i\colon H \to G$ given by $i(x) = x$, where $x \in H$, is a homomorphism.

Example 1.23 G and $\{e\}$ are subgroups of G.

Example 1.24 $\mathbf{Z}$ is a subgroup $\mathbf{Q}$, $\mathbf{Q}$ is a subgroup of $\mathbf{R}$ and $\mathbf{R}$ is a subgroup of $\mathbf{C}$.

Example 1.25 The set of even integers is a subgroup of $\mathbf{Z}$.

Let $f\colon G \to G'$ be a homomorphism of groups. The set $f(G)$ is a subgroup of G'. If e' denotes the identity of G', the set $\{x \in G \mid f(x) = e'\}$ is a subgroup of G, called the *kernel* of f and denoted by $\mathrm{Ker} f$. More generally, the inverse image of a subgroup of G' is a subgroup of G.

The intersection of a family of subgroups of a group is a subgroup. If S is a subset of the group G, the intersection of the family of all the subgroups of G which contain S is called the *subgroup generated by* S. If S consists of just one element a, the subgroup generated by $\{a\}$ is called the *cyclic subgroup generated by* a. It is easily seen that the cyclic subgroup generated by a consists of the powers of a. A group G is called *cyclic* if it coincides with the cyclic subgroup generated by an element $a \in G$.

Example 1.26 $\mathbf{Z}$ is an infinite cyclic group generated by 1.

Example 1.27 $\mathbf{Z}/(m)$ is a cyclic group of order $|m|$, if $m \neq 0$.

Proposition 1.28 *Any subgroup H of $\mathbf{Z}$ is cyclic.*

PROOF: For, if $H = \{0\}$, there is nothing to prove. If $H \neq \{0\}$, let m be the least positive integer in H. Now for any $n \in \mathbf{Z}$ we have $n = qm + r$ where $q, r \in \mathbf{Z}$ and $0 \leq r < m$. If $n \in H$ then $r = n - qm \in H$, which implies that $r = 0$. Hence $H = m\mathbf{Z}$.

NOTATION: For subsets A and B of a group G, we set $AB = \{ab \mid a \in A,\ b \in B\}$. If $A = \{a\}$ (resp. $B = \{b\}$) we write aB (resp. Ab) for $\{a\}B$ (resp. $A\{b\}$). If $A,\ B,\ C \subset G$, it is obvious that $(AB)C = A(BC)$ and we write ABC for either of them.

Let G be a group and let H be a subgroup. Let $R = R_H$ denote the equivalence relation in G defined as follows: xRy, if $x^{-1}y \in H$, where $x, y \in G$. The equivalence class xH to which x belongs is called a *left coset* of G modulo H. If the quotient set G/R consists of n elements, the n is said to be the *index* of H in G and is denoted by $[G : H]$.

Proposition 1.29 *(Lagrange) Let H be a subgroup of a finite group G. Then the order of G is the product of the order of H and the index of H in G. In particular, the order of H is a divisor of the order of G.*

PROOF: We first note that the map $t\colon H \to xH$ given by $t(h) = xh$, where $h \in H$, is a one-one onto map. Therefore the number of elements in any left coset is equal to the order of H. Since any two distinct left cosets are disjoint and the index of H in G is the number of left cosets, the theorem follows.

An element of a group G is said to be of *order* n if the cyclic subgroup generated by a is of order n.

Corollary 1.30 *The order of an element of G is a divisor of the order of G.*

Corollary 1.31 *A group of prime order p is cyclic.*

For, if a is any element different from the identity, the order of a divides p and so is equal to p.

Proposition 1.32 *The following statements are equivalent:*

(i) n is the order of a;

(ii) n is the least positive integer such that $a^n = e$;

(iii) $a^n = e$ and if $a^m = e$, then $n|m$.

PROOF: (i) $\Rightarrow$ (ii). Since the cyclic subgroup generated by a is finite, it follows that the elements $(a^i)_{i\in\mathbf{Z}}$ are not all distinct. If $a^p = a^q$ where $p > q$, then $a^{p-q} = e$. Thus there exists a positive integer m such that $a^m = e$. Taking m to be least positive integer for which $a^m = e$, we observe that the elements $\{a^i \mid 0 \le i < m\}$ are distinct and form a subgroup, which is the cyclic subgroup generated by a. Hence $m = n$.

(ii) $\Rightarrow$ (iii). Let $a^m = e$. We have $m = qn + r$, where $q, r \in \mathbf{Z}$ and $0 \le r < n$. This gives $e = a^m = (a^q)^n a^r = a^r$. Since n is the least positive integer such that $a^n = e$, it follows that $r = 0$. Hence $m = qn$.

(iii) $\Rightarrow$ (i). The elements $(a^i)_{0 \le i < n}$ are all distinct. For, if $a^p = a^q$ where $0 \le p < n$, $0 \le q < n$, and $p > q$, then $a^{p-q} = e$. Therefore, by hypothesis, n divides $p - q$, which is impossible since $p - q$ is less than n. Clearly $\{a^i \mid 0 \le i < n\}$ is the cyclic subgroup generated by a.

The maximum of the orders of the elements of a finite abelian group is called the *exponent* of the group.

Proposition 1.33 *If m is the exponent of a finite abelian group G, then the order of every element of G is a divisor of m.*

We first prove the following.

Lemma 1.34 *Let a and b be elements of a group G such that $ab = ba$. If a and b are of orders m and n respectively such that $(m, n) = 1$, then ab is of order mn.*

PROOF: We have $(ab)^{mn} = a^{mn}b^{mn} = e$. Therefore, if d is the order of ab, then $d|mn$. Again, since $(ab)^d = e$ we have $a^d = b^{-d}$ and so $a^{nd} = e$. Therefore $m|nd$. Since $(m, n) = 1$ it follows that $m|d$. Similarly, $n|d$. Since $(m, n) = 1$, $mn|d$. This proves that ab is of order mn.

PROOF OF THE PROPOSITION: Let a be an element of maximum order m and let b be any element of order n. Let, if possible, $n \nmid m$. Then there exists a prime number p such that if r (resp. s) is the greatest power of p dividing n(resp. m), we have $r > s$. Then a^{p^s}(resp. b^{n/p^r}) has order m/p^s(resp. p^r). Since $(m/p^s, p^r) = 1$ we see, by the above lemma, that the element $a^{p^s}b^{n/p^r}$ is of order $(m/p^s)p^r$ which is greater than m, since $r > s$. This contradicts the assumption on a. Hence the proposition.

Definition 1.35 A subgroup H of a group G is said to be normal in G if $xHx^{-1} = H$, $\forall x \in G$.

A subgroup H of G is normal if and only if $xHx^{-1} \subset H$, $\forall x \in G$.

For any subgroup H of G and any $x \in G, xHx^{-1}$ is a subgroup of G, which is called a *conjugate* of H. By the definition of a normal subgroup, it follows that a subgroup H is normal if and only if all its conjugates coincide with H.

Let $f: G \to G'$ be a homomorphism of groups. The inverse image of a normal subgroup of G' is a normal subgroup of G. Moreover, if f is onto, the image of a normal subgroup of G is a normal subgroup of G'.

G and $\{e\}$ are normal subgroups of G. A subgroup of G other than G is called a *proper* normal subgroup. If a group has no proper normal subgroup other than $\{e\}$, it is called a *simple* group.

Example 1.36 In an abelian group every subgroup is normal.

Example 1.37 An abelian group $G(\neq \{e\})$ is simple if and only if it is cyclic of prime order.

Example 1.38 The kernel of a homomorphism of groups $f: G \to G'$ is a normal subgroup of G.

Example 1.39 If H and K are subgroups of G and if $HK = KH$, then HK is a subgroup of G. The condition $HK = KH$ is satisfied if either H or K is a normal subgroup of G. If both H and K are normal subgroups of G, then HK is also a normal subgroup of G.

Let G be a group and H be a normal subgroup of G. Consider the set G/R of left cosets of G modulo H . We define an operation on G/R by setting $xH \cdot yH = xyH$, where $x, y \in G$. We assert that this operation is well defined. For, if $x' \in xH$, and $y' \in yH$, that is $x' = xh_1$, $y' = yh_2$, where $h_1, h_2 \in H$, then $x'y' = xh_1yh_2 = xy(y^{-1}h_1y)h_2 \in xyH$, since $y^{-1}h_1y \in H$. It is easily seen that G/R is a subgroup under this operation, the identity being $H(= eH)$ and the inverse of xH being $x^{-1}H$. We call this group the *quotient group* of G by H and denote it by G/H. The natural map $q: G \to G/H$ given by $q(x) = xH$ is clearly an onto homomorphism and its kernel is H.

Example 1.40 The group $\mathbf{Z}/(m)$ of residue classes modulo m is the quotient group $\mathbf{Z}/m\mathbf{Z}$.

Let $f: G \to G'$ be an onto homomorphism with kernel H. We define a homomorphism $\bar{f}: G/H \to G'$ by setting $\bar{f}(xH) = f(x)$, where $x \in G$. Clearly $\bar{f}$ is well defined and is an isomorphism of G/H onto G' and we have $\bar{f} \circ q = f$ where $q: G \to G/H$ is the natural map. Thus, "upto an isomorphism" , every homomorphic image of a group is a quotient group. This is usually called the *"fundamental theorem of homomorphisms"*.

Remark 1.41 Let G be a group and let H and K be normal subgroups of G such that $K \subset H$. The homomorphism $\bar{f}\colon G/K \to G/H$ given by $\bar{f}(xK) = xH$, where $x \in G$ is onto and clearly has H/K as kernel. Hence $(G/K)(H/K) \approx G/H$. (*First isomorphism theorem.*)

Remark 1.42 Let H and K be subgroups of a group G and let K be normal in G. Then the homomorphism $f\colon H \to HK/K$ given by $f(h) = hK$, where $h \in H$ has $H \cap K$ as kernel and $H/H \cap K \approx HK/K$. (*Second isomorphism theorem.*)

Remark 1.43 Let G be a cyclic group generated by an element a. The map $f\colon \mathbf{Z} \to G$ given by $f(n) = a^n$, where $n \in \mathbf{Z}$ is an onto homomorphism. Therefore $\mathbf{Z}/\mathrm{Ker}\, f \approx G$. Since Ker $f = m\mathbf{Z}$ for some $m \geq 0$, it follows that every cyclic group is isomorphic to $\mathbf{Z}/m\mathbf{Z}$. It can now be easily shown that subgroups and quotient groups of a cyclic group are cyclic.

Remark 1.44 If G is any group with identity e we have $G/\{e\} \approx G,\ G/G \approx \{e\}$.

Let G be a group and let $a, b \in G$. We say that a is *conjugate* to b, if there exists an element $x \in G$ such that $a = xbx^{-1}$. It is easy to verify that the relation of conjugacy is an equivalence relation. An equivalence class is called a *conjugacy class* or a *class of conjugate elements.*

Remark 1.45 The subset $\{e\}$ of G is a conjugacy class.

Remark 1.46 If a is conjugate to b, then a^m is conjugate to b^m, where $m \in \mathbf{Z}$.

Remark 1.47 A subgroup H of G is normal if and only if it is a union of conjugacy classes.

Let K be a subset of a group G. We define a subset N_K of G called the *normaliser* of K *in* G as follows: $N_K = \{x \in G \mid xK = Kx\}$. If K consists of just one element a we denote the normalizer of $\{a\}$ by N_a and call it the normalizer of a. It is easy to verify that the *normalizer of* a subset K in G is a subgroup of G.

Remark 1.48 A subgroup H is normal in G if and only if $N_H = G$.

Proposition 1.49 *Let G be a finite group and let $a \in G$. Then the number of elements conjugate to a is equal to the index of the normalizer of a in G.*

PROOF: Let C denote the conjugacy class to which a belongs and consider the map $\chi\colon G \to C$ given by $\chi(x) = xax^{-1}$ where $x \in G$. This is an onto map. If $n \in N_a$ then $\chi(xn) = (xn)a(xn)^{-1} = x(nan^{-1})x^{-1} = xax^{-1} = \chi(x)$, $\forall x \in G$. This shows that any two elements of the same left coset of G modulo N_a have the same image in C. Conversely, if $x, y \in G$ and $\chi(x) = \chi(y)$, then $xax^{-1} = yay^{-1}$ giving $(y^{-1}x)a(y^{-1}x)^{-1} = a$. This means $y^{-1}x \in N_a$ and so x and y belong to the same left coset of G modulo N_a. Hence χ induces a one-one correspondence between the left cosets of G modulo N_a and the distinct conjugates of a.

Corollary 1.50 *The number of elements conjugates to a is a divisor of the order of the group G. In particular, if G is of order p^n, where p is a prime, then a conjugacy class consists of p^i elements, where $0 \leq i \leq n$.*

An element $a \in G$ is said to be *central* if $xa = ax$, $\forall x \in G$. The subset of all central elements of G is called the centre of G.

Remark 1.51 An element a of a group G is central if and only if the subset $\{a\}$ is a conjugacy class.

Remark 1.52 The centre of a group is a normal subgroup.

Proposition 1.53 *If G is a group of order p^n where p is a prime and $n \geq 1$ then the centre of G has more than one element.*

PROOF: Let C_i $(1 \leq i \leq m)$ be the distinct conjugacy classes of G and k_i the number of elements of C_i. We have $k_i | p^n$ (Proposition 1.29 and 1.49) so that if $k_i \neq 1$, $p | k_i$. Let C_1 be the conjugacy class containing the identity. If the centre of G reduces to $\{e\}$, we have $C_1 = \{e\}$ and $k_i > 1$ for every $i \neq 1$. Further,

$$p^n = 1 + \sum_{i \geq 2} k_i.$$

Since $p | k_i$ for $i \geq 2$, this is impossible.

1.3 Solvable groups

Definition 1.54 A group G is said to be solvable if there exists a sequence of subgroups.

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = \{e\}$$

such that G_{i+1} is a normal subgroup of G_i and G_i/G_{i+1} is abelian ($0 \leq i < n$). Such a sequence is called a solvable series of G.

Remark 1.55 Every abelian group is solvable.

Proposition 1.56 *Any subgroup and any quotient group of a solvable group is solvable. Conversely, if there is a normal subgroup H of a group G such that H and G/H are solvable, then G is solvable.*

PROOF: Let G be a solvable group having a solvable series

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = \{e\}.$$

If H is a subgroup of G, then

$$H = H \cap G_0 \supset H \cap G_1 \supset \cdots \supset H \cap G_n = \{e\}$$

is a solvable series of H, since $H \cap G_{i+1}$ is a normal subgroup of $H \cap G_i$ and $(H \cap G_i)/(H \cap G_{i+1})$ is isomorphic to a subgroup of G_i/G_{i+1} and so abelian ($0 \leq i < n$). (Compose the inclusion map $H \cap G_i \to G_i$ with the natural map $G_i \to G_i/G_{i+1}$ and apply the fundamental theorem of homomorphisms.) Again, if H is a normal subgroup of G and $q\colon G \to G/H$ is the natural homomorphism, then

$$G/H = q(G_0) \supset q(G_1) \supset \cdots \supset q(G_n) = \{e\}$$

is a solvable series of G/H, since $q(G_{i+1})$ is a normal subgroup of $q(G_i)$ and $q(G_i)/q(G_{i+1})$ which is isomorphic to a quotient of G_i/G_{i+1} is abelian ($0 \leq i < n$).

Conversely, let H be a normal subgroup of G such that H and G/H are solvable. Let $q = G \to G/H$ be the natural homomorphism. Let

$$H = H_0 \supset H_1 \supset \cdots H_n = \{e\}$$

and

$$G/H = G'_0 \supset G'_1 \supset \cdots \supset G'_m = \{e\}$$

be solvable series for H and G/H respectively. Then it is trivial to see that

$$\begin{aligned} G = q^{-1}(G'_0) \supset q^{-1}(G'_1) \supset \cdots \supset q^{-1}(G'_m)\ (= H = H_0) \\ \supset H_1 \supset \cdots \supset H_n = \{e\}. \end{aligned}$$

is a solvable series for G.

Proposition 1.57 *Any group of order p^n where p is a prime, is solvable.*

PROOF: We prove the proposition by induction on n. For $n = 0$, the proposition is trivial. Let $n \geq 1$ and assume that the proposition is true for $r < n$. Let G be a group of order p^n. Then by Proposition 1.53, the centre C of G has order p^s where $s \geq 1$. Then the order of G/C is p^{n-s} and $n - s < n$. By the induction hypothesis G/C is solvable. Now the proposition follows from Proposition 1.56.

Proposition 1.58 *A finite group G is solvable if and only if there exists a sequence of subgroups*

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = \{e\}$$

such that G_{i+1} is a normal subgroup of G_i and G_i/G_{i+1} is cyclic, of prime order $(0 \leq i < n)$.

PROOF: Suppose G is solvable and let

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = \{e\}$$

be a solvable series of G. We shall interpose between G_i and G_{i+1} a sequence of subgroups

$$G_i = H_{i,0} \supset H_{i,1} \supset \cdots \supset H_{i,m} = G_{i+1}$$

such that $H_{i,j+1}$ is a normal subgroup of $H_{i,j}$ and $H_{i,j}/H_{i,j+1}$ is of prime order $(0 \leq j < m)$. For this, it is sufficient to show that given a finite group A and a normal subgroup B of A such that A/B is abelian, there exists a normal subgroup N of A containing B such that A/N is of prime order. Indeed let N be a maximal proper normal subgroup of A containing B. Clearly A/N is simple. However, A/N being a homomorphic image of A/B is abelian and hence of prime order.

The converse is trivial.

1.4 Symmetric groups and solvability

Definition 1.59 Let S_n be the symmetric group of degree n. An r-cycle is a permutation σ such that there exist r distinct integers $x_1, \ldots, x_r$ $(1 \leq x_i \leq n)$ for which $\sigma(x_1) = x_2, \ldots, \sigma(x_{r-1}) = x_r$, $\sigma(x_r) = x_1$ and $\sigma(x) = x$ for $x \neq x_i$, $1 \leq i \leq r$. We then write $\sigma = (x_1, x_2, \ldots, x_r)$. A 2-cycle is called a transposition.

Remark 1.60 An r-cycle is an element of order r.

Remark 1.61 If $\sigma = (x_1, x_2, \ldots, x_r)$ is an r-cycle and τ is any permutation, then $\tau\sigma\tau^{-1} = (y_1, y_2, \ldots, y_r)$, where $\tau(x_i) = y_i$, for $1 \leq i \leq r$.

Proposition 1.62 *S_n is generated by transpositions.*

Proof: We prove the proposition by induction on n. For $n = 1, 2$ the assertion is trivial. Assume the proposition for $n - 1$ and let $\sigma \in S_n$. If $\sigma(n) = n$, then by the induction hypothesis σ is a product of transpositions. If $\sigma(n) = k$ where $k \neq n$, the permutation $\tau = (k, n)\sigma$ is such that $\tau(n) = n$ and so is a product of transpositions. Therefore $\sigma = (k, n)\tau$ is also a product of transpositions.

Corollary 1.63 *S_n is generated by the transpositions $(1, n)$, $(2, n), \ldots, (n-1, n)$.*

For, $(i, j) = (i, n)(j, n)(i, n)$.

Lemma 1.64 *If a permutation can be expressed as a product of m transpositions and also as a product of n transpositions, then $m - n$ is even.*

Proof: The map $f\colon S_n \to \{-1, 1\}$ given by

$$f(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j},$$

where $\sigma \in S_n$ is easily seen to be a homomorphism of groups. If σ is a transposition, then $f(\sigma) = -1$. Regarding σ as a product of m (resp. n) transpositions, we get $f(\sigma) = (-1)^m$(resp. $f(\sigma) = (-1)^n$). Hence $m - n$ is even.

Definition 1.65 A permutation is said to be odd (resp. even) if it can be expressed as a product of an odd (resp. even) number of transpositions.

It should be noted that, in view of the preceding lemma, the notion of odd and even permutations is well defined.

The set of even permutations is a normal subgroup of S_n and is denoted by A_n. It is called the *alternating group of degree n*. We note that the quotient group S_n/A_n is of order 2 if $n > 1$.

Remark 1.66 S_n is solvable for $n \leq 4$. For $n = 1, 2$ there is nothing to prove. For $n = 3$,

$$S_3 \supset A_3 \supset \{e\}$$

is a solvable series of S_3. For $n = 4$,

$$S_4 \supset A_4 \supset V_4 \supset \{e\}$$

is a solvable series of S_4, where

$$V_4 = \{e, (1, 2), (3, 4), (1, 3), (2, 4), (1, 4)(2, 3)\}.$$

It can be verified that V_4 is a normal subgroup of A_4 and A_4/V_4 is a group of order 3 and so is cyclic. Also, V_4 is abelian.

Theorem 1.67 *S_n is not solvable for $n > 4$.*

We need the following

Lemma 1.68 *If a subgroup G of $S_n (n > 4)$ contains every 3-cycle and if H is a normal subgroup of G such that G/H is abelian, then H contains every 3-cycle.*

Proof: Let $q\colon G \to G/H$ be the natural homomorphism. If $\sigma, \tau \in G$, $q(\sigma^{-1}\tau^{-1}\sigma\tau) = q(\sigma)^{-1}q(\tau)^{-1}q(\sigma)q(\tau) = e$, since G/H is abelian. Therefore $\sigma^{-1}\tau^{-1}\sigma\tau \in H$, $\forall \sigma, \tau \in G$. Let (i, j, k) be an arbitrary 3-cycle. Since $n > 4$, we can choose $\sigma = (i, k, l)$, $\tau = (j, k, m)$ where i, j, k, l and m are all distinct. Then

$$\sigma^{-1}\tau^{-1}\sigma\tau = (l, k, i)(m, k, j)(i, k, l)(j, k, m) = (i, j, k) \in H,$$

Proof of Theorem: Let, if possible,

$$S_n = G_0 \supset G_1 \supset \cdots \supset G_m = \{e\}$$

be a solvable series. Since S_n contains every 3-cycle, it follows from the above lemma that G_i contains every 3-cycle for every i where $1 \leq i \leq m$. But, for $i = m$ this is clearly impossible.

Chapter 2

Rings and Vector Spaces

2.1 Rings and homomorphisms

Definition 2.1 A ring A is a triple (A, ϕ, ψ), where A is a set and ϕ, ψ mappings of $A \times A$ into A (we write $\phi(x, y) = x + y, \psi(x, y) = xy$, for $x, y \in A$) such that

(i) (A, ϕ) is an abelian group;

(ii) $x(yz) = (xy)z$, for $x, y, z \in A$ (associativity);

(iii) $x(y + z) = xy + xz, (y + z)x = yx + zx$, for every $x, y, z \in A$ (distributivity);

(iv) there exists an element $1 \in A$ called the unit element such that $1x = x1 = x$, for every $x \in A$.

Remark 2.2 ϕ and ψ are called the ring operations. ϕ is called the *addition* and ψ, the *multiplication* in the ring A; we often write $(A, +)$ for the abelian group (A, ϕ).

Remark 2.3 The identity of (A, ϕ) is called the *zero element* of A and is denoted by 0.

Remark 2.4 The unit element is unique.

Remark 2.5 The associative law for multiplication is valid for any number of elements.

Remark 2.6 For $a, b \in A$ with $ab = ba$ and any integer $n \geq 0$, we have $(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}$, where, for any $x \in A$ and any positive integer m, we write $x^m = x \ldots x(m$ times). We set $x^0 = 1$.

Remark 2.7 For any $a \in A$, by (iii), the map $x \to ax$ (resp. $x \to xa$) is a homomorphism of the group $(A, +)$ into itself and hence $a0 = 0$ (resp. $0a = 0$).

Definition 2.8 A ring A is commutative if $xy = yx$, for every $x, y \in A$.

Example 2.9 The set $\mathbf{Z}$ (resp. $\mathbf{Q}, \mathbf{R}, \mathbf{C}$) of integers (resp. rationals, reals, complex numbers) is a commutative ring with the "usual" addition and multiplication.

Example 2.10 The additive group of residue classes modulo an integer m is a ring, the multiplication being given by $\bar{r}\bar{s} = \bar{rs}$, where $\bar{r}, \bar{s} \in \mathbf{Z}/(m)$.

Example 2.11 Let G be any abelian group. The set $\mathrm{Hom}(G, G)$ of all homomorphisms of G into itself is a ring with respect to the ring operations given by $(f + g)(x) = f(x) + g(x)$, $(fg)(x) = f(g(x))$ for $f,\ g \in \mathrm{Hom}(G, G),\ x \in G$.

Note that $\mathrm{hom}(G, G)$ is, in general, not commutative.

Let A be a ring. A *subring* B of A is a sub-group of $(A, +)$ such that $1 \in B$ and, for $x, y \in B, xy \in B$. We observe that B is a ring under the induced operations. The intersection of any family of subrings of A is again a subring. Let S be a subset of A. The intersection of the family of all subrings of A containing S is called the *subring generated by S*.

Unless otherwise stated, all the rings we shall consider hereafter will be assumed commutative.

Let $a, b \in A$. We say that a *divides* b (or that a is a divisor of b, notation $a|b$) if there exists $c \in A$ such that $b = ac$. If a does not divide b, we write $a \nmid b$. An element $a \in A$ is said to be a *zero divisor* if there exists $x \in A, x \neq 0$ such that $ax = 0$. A is said to be an *integral domain* if $A \neq \{0\}$ and it has no zero-divisors other than 0. An element $a \in A$ is said to be a *unit* in A if there exists $a^{-1} \in A$ such that $aa^{-1} = a^{-1}a = 1$. Let A be an integral domain. A non-zero element $a \in A$ is called *irreducible* if it is not a unit and $a = bc$ with $b, c \in A$ implies that either b or c is a unit.

A commutative ring A is said to be a field if $A^* = A - \{0\}$ is a group under multiplication, so that every non-zero element is a unit. Clearly, a field contains at least two elements. A subring R of a field K is called a *subfield* of K if the ring R is a field. Any intersection of subfields of K is again a subfield. If S is a subset of K, then the intersection of all subfields of K containing S is called the *subfield generated by* S.

Example 2.12 $\mathbf{Z}$ is an integral domain.

Example 2.13 $\mathbf{Z}/(m)$ is a field if and only if m is a prime. For, if $m = rs$, with $|r|, |s| \neq 1$, then $\bar{r}\bar{s} = \overline{rs} = 0$, but $\bar{r}, \bar{s} \neq 0$. Hence $\mathbf{Z}/(m)$ is not an integral domain and a fortiori is not a field. Let m be prime and $\bar{r} \in \mathbf{Z}/(m)$ with $\bar{r} \neq 0$. then $(r, m) = 1$, i.e. there exist $s, t \in \mathbf{Z}$ with $sr + tm = 1$. Obviously $\bar{s}\bar{r} = 1$. Hence $\mathbf{Z}/(m)$ is a field.

Example 2.14 $\mathbf{Q}, \mathbf{R}, \mathbf{C}$ are fields.

Let A, A' be rings. A map $f\colon A \to A'$ is called a *homomorphism* if (i)$f(x + y) = f(x) + f(y)$, (ii)$f(xy) = f(x)f(y)$ for every $x, y \in A$, and (iii) $f(1) = 1$.

For any ring A, the identity map is a homomorphism. Let A, B, C be rings and let $f\colon A \to B$ and $g\colon B \to C$ be homomorphisms. Then $g \circ f\colon A \to C$ is a homomorphism.

A homomorphism $f\colon A \to A'$ is said to be an *isomorphism* if there exists a homomorphism $g\colon A' \to A$ such that $g \circ f = I_A$, $f \circ g = I_{A'}$; the rings A and A' are then said to be *isomorphic* and we write $A \approx A'$. An isomorphism $f\colon A \to A$ is called an *automorphism.*

Remark 2.15 A homomorphism is an isomorphism if and only if it is one-one and onto.

Remark 2.16 Let $f\colon A \to A'$ be a ring homomorphism. If B is a subring of A, then $f(B)$ is a subring of A'.

Example 2.17 Let A be a ring and B a subring of A. Then the inclusion $i\colon B \to A$ is a one-one homomorphism.

Example 2.18 The natural map $q\colon \mathbf{Z} \to \mathbf{Z}/(m)$ is a homomorphism.

Example 2.19 The map $f\colon \mathbf{C} \to \mathbf{C}$ given $f(z) = \bar{z}$ is an automorphism of $\mathbf{C}$.

Let A be an integral domain. Let A^* denote the set of non-zero elements of A. On the set $A \times A^*$ we define the relation $(a, b) \sim (c, d)$ if $ad = bc$. Since A is an integral domain, it can be verified that this is an equivalence relation. We make the quotient set $K = (A \times A^*)/\sim$ a ring by defining the ring operations as follows $a/b + c/d = (ad + bc)/bd$, $(a/b)(c/d) = ac/bd$, where a/b denotes the equivalence class containing (a, b). It is easily verified that these operations are well defined and the K is a ring. In fact, K is a field, the inverse of a/b, $a \neq 0$, being b/a. K is called the *fraction field* of A. The map $i\colon A \to K$ given by $i(a) = a/1$ is a 1-1 homomorphism. We shall identify A with the subring $i(A)$ of K. If $f\colon A \to L$ is a one-one homomorphism of A into a field L, then f can be extended in a unique manner to a one-one homomorphism $\bar{f}$ of K into L, by defining $\bar{f}(a/b) = f(a)f(b)^{-1}$ for $b \neq 0$. If A is a subring of L, the subfield generated by A is the quotient field of A.

Example 2.20 $\mathbf{Q}$ is the quotient field of $\mathbf{Z}$.

2.2 Ideals and quotient rings.

Definition 2.21 Let A be a commutative ring. An ideal I of A is a subgroup of $(A, +)$ such that for $x \in I$, $a \in A$, we have $ax \in I$.

For any ring A, the intersection of any of family if ideals of A is again in ideal. Let S be a subset of A. The intersection of the family of all ideals containing S is called the *ideal generated by S*. It is easily seen that if S is not empty, then this ideal consists precisely of all finite sums of the form $\sum \lambda_i x_i$, $\lambda_i \in A$, $x_i \in S$. For $a \in A$, the ideal generated by $\{a\}$, namely $\{xa \mid x \in A\}$ is called the principal ideal generated by a and is denoted by $\{a\}$. An integral domain for which every ideal is principal is called a *principal ideal domain.*

Example 2.22 $\{0\}$ and A are ideals of A.

Example 2.23 $\mathbf{Z}$ is a principal ideal domain, the ideals of $\mathbf{Z}$ being precisely subgroups of $\mathbf{Z}$.

Example 2.24 Let $f\colon A \to A'$ be a homomorphism, then $\ker f = \{x \in A \mid f(x) = 0\}$ is an ideal.

Proposition 2.25 *A commutative ring A is a field if and only if $1 \neq 0$ and it has no ideals other than A and (0).*

Proof: Let A be a field. Clearly $1 \neq 0$. Let I be a non-zero ideal of A. Then there exists $a \in I$, $a \neq 0$. We have $1 = a^{-1}a \in I$ and hence $A = I$. Conversely, assume that $1 \neq 0$ and that the only ideals of A are (0) and A. Then for any $a \in A$, $a \neq 0$, $(a) = A$. Hence there exists $b \in A$ with $ba = 1$, i.e. A is a field.

Let I be an ideal of A. The additive group A/I is a ring called the *quotient ring* with respect to the multiplication $(x+I)(y+I) = xy+I$, for $x, y \in A$. Since I is an ideal this multiplication is well-defined. The natural map $q\colon A \to A/I$ is an onto homomorphism with kernel I.

Example 2.26 The ring $\mathbf{Z}/(m)$ of residue classes modulo m is the quotient ring of $\mathbf{Z}$ by the principal ideal (m).

Let $f\colon A \to A'$ be an onto homomorphism. Let I be the kernel of f. The homomorphism f induces a homomorphism $\bar{f}\colon A/I \to A'$, by setting $\bar{f}(x+I) = f(x)$ for $x \in A$ it is easy to verity that $\bar{f}$ is an isomorphism of rings and that $\bar{f} \circ q = f$ where q is the natural map $A \to A/I$. This is called the *fundamental theorem of homomorphisms for rings.*

Remark 2.27 Let K be a field. Consider the homomorphism $f\colon \mathbf{Z} \to K$ given by $f(n) = n1 (= 1 + \cdots + 1, n \text{ times})$. By the fundamental theorem of homomorphisms, we have $\mathbf{Z}/\ker f \approx f(\mathbf{Z})$. We know that $\ker f = (p)$ for some $p \geq 0$. We call p the characteristic of the field K. Clearly $pa = 0$ for every $a \in K$. If $p \neq 0$ then p is a prime. Obviously $p \neq 1$ and if $p = rs, r > 0, s > 0$, then $f(p) = f(r)f(s) = 0$. Since K is a field, either $f(r) = 0$ or $f(s) = 0$ i.e. $p|r$ or $p|s$. Since $r \geq 1$, $s \geq 1$, it follows that either $r = 1$ or $s = 1$. Thus $\mathbf{Z}/(p)$ is a field and K contains a subfield isomorphic to $\mathbf{Z}/(p)$. If $p = 0$, then the one-one homomorphism $f\colon \mathbf{Z} \to K$ can be extended to an isomorphism of $\mathbf{Q}$ onto a subfield of K. Hence K contains a subfield isomorphic to $\mathbf{Q}$. Thus we have the following

Proposition 2.28 *Every field contains a subfield isomorphic either to the field of rational numbers or to the field of residue classes of integers modulo a prime p.*

The fields $\mathbf{Q}, \mathbf{Z}/(p)$ where p is a prime are called *prime fields.*

If k is a field of characteristic $p > 0$, then we have,

$$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i} = a^p + b^p \text{ for } a, b \in K.$$

The mapping $x \to x^p$ is a one-one homomorphism of K into K.

Let K be a finite field (i.e. K has a finite number of elements); then the characteristic p of K is > 0. The mapping $x \to x^p$ is then an automorphism of K.

2.3 Polynomial rings.

Let A be a ring. Consider the set R of sequences $f = (a_0, a_1, \ldots, a_n)$, where, $a_n \in A$ and $a_n = 0$ for all but a finite number of n. Let $f, g \in R$ where $f = (a_0, \ldots, a_n, \ldots)$ and $g = (b_0, \ldots, b_n, \ldots)$. We make R into a ring by defining the ring operations as follows:

$$f + g = (a_0 + b_0, \ldots, a_n + b_n, \ldots), fg = (c_0, \ldots, c_n, \ldots), c_n = \sum_{i+j=n} a_i b_j,$$

The unit element of R is $(1, 0, 0, ...)$. The mapping $f: A \to R$ defined by $f(a) = (a, 0, \ldots)$ is clearly a one-one homomorphism and we identify A with the subring $f(A)$ of R. If we write $X = (0, 1, 0, \ldots)$, then, for $i > 0$, $X^i = (d_0, d_1, \ldots)$ where $d_i = 1$ and $d_j = 0$ for $j \neq i$. It is easy to see that every $f \in R$ can be written uniquely as a finite sum $\sum a_i X^i$, $a_i \in A$. The ring R is denoted by $A[X]$, and is called the *polynomial ring in one variable* over A. The elements of $A[X]$ are called polynomials.

Let A, B be rings and $\phi: A \to B$ a ring homomorphism. Then ϕ admits a unique extension to a ring homomorphism $\phi: A[X] \to B[X]$, with $\phi(X) = X$. We have only to set $\phi(\sum a_i X^i) = \sum \phi(a_i) X^i$.

Let B be a ring and A a subring of B. For any $\alpha \in B$ we define a map $\psi: A[X] \to B$ by setting $\psi(\sum a_i X^i) = \sum a_i \alpha^i$. It is easily verified that ψ is a ring homomorphism. We write $\psi(A[X]) = A[\alpha]$ and for $f(X) = \sum a_i X^i \in A[X]$, we write $\psi(f) = f(\alpha)(= \sum a_i \alpha^i)$. We say that α is a *root* of f if $f(\alpha) = 0$.

Let $f = \sum a_i X^i \in A[X]$, $f \neq 0$. Then we define the *degree* of f (notation : $\deg f$) to be the largest integer n such that $a_n \neq 0$. We call a_n the *leading coefficient* of f. If $a_n = 1$, f is said to be a *monic polynomial.* We have $\deg(f+g) \leq \max(\deg f,\ \deg g)$ if $f \neq 0$, $g \neq 0$ and $f + g \neq 0$. A polynomial of degree 1 is called a *linear polynomial.*

Remark 2.29 If A is an integral domain and $f, g \in A[X]$, with $f \neq 0$, $g \neq 0$,then $fg \neq 0$, i.e. $A[X]$ is an integral domain and we have $\deg(fg) = \deg f + \deg g$.

Remark 2.30 If A is an integral domain, the the units of $A[X]$ are precisely the units of A.

Proposition 2.31 *(Euclidean Algorithm.) Let A be a commutative ring. Let $f, g \in A[X]$, and let g be a monic polynomial. Then there exist $q, r \in A[X]$ such that $f = qg + r$, where $r = 0$ or $\deg r < \deg g$. Further q and r are unique.*

PROOF: Suppose $\deg\ f = n, \deg\ g = m$. If $n < m$ choose $q = 0$ and $r = f$. If $n \geq m$, we prove the lemma by induction on n. Assume the lemma to be true for polynomials f of degree $< n$. We have $\deg(f - a_n X^{n-m} g) < n$ where a_n is the leading coefficient of f and so by induction hypothesis,

$$f - a_n X^{n-m} g = q_1 g + r_1$$

with $r_1 = 0$ or $\deg r_1 < m$. Hence $f = qg + r$ where $q = a_n X^{n-m} + q_1$ and $r = r_1$.

We next prove the uniqueness. Suppose, further, that $f = q'g + r'$, where $r' = 0$ or $\deg r' < m$. Then $(q - q')g = r' - r$. If $r' \neq r$ then $q \neq q'$ and since g is a monic polynomial $\deg(r' - r) \geq m$. This is a contradiction. Hence $r' = r$. Since g is monic, it follows that $q' = q$.

Remark 2.32 The above proposition is valid, more generally, if the leading coefficient of g is a unit. In particular, if A is a field, it is enough to assume that $g \neq 0$.

Corollary 2.33 *Let $f \in A[X]$. Then $\alpha \in A$ is a root of f if and only if $X - \alpha$ divides f.*

PROOF: By the above lemma we have $f = q(X - \alpha) + a$ with $a \in A$. Hence $f(\alpha) = q(\alpha)0 + a$, i.e. $f(\alpha) = 0$ if and only if $X - \alpha$ divides f.

Let $f \in A[X]$, $f \neq 0$. We say that $\alpha \in A$ is a *simple root* of f if $(X - \alpha)|f$ and $(X - \alpha)^2 \nmid f$. If $(X - \alpha)^r|f$ with $r > 1$, we say that α is a *multiple root* of f.

Proposition 2.34 *Let A be an integral domain and let f be an element of $A[X]$ of degree n. Then f has at most n roots.*

PROOF: If $\alpha \in A$ is a root of f, we have $f = (X - \alpha)g$ where $g \in A[X]$ and $\deg g = n - 1$. If $\beta \in A,\ \beta \neq \alpha$ is a root of f, we have $0 = f(\beta) = (\beta - \alpha)g(\beta)$. Since A is an integral domain, we have $g(\beta) = 0$. Now the proposition follows by induction on n.

Proposition 2.35 *Let K be a field. Then $K[X]$ is a principal ideal domain.*

PROOF: Let I be a non-zero ideal of $K[X]$. Let $g \in I$ be a non-zero polynomial of smallest degree in I. For any $f \in I,\ f \neq 0$, by Proposition 2.31, we have $f = qg + r$, where $r = 0$ or $\deg\ r < \deg\ g$. Since $r = f - qg \in I$, we have $r = 0$. Hence $I = (g)$.

Proposition 2.36 *Let K be a field. Any non-constant polynomial $f \in K[X]$ can be expressed as a product $f = c\prod_{i=1}^{m} p_i$, where $c \in K$ and p_i are monic irreducible polynomials. Further, this expression is unique except for the order of factors.*

PROOF: We prove the existence by induction on $n = \deg f$. If $n = 0$, $f \in K$ and there is nothing to prove. Further if f is irreducible, then $f = c(c^{-1}f)$, where $c \in K$ is so chosen that $c^{-1}f$ is a monic irreducible polynomial. If f is not irreducible, then $f = gh$ where $\deg h \neq 0,\ \deg g \neq 0$. Since $\deg g < n,\ \deg h < n$, by induction hypothesis $g = a\prod_{i=1}^{r} p_i,\ h = b\prod_{j=1}^{q} q_j$, where $a, b \in K$ and p_i, q_j are monic irreducible polynomials. Hence $f = ab\prod_{i=1}^{r} p_i \prod_{j=1}^{s} q_j$.

To prove the uniqueness we need the following

Lemma 2.37 *Let p be an irreducible polynomial in $K[X]$. Then $K[X]/(p)$ is a field. In particular, if $p|gh$, where $g, h \in K[X]$, then $p|g$ or $p|h$.*

PROOF: Let $\bar{g} \in K[X]/(p)$ with $\bar{g} \neq 0$. Let $g \in K[X]$ represent $\bar{g}$. Then $g \notin (p)$. Consider the ideal I generated by p and g. Since $K[X]$ is a principal ideal domain, we have $I = (t)$, for some $t \in K[X]$. Since $p \in I,\ p = wt,\ w \in K[X]$. We assert that w is not a unit. For otherwise $I = (p)$ and hence $g \in (p)$ and this contradicts our hypothesis. Since p is irreducible, t is a unit. Hence $I = K[X]$ and $1 = up + vg$, for some $u, v \in K[X]$. Thus $\bar{v}\bar{g} = 1$ where $\bar{v} \in K[X]/(p)$ is the class of v. This proves the lemma.

Assume that $f = c\prod_{i=1}^{r} p_i = c'\prod_{j=1}^{s} p'_j$ with $c, c' \in K$ and p_i, p'_j monic irreducible polynomials in $K[X]$. It is evident that $c = c'$. Hence we have $\prod_{i=1}^{r} p_i = \prod_{j=1}^{s} p'_j$. We shall prove the uniqueness by induction on r. Since p_r divides the product $\prod_{j=1}^{s} p'_j$, by the above lemma p_r divides one of the factors of $\prod_{j=1}^{s} p'_j$. We may assume $p_r | p'_s$. Since p_r, p'_s are monic irreducible polynomials we have $p_r = p'_s$. Hence $\prod_{i=1}^{r-1} p_i = \prod_{j=1}^{s-1} p'_j$. By induction hypothesis, the uniqueness follows.

Proposition 2.38 *(Gauss.) Any non-constant irreducible polynomial in $\mathbf{Z}[X]$ is also an irreducible polynomial in $\mathbf{Q}[X]$.*

Proof: Let f be a non-constant irreducible polynomial in $\mathbf{Z}[X]$. Then the g.c.d. of the coefficients of f is 1. If possible let $f = gh$ where $g, h \in \mathbf{Q}[X]$ and $\deg g > 0,\ \deg h > 0$. Then we have $df = g'h'$, where $d \in \mathbf{Z},\ d > 0$ and $g', h' \in \mathbf{Z}[X],\ \deg g' > 0,\ \deg h' > 0$. Let d_1 (resp.d_2) be the g.c.d. of the coefficients of g' (resp. h'). Since the g.c.d. of the coefficients of f is 1, it follows that $d_1 d_2 | d$. Hence we may assume without loss of generality that the g.c.d. of the coefficients of g' (resp. h') is 1. Let p be a prime factor of d. Let $\eta\colon \mathbf{Z}[X] \to \mathbf{Z}/(p)[X]$ be the ring homomorphism given by $\eta(\sum a_i X^i) = \sum \bar{a}_i X^i$, where $\bar{a}_i$ is the class of a_i. We have $0 = \eta(df) = \eta(g')\eta(h')$. Since $\mathbf{Z}/(p)[X]$ is an integral domain, either $\eta(g') = 0$ or $\eta(h') = 0$, i.e. p divides all the coefficients of either g' or h'—a contradiction. Hence $d = 1$, i.e. $f = g'h'$. Since f is irreducible in $\mathbf{Z}[X]$, either g' or h' is a unit. This is a contradiction.

Proposition 2.39 *(Eisenstein's irreducibility criterion). Let $f = a_0 + a_1 X + \cdots + a_n X^n \in \mathbf{Z}[X]$. Suppose $a_i \equiv 0 (\bmod p)$ for $i < n,\ a_n \not\equiv 0 (\bmod\ p)$ and $a_0 \not\equiv 0 (\bmod\ p^2)$;(here p is a prime). Then f is irreducible in $\mathbf{Q}[X]$.*

Proof: We may assume that the g.c.d. of the coefficients of f is 1. By virtue of the above proposition it is enough to prove that f is irreducible in $\mathbf{Z}[X]$. Let if possible $f = gh$, where $g, h \in \mathbf{Z}[X]$ and $\deg g > 0,\ \deg h > 0$. Let $\eta\colon \mathbf{Z}[X] \to \mathbf{Z}/(p)[X]$ be the ring homomorphism given by $\eta(\sum b_i X_i) = \sum \bar{b}_i X^i$, where $\bar{b}_i$ is the residue class of b_i. Putting $\eta(u) = \bar{u}$ for $u \in \mathbf{Z}[X]$ we have $\bar{f} = \bar{g}\bar{h}$. Since $\bar{f} = \bar{a}_n X^n$, it follows by uniqueness of factorization in $\mathbf{Z}/(p)[X]$ that $\bar{g} = \bar{b} X^l,\ \bar{h} = \bar{c} X^{n-l}$. Since $a_n \not\equiv 0 (\bmod\ p)$,we have $l = \deg \bar{g} = \deg g > 0$ and $n - l = \deg \bar{h} = \deg h > 0$. Hence the constant terms of g and h are divisible by p which implies $a_0 \equiv 0 (\bmod p^2)$. This contradicts the assumption on a_0.

2.4 Vector spaces

Definition 2.40 A vector space over a field K is a triple $(V, +, \psi)$ where

(1) $(V, +)$ is an abelian group,

(2) $\psi\colon K \times V \to V$ (we write $\psi(\lambda, x) = \lambda x$) is such that

(a) $\lambda(x + y) = \lambda x + \lambda y$,

(b) $(\lambda + \mu)x = \lambda x + \mu x$,

(c) $\lambda(\mu x) = (\lambda\mu)x$,

(d) $1x = x$,

where $\lambda, \mu \in K,\ x, y \in V$.

Remark 2.41 The elements of K are called scalars and the elements of V are called vectors, ψ is called the scalar multiplication.

Remark 2.42 $\lambda x = 0$ if and only if $\lambda = 0$ or $x = 0$. For (a) (resp.(b)) implies $\lambda 0 = 0$(resp. $0x = 0$). On the other hand, if $\lambda x = 0$ and $\lambda \neq 0$, we have $0 = \lambda^{-1}(\lambda x) = (\lambda^{-1}\lambda)x = 1x = x$.

Example 2.43 Let K be a field and k a subfield of K. Then K is a vector space over k if we set $\psi(\lambda, x) = \lambda x$ for $\lambda \in k,\ x \in K$.

Example 2.44 For any field K, the set K^n of all ordered n-tuples $(\lambda_1, \dots, \lambda_n),\ \lambda_i \in K$, is a vector space over K if we set

$$(\lambda_1, \dots, \lambda_n) + (\mu_1, \dots, \mu_n) = (\lambda_1 + \mu_1, \dots, \lambda_n + \mu_n)$$

and

$$\lambda(\lambda_1, \dots, \lambda_n) = (\lambda\lambda_1, \dots, \lambda\lambda_n).$$

Example 2.45 For any field K, the ring $K[X]$ becomes a vector space over K if we set $\psi(\lambda, f) = \lambda f,\ \lambda \in K,\ f \in K[X]$.

A subset W of V is called a *subspace* of V if W is a subgroup of $(V, +)$ and $\lambda x \in W$ for $\lambda \in K,\ x \in W$. Then W is a vector space over K under the induced operations. We say that a subspace W is a *proper* subspace of V if $W \neq V$.

Example 2.46 (0) and V are subspaces of V.

Example 2.47 If K is a field, any ideal in $K[X]$ is a subspace of $K[X]$.

Example 2.48 The intersection of a family of subspaces of V is a subspace of V. If S is a subset of V, the intersection W of the family of all subspaces containing S is called the *subspace generated by* S and S is called a *set of generators* of the subspace W. It is easy to see that if S is not empty, W consists precisely of elements of the form $\sum_{i=1}^{n} \lambda_i x_i,\ \lambda_i \in K,\ x_i \in S,\ n > 0$; if $S = \phi$, then $W = \{0\}$.

Let V, W be vector spaces over a field K. A map $f: V \to W$ is called a K-*linear map* if f is a homomorphism of $(V, +)$ into $(W, +)$ and $f(\lambda x) = \lambda f(x)$ for $\lambda \in K,\ x \in V$. A K-*linear* map $f: V \to W$ is called an *isomorphism* if there exists a K-linear map $g: W \to V$ such that $g \circ f = I_V,\ f \circ g = I_W$. It is easy to see that a K-linear map $f: V \to W$ is an isomorphism if and only if f is one-one and onto.

Example 2.49 The map $p_i: K^n \to K$ defined by $p_i(x_1, \ldots, x_n) = x_i$ is a K-linear map. The maps p_i are called *projections*.

Example 2.50 The map $z \to \bar{z}$ is an $\mathbf{R}$-linear isomorphism of the vector space $\mathbf{C}$ onto $\mathbf{C}$.

Let V be a vector space and W a subspace of V. The additive group V/W becomes a vector space if we set $\lambda\bar{x} = \overline{\lambda x}$ for $\bar{x} \in V/W,\ \lambda \in K$. The vector space V/W is called the *quotient space* of V by W. The natural map $q: V \to V/W$ is a K-linear map.

Remark 2.51 It is easy to see that if $f: V \to W$ is a linear map, then $\ker f$ is a subspace of V and that if f is onto, it induces a linear isomorphism $\bar{f}$ of $V/\ker f$ onto W.

Let $x_i,\ 1 \le i \le n$ be elements of V. We say that they are *linearly independent* if $\sum_{1 \le i \le n} \lambda_i x_i = 0, \lambda_i \in K$ implies $\lambda_i = 0$ for every $i,\ 1 \le i \le n$.

A subset S of V is said to be *linearly independent* if every finite subset of elements of S is linearly independent. A set consisting of a single non-zero element of V is linearly independent. Note that a subset of a linearly independent set is linearly independent. S is said to be *linearly dependent* if it is not linearly independent.

Definition 2.52 A subset S of V is called a base (or a K-base) of V if S is linearly independent and generates V.

Clearly S is a base of V if and only if every element $v \in V$ can be uniquely written as finite sum $v = \sum \lambda_i s_i,\ \lambda_i \in K,\ s_i \in S$.

Example 2.53 The set $\{1, x, x^2, \ldots\}$ is a base for the vector space $K[X]$.

Example 2.54 For any field K, the elements $e_i = (\delta_{i1}, \ldots, \delta_{in}),\ 1 \leq i \leq n$, form a base for the vector space K^n, where $\delta_{ij} = 0$ for $i \neq j$, and $\delta_{ij} = 1$ for $i = j$.

Proposition 2.55 *Let V be a vector space. Let $x_i,\ 1 \leq i \leq m$, generate V. If S is any linearly independent set of V, then S contains at most m elements.*

PROOF: We shall prove the proposition by induction on m. If $m = 0$, then $V = 0$ and $S = \emptyset$. Let $m > 0$ and let $y_1, \ldots, y_n$ be finitely many elements of S. Let V' be the subspace of V generated by $x_2, \ldots, x_m$. If $y_i \in V'$, for $1 \leq i \leq n$, then by the induction hypothesis, $n \leq m - 1$. Otherwise $y_i \notin V'$ for some i, say for $i = 1$. Then $y_1 = \sum \alpha_i x_i,\ \alpha_1 \neq 0$, so that $x_1 = \beta_1 y_1 + \sum_{2 \leq i \leq m} \beta_i x_i,\ \beta_i \in K$. $y_i - \lambda_i y_1 \in V'$. Clearly the elements $y_i - \lambda_i y_1,\ 2 \leq i \leq n$, are linearly independent and hence by the induction hypothesis, $n - 1 \leq m - 1$. Thus S consists of at most m elements.

Corollary 2.56 *If $\{x_1, \ldots, x_m\}$ and $\{y_1, \ldots, y_n\}$ are bases of V, then $m = n$.*

We say that a vector space is of *dimension* n (notation : $\dim V = n$) if there exists a base of V consisting of n elements. If $\dim V = n$, then by Corollary 2.56 every base of V consists of n elements.

Corollary 2.57 *Let W be a subspace of V with $\dim V = n$. Then W has a base consisting of at most n elements, i.e. $\dim W \leq \dim V$. If W is a proper subspace of V, then $\dim W < \dim V$.*

PROOF: Any linearly independent set in V consists of at most n elements. Choose a maximal set of linearly independent elements in W. This forms a base of W. Hence $\dim W \leq \dim V$. Since any linearly independent set consisting of n elements generates V, it follows that if W is a proper subspace of V, then $\dim W < \dim V$.

Proposition 2.58 *Let V be a vector space over an infinite field K. Then V is not the union of a finite number of proper subspaces.*

PROOF: We shall prove that given n proper subspaces (V_i), $1 \leq i \leq n$, there exists an $x \in V$, $x \notin \bigcup_{i=1}^n V_i$. We shall prove this by induction on n. If $n = 1$, choose $x \notin V_1$. Assume there exists an $e \notin V_i$, $1 \leq i \leq n-1$. If $e \notin V_n$, there is nothing to prove. Suppose $e \in V_n$. Choose $f \notin V_n$. Then $e + \lambda f \notin V_n$ for every $\lambda \in K^*$. We claim that there exists a $\lambda_0 \in K^*$ such that $e + \lambda_0 f \notin V_i$ $1 \leq i \leq n$. For otherwise, since K is infinite, there exist $\lambda,\ \lambda' \in K^*,\ \lambda \neq \lambda'$ such that $e + \lambda f,\ e + \lambda' f \in V_i$, for some $i < n$. Then $(\lambda - \lambda')f \in V_i$, i.e. $f \in V_i$. Hence $e \in V_i$. This is a contradiction.

Chapter 3

Field Extensions

3.1 Algebraic extension

Let K be a field and k a subfield of K. Then K will be called an *extension* of K and written K/k. Two extensions K/k, K'/k are said to be *k-isomorphic* if there exists an isomorphism σ of K onto K' such that $\sigma|k$ is the identity. σ is then called a k-isomorphism. Let $\alpha_1, \ldots, \alpha_n \in K$. We denote by $k(\alpha_1, \ldots, \alpha_n)$ (resp.$k[\alpha_1, \ldots, \alpha_n]$) the subfield (resp. subring) of K generated by k and $\alpha_1, \ldots, \alpha_n$. Clearly $k[\alpha_1, \ldots, \alpha_n]$ is a subring of $k(\alpha_1, \ldots, \alpha_n)$. Clearly, any $\alpha \in k(\alpha_1, \ldots, \alpha_n)$ can be written as $\alpha = \dfrac{f(\alpha_1, \ldots, \alpha_n)}{g(\alpha_1, \ldots, \alpha_n)}$ where $f(\alpha_1, \ldots, \alpha_n)$ (resp. $g(\alpha_1, \ldots, \alpha_n)$) $= \sum_{i_1 \ldots i_n} a_{i_1 \ldots i_n} \alpha_1^{i_1} \cdots \alpha_{i_n}^{n}$ (resp. $= \sum_{j_1 \ldots j_n} b_{j_1 \ldots j_n} \alpha_1^{s_1} \ldots \alpha_n^{s_n}$) with $a_{i_1 \ldots i_n}$, $b_{j_1 \ldots j_n} \in k$ and $g(\alpha_1, \ldots, \alpha_n) \neq 0$. For $\alpha \in K$, the field $k(\alpha)$ is called a *simple extension* of k. The map $\phi: k[X] \to k[\alpha]$ defined by $\phi(g) = g(\alpha)$ for any $g \in k[X]$ is clearly an onto homomorphism of rings.

Case (i) Ker $\phi = (0)$, i.e. α is not a root of any non-zero polynomial over k. We say in this case that α is *transcendental over k*. Then the one-one homomorphism $\phi: k[X] \to k(\alpha)$ can be extended to a one-one homomorphism of $k(X)$ the quotient field of $k[X]$, onto a subfield of $k(\alpha)$. However, this subfield contains α and k, and it must therefore coincide with $k(\alpha)$. Hence $k(\alpha)$ is isomorphic to $k(X)$.

Case (ii) Ker $\phi \neq (0)$, i.e. α is root of a non-zero polynomial. We say then that α is *algebraic over k*. Since every ideal in $k[X]$ is a principal ideal (Chapter 2 Proposition 2.25), we have Ker $\phi = (f)$ for some $f \in k[X]$. Clearly, f is not a constant. The polynomial f is irreducible. In fact, suppose $f = gh$ where $\deg g$ and $\deg h$ are both less than $\deg f$. We then have $0 = f(\alpha) = g(\alpha)h(\alpha)$. Hence either $g(\alpha) = 0$ or $h(\alpha) = 0$ i.e. $g \in (f)$ or $h \in (f)$. This is impossible in view of our assumption on the degrees of g and h.

We have an isomorphism $k[X]/(f) \approx k[\alpha]$. Since $k[X]/(f)$ is a field (see Chapter 2), it follows that $k[\alpha]$ is a field, and since it contains α and k we have $k[\alpha] = k(\alpha)$. Hence $k[X]/(f) \approx k(\alpha)$. We may assume that f is a monic polynomial. The polynomial f is then called the *minimal polynomial* of α over k.

An extension K/k is called an *algebraic extension* if every $\alpha \in K$ is algebraic over k. We note that if $\alpha \in K$ is algebraic over k it is algebraic over any field L such that $K \supset L \supset k$.

Proposition 3.1 *Let $\alpha \in K$ be algebraic over k and let n denote the degree of its minimal polynomial. Then the k-vector space $k(\alpha)$ has dimension n over k.*

PROOF: In fact $1, \alpha, \ldots \alpha^{n-1}$ form a k-base for $k(\alpha)$. Since α cannot satisfy a polynomial of degree $< n$, the elements $1, \alpha, \ldots, \alpha^{n-1}$ are linearly independent over k. Moreover it is clear by induction that any α^i can be expressed as a linear combination of $1, \alpha, \ldots, \alpha^{n-1}$ with coefficients in k.

Let K/k be an extension such that K is a vector space of dimension n over k. We then say that K is a *finite extension* of k and write $(K\colon k) = n$(n is called the *degree* of K over k). If $\alpha_1, \ldots, \alpha_n \in K$ form a k-base of K, we have $K = k(\alpha_1, \ldots, \alpha_n)$.

Proposition 3.2 *Any finite extension K/k is an algebraic extension.*

PROOF: For any $\alpha \in K$, $\alpha \neq 0$ there exists a non-zero integer n such that $1, \alpha, \ldots, \alpha^n$ are linearly dependent over k and hence there exist $a_1, \ldots, a_n \in k$, with $a_i \neq 0$ for at least one i such that $\sum_{0 \le i \le n} a_i \alpha^i = 0$ i.e. α is a root of the non-zero polynomial $\sum_{0 \le i \le n} a_i X^i$.

Proposition 3.3 *Let K/k and L/k be extensions such that $(K\colon k) = m$ and $(L\colon K) = n$. Then $(L\colon k) = mn$.*

PROOF: Let $\alpha_1, \ldots, \alpha_m$ be a k-base of K and let $\beta_1, \ldots, \beta_n$ K-base of L. We assert that the elements $\alpha_i\beta_j$, $1 \le i \le m$, $1 \le j \le n$, form a k-base for L. In fact let $\alpha \in L$. Then $\alpha = \sum_{1 \le j \le n} t_j \beta_j$ with $t_j \in K$. Let $t_j = \sum_{1 \le i \le m} s_{ij} \alpha_i$ with $s_{ij} \in k$. We then have $\alpha = \sum_{\substack{1 \le i \le m \\ 1 \le j \le n}} s_{ij} \alpha_i \beta_j$. Hence the $\alpha_i\beta_j$ generate L as a k-vector space. On the other hand, suppose that $\sum_{\substack{1\le i\le m\\1\le j\le n}} s_{ij}\alpha_i\beta_j = 0$ where $s_{ij}\in K$. We must then have $\sum_{1\le i\le m} s_{ij}\alpha_i = 0$ for every j. This implies that $s_{ij}=0$ for every i,j with $1\le i\le m$, $1\le j\le n$. Thus the $\alpha_i\beta_j$ are linearly independent.

Corollary 3.4 *Let K/k be any extension and $\alpha_1,\dots,\alpha_n\in K$ be algebraic over k. Then $k(\alpha_1,\dots,\alpha_n)/k$ is a finite extension.*

PROOF: In fact, the corollary has already been proved for $n=1$ (Proposition 3.1). Let us assume by induction that $k(\alpha_1,\dots,\alpha_{n-1})/k$ is a finite extension. Then $k(\alpha_1,\dots,\alpha_n)=k(\alpha_1,\dots,\alpha_{n-1})(\alpha_n)$ is a finite extension of $k(\alpha_1,\dots,\alpha_{n-1})$. The corollary now follows from Proposition 3.3.

It follows from Corollary 3.4, that if $\alpha,\beta\in K$ are algebraic, then $\alpha+\beta$, $\alpha^{-1}(\alpha\ne 0)$ and β are algebraic.

Corollary 3.5 *If K/k and L/K are algebraic extensions, then L/k is algebraic.*

PROOF: Let $\alpha\in L$ and let $\sum_{0\le i\le n} a_i\alpha^i = 0$ with $a_0,\dots,a_n\in K$, $a_i\ne 0$ for at least one i. Clearly α is algebraic over $k(a_0,\dots,a_n)$. Since $k(a_0,\dots,a_n)/k$ is finite by Corollary 3.4, it follows from Proposition 3.3that $k(\alpha,a_0,\dots,a_n)/k$ is finite. Hence α is algebraic over k, by Proposition 3.2.

Example 3.6 Any field is an extension of its prime field.

Example 3.7 $\mathbf{C}/\mathbf{R}$ is an extension of degree 2.

Example 3.8 For any field k, $k(X)/k$ is not algebraic; here $k(X)$ is the fraction field of $k[X]$. In fact X is transcendental over k.

3.2 Splitting fields and normal extensions

Definition 3.9 Let k be a field and let $f\in k[X]$. An extension K/k is called a splitting field of f if

(i) $f(X)=c\prod_{1\le i\le n}(X-\alpha_i)$; $\alpha_i\in K$, $c\in k$;

(ii) $K=k(\alpha_1,\dots,\alpha_n)$.

Proposition 3.10 *Any nonconstant polynomial $f\in k[X]$ has a splitting field.*

PROOF: Let $f \in k[X]$ be an irreducible polynomial. Then $k[X]/(f)$ is a field (see Chapter 2). The map $a \to \bar{a}$ of k into $k[X]/(f)$, where $\bar{a}$ is the coset of a in $k[X]/(f)$, is clearly a one-one homomorphism and we identify k with its image. Thus $k[X]/(f)$ is an extension of k. Let $q\colon k[X] \to k[X]/(f)$ denote the natural map and let $q(X) = \alpha$. Clearly $f(\alpha) = 0$. Let $\deg f = n$. Since $1, \alpha, \ldots, \alpha^{n-1}$ form a k-base for $k[X]/(f)$ (Proposition 3.1), we note that $(k[X]/(f)\colon k) = \deg f$.

We prove the proposition by induction on $n = \deg f$. If $n = 1$, f is a linear polynomial and k is obviously a splitting field of f. Let us assume $n \geq 2$ and that for any polynomial g of degree $n-1$ over any field, there exists a finite extension in which g can be written as a product of linear factors. Let f be any polynomial of degree n. Let f_1 be an irreducible factor of f. Let $K_1 = k(\alpha)$ be an extension of k such that $f_1(\alpha) = 0$. Then $f(\alpha) = 0$ and therefore $f = (X - \alpha)g$, where $g \in K_1[X]$ with $\deg g = n - 1$ (corollary to Proposition 2.31) By induction, there exists a finite extension of K_1 in which g can be written as a product of linear factors. Thus, there exists a finite extension K/k such that $f(X) = c\prod_{1\leq i\leq n}(X - \alpha_i)$; $\alpha_i \in K$, $c \in k$. Then $k(\alpha_1, \ldots, \alpha_n)$ is a splitting field of f. This proves the proposition.

Let k, k' be fields and let $\sigma\colon k \to k'$ be an isomorphism. If we define for any $f = a_0 + \cdots + a_nX^n \in k[X]$, $\bar{\sigma}(f) = \sum_{0\leq i\leq n}\sigma(a_i)X^i$, we have an isomorphism $\bar{\sigma}\colon k[X] \to k'[X]$ such that $\bar{\sigma}|k = \sigma$. We shall often write σ for $\bar{\sigma}$. If $f \in k[X]$ is irreducible, then $\sigma(f)$ is irreducible in $k'[X]$ and we have an induced isomorphism $k[X]/(f) \approx k'[X]/(\sigma(f))$. Since for any root α of f, we have an isomorphism $k[X]/(f) \approx k(\alpha)$, in which the coset of X is mapped on to α, this implies that if α (resp. α') is a root of f(resp. $\sigma(f)$), we have an isomorphism $k(\alpha) \approx k(\alpha')$ (in which α is mapped onto α') and which coincides with σ on k.

In particular, if $k' = k$ and $\sigma =$ identity, then for any two roots α, α' of f we have a k-isomorphism $k(\alpha) \approx k(\alpha')$ which maps α onto α'.

Definition 3.11 Let K/k be an algebraic extension. Two elements $\alpha, \alpha' \in K$ are said to be conjugates over k if there exists a k-isomorphism of $k(\alpha)$ onto $k(\alpha')$ which maps α onto α'.

Proposition 3.12 *Let K/k be an algebraic extension and let $\alpha, \alpha' \in K$. Then α and α' are conjugates over k if and only if they have the same minimal polynomial over k.*

PROOF: If α and α' have the same minimal polynomial oner k, we have proved above that α and α' are conjugates. Conversely, suppose that

α, α' are conjugates over k. Let f and g denote the minimal polynomials of α and α' respectively. Let $\sigma\colon k(\alpha) \approx k(\alpha')$ be a k-isomorphism such that $\sigma(\alpha) = \alpha'$. We have

$$0 = \sigma(f(\alpha)) = f(\sigma(\alpha)) = f(\alpha').$$

Thus $g|f$. Since f is monic and irreducible we have $f = g$.

Proposition 3.13 *Let k, k' be fields and let $\sigma\colon k \to k'$ be an isomorphism. Let f be any polynomial with coefficients in k, and let K, K' be splitting fields of f and $\sigma(f)$ respectively. Then there exists an isomorphism $\tau\colon K \to K'$ such that $\tau|k = \sigma$.*

PROOF: We proceed by induction on the degree of f. If $\deg f = 0$ there is nothing to prove. Let $\deg f \geq 1$ and let f_1 be an irreducible factor of f. Let α be a root of f_1 and let α' be any root of $\sigma(f_1)$. By what we have seen above, σ can be extended to an isomorphism $\sigma_1\colon k(\alpha) \to k'(\alpha')$ such that $\sigma_1(\alpha) = \alpha'$. Let $f = (X - \alpha)g$, with $g \in k(\alpha)[X]$. Then $\sigma(f) = (X - \alpha')\sigma_1(g)$. The field K (resp. K') is a splitting field of the polynomial g (resp. $\sigma_1(g)$ over $k(\alpha)$ (resp. $k'(\alpha')$). By induction, σ_1 admits an extension to an isomorphism $\tau\colon K \to K'$. We clearly have $\tau|k = \sigma$.

In particular, taking $k = k'$ and $\sigma =$ identity, we obtain the

Corollary 3.14 *Any two splitting fields of a polynomial are isomorphic, i.e. the splitting field of a polynomial is unique " up to k-isomorphism".)*

In view of the above corollary, we can talk of "the splitting field" of a polynomial f over k.

Let k be a field and let K, K' be extensions of k. A one-one homomorphism $\sigma\colon K \to K'$ such that $\sigma|k =$ identity is called a k-isomorphism of K into K'.

Proposition 3.15 *Let K be the splitting field of a polynomial f over a field k and let L/K be any extension. Then, for any k-isomorphism σ of K into L, we have $\sigma(K) = K$.*

PROOF: For, let $\alpha_1, \ldots, \alpha_n$ be the roots of f in K. Since $\sigma(\alpha_i)$ is also a root of f and since f can have at most n roots in L, we must have $\sigma(\alpha_i) = \alpha_j$ for some j. Since σ is one-one, it permutes the elements $\alpha_1, \ldots, \alpha_n$. Hence $\sigma(K) = K$.

Proposition 3.16 *Let K be the splitting field of polynomial f over k and let ϕ be an irreducible polynomial over k. If ϕ has a root in K, then ϕ is a product of linear factors in K. Conversely, if K/k is a finite extension which is such that any irreducible polynomial over k having a root in K is a product of linear factors in K, then K is the splitting field of some polynomial over k.*

PROOF: Let $K = k(\alpha_1, \ldots, \alpha_n)$ be the splitting field of f where $\alpha_1, \ldots, \alpha_n$ are the roots of f. Let $\beta \in K$ be a root of ϕ and let L be the splitting field of ϕ over K. Let β' be any root of ϕ in L. We have a k-isomorphism $\sigma: k(\beta) \approx k(\beta')$ such that $\sigma(\beta) = \beta'$. Since the splitting field of f (resp. $\sigma(f) = f$) over $k(\beta)$(resp. $k(\beta')$) is $K(\beta) = k(\beta, \alpha_1, \ldots, \alpha_n) = K$ (resp. $K(\beta') = k(\beta', \alpha_1, \ldots, \alpha_n)$), σ can be extended to a k-isomorphism of K onto $K(\beta')$. Since K is a splitting field, it follows by Proposition 3.15 that this k-isomorphism is an automorphism of K, i.e. $K = K(\beta')$ or $\beta' \in K$.

Suppose now that K/k is a finite extension such that any irreducible polynomial which has a root in K is a product of linear factors in K. Let $K = k(\alpha_1, \ldots, \alpha_n)$ and let $f_1, \ldots, f_n$ denote the minimal polynomials of $\alpha_1, \ldots, \alpha_n$ respectively. Clearly, K is the splitting field of $\prod_{1 \le i \le n} f_i$.

Definition 3.17 A normal extension K/k is an algebraic extension such that any irreducible polynomial over k which has a root in K is a product of linear factors in K.

It follows from Proposition 3.16 that finite normal extensions are precisely splitting fields.

Proposition 3.18 *Let K/k be a finite extension. Then there exists a finite normal extension L/k such that K is a subfield of L. Let K_i/k, $i = 1, 2, \ldots, n$ be finite extensions. Then there exists a finite normal extension L/k and k-isomorphisms σ_i of K_i into L.*

PROOF: For, let $K = k(\alpha_1, \ldots, \alpha_n)$ and let f_i, $1 \le i \le n$, be the minimal polynomial of α_i over k. The splitting field of $\phi = \prod_{1 \le i \le n} f_i$ considered as a polynomial over K is easily seen to be the splitting field of ϕ over k and we may take L to be this field.

Let now K_i/k, $1 \le i \le n$, be finite extensions. Let N_i/k, $1 \le i \le n$, be finite normal extensions such that K_i is a subfield of N_i for $1 \le i \le n$. Let N_i be the splitting field of ϕ_i over k. Let $\phi = \prod_{1 \le i \le n} \phi_i$. We take L to be the splitting field of ϕ over k. Since ϕ_i splits in L, L contains a splitting field of ϕ_i $(1 \leq i \leq n)$. Hence there exists a k-isomorphism of N_i (and hence K_i) onto L.

Example 3.19 Let α be a root of $X^3 - 2 \in \mathbf{Q}[X]$. Then $\mathbf{Q}(\alpha)/\mathbf{Q}$ is *not* a normal extension.

Example 3.20 The field $\mathbf{C}$ of complex numbers is such that every non-constant polynomial with coefficients in $\mathbf{C}$ has a root in $\mathbf{C}$ ("Fundamental Theorem of Algebra"), i.e. $\mathbf{C}$ contains a splitting field of any polynomial in $\mathbf{C}[X]$. Such fields are said to be *algebraically closed.*

3.3 Separable extensions

Definition 3.21 Let k be a field. An irreducible polynomial $f \in k[X]$ is called separable if all its roots (in the splitting field) are simple. Otherwise, f is called inseparable. A non-constant polynomial $f \in k[X]$ is called separable if all its irreducible factors are separable.

Let K/k be an algebraic extension. An element $\alpha \in K$ is called separable over k if the minimal polynomial of α over k is separable. An element $\alpha \in K$ which is not separable will be called *inseparable.* An algebraic extension K/k will be called *separable* if all its elements are separable over k, otherwise it is called *inseparable.*

If $\alpha \in K$ is separable over k, α is separable over any L with $K \supset L \supset k$. In fact the minimal polynomial g of α over L divides the minimal polynomial f of α over k. Since f is separable, it follows that g is separable.

Before treating separable extensions further, we introduce some results on roots of polynomials.

Let $f \in k[X]$ and let $f = \sum_{0 \leq i \leq n} a_i X^i$. We define the *derivative* of f, denoted by f', by $f' = \sum_{1 \leq i \leq n} i a_i X^{i-1}$. The following properties are then easily verified; we suppose that $f,\ g \in k[X]$ and $a \in k$.

(i) If $f \in k$, then $f' = 0$,

(ii) $(f+g)' = f' + g'$,

(iii) $(fg)' = fg' + f'g$,

(iv) $(af)' = af'$.

Let $\alpha \in k$ be a root of a polynomial f. Let $f = (X - \alpha)g$. We then have

$$f' = (X - \alpha)g' + g.$$

This gives $g(\alpha) = f'(\alpha)$.

Proposition 3.22 *Let $f \in k[X]$ be a non-constant polynomial with α as a root. Then α is a multiple root if and only if $f'(\alpha) = 0$.*

Proof: Let $f = (X - \alpha)g$. Clearly, α is a multiple root of f if and only if $g(\alpha) = 0$. Since $f'(\alpha) = g(\alpha)$, the proposition follows.

Corollary 3.23 *Let f be an irreducible polynomial. Then f has a multiple root if and only if $f' = 0$.*

Proof: We may suppose that f is monic. Let α be a root of f. By the above corollary α is a multiple root of f if and only if it is a root of f'. Since f is the minimal polynomial of α, this is the case if and only if $f|f'$. If $f' \neq 0$, we have $\deg f' < \deg f$ and f cannot divide f'.

Corollary 3.24 *Any irreducible polynomial f over a field of characteristic 0 is separable. An irreducible polynomial f over a field k of characteristic $p > 0$, is inseparable if and only if there exists $g \in k[X]$ such that $f(X) = g(X^p)$.*

Suppose f is inseparable. Let $f = \sum_{0 \leq i \leq n} a_i X^i$. In view of Corollary 3.23, we must have $\sum_{1 \leq i \leq n} i a_i X^{i-1} = 0$, which implies that $i a_i = 0$ for $1 \leq i \leq n$. If k is of characteristic 0, this implies that $a_i = 0$ for $i \geq 1$. If k is of characteristic $p \neq 0$, and if $a_i \neq 0$, we have $p|i$.

Remark 3.25 Let k be a field of characteristic 0. Then any algebraic extension of k is separable.

Remark 3.26 Let k be a field of characteristic $p \neq 0$ having an element α such that the polynomial $f = X^p - \alpha$ has no root in k. Then we assert that $X^p - \alpha$ is an irreducible polynomial over k which is inseparable over k. Let β_1, β_2 be two roots of this polynomial (in a splitting field). Then $\beta_1^p = \beta_2^p = \alpha$ and hence $\beta_1 = \beta_2$. Thus all the roots of this polynomial are equal, say, to β. Let g be the minimal polynomial of β. If h is any monic irreducible factor of f, we have $h(\beta) = 0$ and hence $g = h$. There is thus an integer i such that $f = g^i$. This equation implies that $p = ni$, where $n =$ degree of g. Since g is not linear $n \neq 1$. Hence $i = 1$.

In particular, let $k(x)$ be the field of rational functions in one variable x over a field of characteristic $p \neq 0$. Then $X^p - x$ is an irreducible inseparable polynomial over $k(x)$. For, if $X^p - x$ has a root in $k(x)$ there exist $g,\ h \in k[X]$ with $x = (g/h)^p$,i.e. $xh^p = g^p$. But this implies that $p \deg h + 1 = p \deg g$, which is impossible. Thus there exist inseparable algebraic extensions.

Lemma 3.27 *Let K/k and L/K be finite extensions. Let N/k be a finite normal extension of k such that L is a subfield of N. Let m be the number of (distinct) k-isomorphisms of K into N and let n be the number of (distinct) K-isomorphisms of L into N. Then the number of distinct k-isomorphisms of L into N is mn.*

Proof: Let $(\sigma_i)_{1 \leq i \leq m}$ be the distinct k-isomorphisms of K into N, and let $(\tau_j)_{1 \leq j \leq n}$ be the distinct K-isomorphisms of L into N, For $1 \leq i \leq m$ let $\bar{\sigma}_i$ be an extension of σ_i to an automorphism of N; (this exists by Proposition 3.13). We assert that $\bar{\sigma}_i \circ \tau_j$ are distinct. Suppose $\bar{\sigma}_i \circ \tau_j(x) = \bar{\sigma}_i \circ \tau_s(x)$ for every $x \in L$. Therefore, for every $x \in K$, we get $\sigma_i(x) = \sigma_r(x)$, which implies that $i = r$. Therefore $\tau_j(x) = \tau_s(x)$ for every $x \in L$ which implies that $j = s$. Let θ be any k-isomorphisms of L into N, Clearly $\theta|K = \sigma_i$ for some i.Then $(\bar{\sigma}_i)^{-1} \circ \theta|K =$ identity. Thus $(\bar{\sigma}_i)^{-1} \circ \theta = \tau_j$ for some j. Hence $\theta = \bar{\sigma}_i \circ \tau_j$.

Proposition 3.28 *Let K/k be an extension of degree n and N/k a finite normal extension such that K is a subfield of N. Then there are at most n distinct k-isomorphisms of K into N.*

Proof: We prove the proposition by induction on $(K{:}\,k)$. If $(K{:}\,k) = 1$, there is nothing to prove. Assume that $(K{:}\,k) > 1$. Choose $\alpha \in K$ with $\alpha \notin k$. Then $[K{:}\,k(\alpha)] < (K{:}\,k)$. Hence, by induction, the number of distinct $k(\alpha)$-isomorphisms of K into N is at most $[K{:}\,k(\alpha)]$. On the other hand, for any $\alpha \in K$, the number of (distinct) conjugates of α is at most equal to the degree of the minimal polynomial of α. Since any k-isomorphism of $k(\alpha)$ into N takes α into a conjugate of α and, given a conjugate $\beta \in N$, there exists a unique k-isomorphism of $k(\alpha)$ into N which maps α on β, it follows that the number of distinct k-isomorphism of $k(\alpha)$ into N is at most $[k(\alpha){:}\,k]$. The proposition now follows from the lemma above.

Proposition 3.29 *A finite extension K/k of degree n is separable if and only if for any finite normal extension N/k such that K is a subfield of N, there are n distinct k-isomorphisms of K into N.*

PROOF: Let K/k be separable. Let K be a subfield of any finite normal extension N of k. We prove the assertion by induction on n. If $n = 1$, there is nothing to prove. Let $n > 1$. Choose $\alpha \in K$, $\alpha \notin k$. Then $[K\colon k(\alpha)] < n$ and since $K/k(\alpha)$is separable, the number of distinct $k(\alpha)$-isomorphisms of K into N is precisely $[K\colon k(\alpha)]$. On the other hand, since α is separable, all the roots of its minimal polynomial are simple and hence the number of distinct k-isomorphisms of $k(\alpha)$ into N is $[k(\alpha)\colon k]$. The lemma above now proves the assertion.

Conversely, suppose K/k has n-distinct isomorphisms into a finite normal extension N/k containing K as a subfield. Let $\alpha \in K$. By Proposition 3.28, the number of distinct $k(\alpha)$-isomorphisms of K into N is at most $[K : k(\alpha)]$. Also, the number of k-isomorphisms of $k(\alpha)$ into N is at most $[k(\alpha) : k]$. Since $n = [K : k(\alpha)][k(\alpha) : k]$, it follows that $[k(\alpha) : k] =$ number of distinct k-isomorphisms of $k(\alpha)$ into N, i.e. all the conjugates of α are distinct. Hence α is separable.

Corollary 3.30 *If K/k is a finite separable extension and L/K is a finite separable extension, then L/k is separable.*

In view of the lemma, it follows that the number of distinct k-isomorphisms of L into any normal extension N/k containing L as a subfield is equal to $(L : K)(K : k) = (L : k)$. Hence L/k is separable.

Corollary 3.31 *If $\alpha_1 \ldots, \alpha_n \in K$ are separable elements over k, then $k(\alpha_1, \ldots, \alpha_n)/k$ is separable.*

3.4 Finite fields

Let F be a finite field of characteristic $p \neq 0$. We know then that $F/(\mathbf{Z}/(p))$ is a finite extension. Let $(F : \mathbf{Z}/(p)) = n$. Let $\alpha_1, \ldots, \alpha_n \in F$ be a $\mathbf{Z}/(p)$-base for F. Then every element of F can be uniquely expressed as $\sum_{1\leq i\leq n} a_i\alpha_i$; $a_i \in \mathbf{Z}/(p)$. Since $\mathbf{Z}/(p)$ has p elements, it follows that F has p^n elements. Now $F^* = F - \{0\}$ is a group of order $p^n - 1$ and hence any non-zero element of F is a root of the polynomial $X^{p^n-1} - 1$. Thus any element of F satisfies the polynomial $X^{p^n} - X \in \mathbf{Z}/(p)[X]$. Since F has p^n elements, it follows that F is *the splitting field of the polynomial* $X^{p^n} - X$ over $\mathbf{Z}/(p)$. Since all the roots of this polynomial are distinct, it follows that F is a separable extension of $\mathbf{Z}/(p)$. In view of the uniqueness of splitting fields, it follows that *any* *two finite fields with the same number of elements are isomorphic.* It is also clear that any algebraic extension of a finite field is separable.

Proposition 3.32 *For any finite field F, $F^* = F - \{0\}$ is a cyclic group.*

PROOF: Let α be an element of F^* of maximum order, say, n. Then $\beta^n = 1$ for every $\beta \in F^*$ (Proposition 1.33, Chapter 1). Since the polynomial $X^n - 1$ has at most n roots, it follows that the order of $F^* \leq n$. However $1, \alpha, \ldots, \alpha^{n-1} \in F^*$. Hence F^* is generated by α.

Remark 3.33 Let F be a finite field with $1 = a_0, \ldots, a_n$ as its elements. Then the polynomial $f(X) = a_0 + \prod_{0 \leq i \leq n}(X - a_i)$ has no root in F. Thus a finite field is not algebraically closed.

3.5 Simplicity of finite separable extension

Theorem 3.34 *Let K/k be a finite separable extension. Then there exists an $\alpha \in K$ such that $K = k(\alpha)$ (i.e. any finite separable extension is simple).*

PROOF: CASE (i) *k is a finite field.* Then K being a finite extension of a finite field is finite. Hence K^* is a cyclic group by Proposition 3.32. Let α be a generator. We then have $K = k(\alpha)$.
CASE (ii) k is an *infinite field.* Let $(K : k) = n$. Let N/k be a finite normal extension containing K as a subfield. Since K/k is separable, it follows by Proposition 3.29 that there exist n distinct k-isomorphisms $\sigma_1, \ldots, \sigma_n$ of K into N. For each $i \neq j$, let $V_{ij} = \{x \in K \mid \sigma_i(x) = \sigma_j(x)\}$. Then V_{ij} is clearly a subspace of the k-vector space K. Since by assumption, $\sigma_i \neq \sigma_j$ for $i \neq j$, it follows that V_{ij} is a *proper* subspace of K. By Proposition 2.58, Chapter 2 $\bigcup_{i \neq j} V_{ij}$ is a proper subset of K. Hence there exists an $\alpha \in K$ such that $\sigma_i(\alpha) \neq \sigma_j(\alpha)$ for $i \neq j$. Thus α has n distinct conjugates, and we have $(k(\alpha) : k) = n$. Thus $K = k(\alpha)$.

Chapter 4

Fundamental Theorem of Galois Theory

LET K be a field. If σ_1 and σ_2 are two automorphism of K, then the mapping $\sigma_1 \circ \sigma_2 \colon K \to K$ defined by $(\sigma_1 \circ \sigma_2)(x) = \sigma_1(\sigma_2(x)),\ x \in K$, is again an automorphism of K. Thus if A is the set of all automorphisms of K, it is easily verified that A is a group with the group operation $\phi \colon A \times A \to A$ defined by $\phi(\sigma_1, \sigma_2) = \sigma_1\sigma_2 = \sigma_1 \circ \sigma_2$. We say that G is a *group of automorphisms* of K if G is a subgroup of A. Let k be a subfield of K. Then we denote by $G(K/k)$ the subset of A formed by the k-automorphisms of K, i.e. an element of A belongs to $G(K/k)$ if and only if $\sigma(x) = x$ for every $x \in k$. We see that $G(K/k)$ is a subgroup of A.

An extension K/k of fields is said to be a Galois extension if it is finite, normal and separable. Then the group $G(K/k)$ of k-automorphisms of K is called the *Galois group* of K over k.

If G is a group of automorphisms of a field K, then the set k of elements $x \in K$ such that $\sigma(x) = x$ for every $\sigma \in G$, is a subfield of K, called the *fixed field* of G.

Let G be a group of automorphism of a field K and $f = \sum_{i=0}^{n} a_i X^i$ be a polynomial over K. Then if $\sigma \in G$, we define the polynomial $\sigma(f)$ by $\sigma(f) = \sum_{i=0}^{n} \sigma(a_i) X^i$. If $\sigma(f) = f$ for every $\sigma \in G$, the coefficients a_i belong to the fixed field k of G.

Proposition 4.1 *Let K/k be a Galois extension. Then $G(K/k)$ is a finite group of order $(K : k)$ and k coincides with the fixed field of $G(K/k)$.*

This is an immediate consequence of the results proved in the last chapter. It follows from Proposition 3.15 and 3.29 of Chapter 3 that $G(K/k)$ is finite and order of $G = (K : k)$. To prove that k coincides with the fixed field of $G(K/k)$, we may assume that $K \neq k$. Now if α is an element of K not belonging to k, there exists an element $\beta \in K$, $\alpha \neq \beta$, such that α and β are conjugate over k, since K/k is normal and separable (Sections 2 and 3, Chapter 3). Now $k(\alpha)$ and $k(\beta)$ are k-isomorphic and since this isomorphism can be extended to a k-automorphism of K (Proposition 3.13, Chapter 3), there exists an element $\sigma \in G(K/k)$ such that $\sigma(\alpha) = \beta$. This shows that the fixed field of $G(K/k)$ is k.

The following theorem is in some sense a converse of Proposition 4.1.

Theorem 4.2 *Let H be a finite group of automorphisms of a field K. Then if k is the field of H, K/k is a Galois extension and $H = G(K/k)$.*

Let $\sigma_1, \dots, \sigma_n$ be the distinct elements of H. Let α be an element of K, and $\beta_1, \dots, \beta_m$ be the distinct elements among $\sigma_1(\alpha), \dots, \sigma_n(\alpha)$. Now if σ is an element of $H, \sigma(\beta_1), \dots, \sigma(\beta_m)$ are again distinct, since σ is an automorphism. Further $\sigma\sigma_1, \dots, \sigma\sigma_n$ is a permutation of $\sigma_1, \dots, \sigma_n$, from which it follows that $\sigma(\beta_1), \dots, \sigma(\beta_m)$ is a permutation of $\beta_1, \dots, \beta_m$. Consider the polynomial $f \in K[X]$ defined by $f = \prod_{i=1}^{m}(X - \beta_i)$. We have $\sigma(f) = \prod_{i=1}^{m}(X - \sigma(\beta_i)) = \prod_{i=1}^{m}(X - \beta_i) = f$, for every $\sigma \in H$. It follows that f is a polynomial over k. All the roots of f lie in K and are distinct; therefore f is a separable polynomial over k. Further, f is irreducible over k. In fact, if g is the minimal polynomial of α over k, we have $g(\sigma_i(\alpha)) = \sigma_i(g(\alpha)) = 0$. Thus $\deg g \geq \deg f$. Since $g|f$, we have $f = g$. Since $f(\alpha) = 0$, α is algebraic and separable over k and $(k(\alpha) : k) \leq n =$ order of H. It follows that K/k is an algebraic, separable extension.

Let N/k be a finite extension such that N is a subfield of K. Then since N/k is separable, $N = k(\beta)$, for some $\beta \in K$ (Theorem 3.34, Chapter 3.) Thus we have $(N : k) \leq n$. We choose now N such that N/k is finite and $(N : k)$ is maximum among all subfields of K containing k and finite over k. We have $N = k(\alpha)$. Let now θ be any element of K. Let M be the subfield of K generated by N and θ. Then M/k is finite (Corollary 3.4, Proposition 3.3, Chapter 3) and therefore by the choice of N, we have $(M\colon k) \leq (N\colon k)$. But M contains N so that $(M\colon k) = (N\colon k)(M\colon N)$. (Proposition 3.3, Chapter 3). It follows that $(M : N) = 1$ and thus $M = N$. Therefore every element of K

belongs to N, i.e. $K = N$. We have therefore proved that K/k is a finite separable extension. Now $K = k(\alpha)$ and since $\sigma_1, \ldots, \sigma_n$ are distinct k-automorphisms of K, $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$ are distinct. Therefore the polynomial $f = \prod_{i=1}^{n}(X - \sigma_i(\alpha))$ over k of degree n, is the minimal polynomial of α over k and K is obviously the splitting field of f. We have $H \subset G(K/k)$ and order of $G(K/k) = n$ (Proposition 3.28, Chapter 3). Therefore $H = G(K/k)$. This concludes the proof of the theorem.

Let K/k be a Galois extension. Let $S(K/k)$ denote the set of subfields of K containing k and $S(G)$ denote the set of subgroups of $G = G(K/k)$. We define mappings:

$$\Phi \colon S(K/k) \to S(G)$$

$$\Psi \colon S(G) \to S(K/k)$$

as follows: if K_1 is an element of $S(Kk)$, i.e. a subfield of K containing k, K/K_1 is also a Galois extension (the finitness and separability of K/K_1 are immediate; to show that K/K_1 is normal, we can use the fact that K is the splitting field of a polynomial f over k and a fortiori K is the splitting field of f over K_1, so that the normality of K/K_1 follows). Now we set $\Phi(K_1) = G(K/K_1)$. If H is a subgroup of G, we denote by $\Psi(H)$ the fixed field of H.

Theorem 4.3 *(Fundamental theorem of Galois Theory.) The maps $\Phi \circ \Psi \colon S(G) \to S(G)$ and $\Psi \circ \Phi \colon S(K/k) \to S(K/k)$ are identity mappings.*

Proof: That $\Psi \circ \Phi \colon S(K/k) \to S(K/k)$ is the identity map, is equivalent to the statement that if K_1/k is an extension such that K_1 is a sub-field of K, then K_1 is the fixed field of $G(K/K_1)$. This results from Proposition 4.1. That $\Phi \circ \Psi \colon S(G) \to S(G)$ is the identity map, is equivalent to the assertion that if H is a subgroup of G and K_1 the fixed field of H, we have $H = G(K/K_1)$. This results from Theorem 4.2.

Corollary 4.4 *Let K_1/k be an extension such that K_1 is a subfield of K. Then K_1/k is a Galois extension if and only if $G(K/K_1)$ is a normal subgroup of $G(K/k)$ and then there is a natural isomorphism of $G(K_1/k)$ onto the quotient group $G(K/k)/G(K/K_1)$.*

If σ is an element of $G(K/k)$, then $\sigma(K_1)$ is again a subfield of K containing k and $G(K/\sigma(K_1))$ is the subgroup of $\sigma G(K/K_1)\sigma^{-1}$ of $G(K/k)$, as is verified easily. Now K_1/k is normal if and only if $\sigma(K_1) = K_1$ for every $\sigma \in G(K/k)$ (this follows from Proposition 3.15, Chapter 3). Now if $\sigma(K_1) = K_1$, $\sigma G(K/K_1)\sigma^{-1} = G(K/K_1)$ for every $\sigma \in G(K/k)$, which shows that $G(K/K_1)$ is a normal subgroup of $G(K/k)$. Conversely if $\sigma G(K/K_1)\sigma^{-1} = G(K/K_1)$ for every $\sigma \in G(K/k)$, the fixed field of $G(K/K_1)$ is the same as that of $\sigma G(K/K_1)\sigma^{-1}$ for every $\sigma \in G(K/K_1)$. By Proposition4.1 the fixed field of $G(K/K_1)$ is K_1 and that of $\sigma G(K/K_1)\sigma^{-1}$ is $\sigma(K_1)$. Therefore $K_1 = \sigma(K_1)$ for every $\sigma \in G(K/k)$, which shows that K_1 normal. This completes the proof of the first part of the corollary.

Suppose now that K_1 is an extension of $k, K \supset K_1 \supset k$, such that K_1/k is normal. We have seen that if $\sigma \in G(K/k)$, we have $\sigma(K_1) = K_1$. We thus get a mapping $f\colon G(K/k) \to G(K_1/k)$, namely, if σ is in $G(K/k)$, $f(\sigma)$ is the restriction of σ to K_1. It is verified easily that f is a homomorphism of groups. Further f is onto, because every k-automorphism of K_1 can be extended to a k-automorphism of K (Proposition 3.13, Chapter 3). The kernel of f is precisely $G(K/K_1)$ so that $G(K/k)/G(K/K_1)$ is naturally isomorphic to $G(K_1/k)$, q.e.d.

Let K_1/k and K_2/k be two extensions of a field k such that K_1 and K_2 are again contained in an extension N of k. We denote by K_1K_2 the subfield of N generated by K_1 and K_2 (the extension K_1K_2/k is often called a *composite of* K_1/k and K_2/k over k.) We note that $K_1K_2 \supset K_1$, $K_1K_2 \supset K_2$.

Proposition 4.5 *Let K_1/k be a Galois extension, then K_1K_2/K_2 is also a Galois extension. Further there is a natural group homomorphism $f\colon G(K_1K_2/K_2) \to G(K_1/k)$ such that the kernel of f reduces to the identity element, i.e. $G(K_1K_2/K_2)$ can be identified with a subgroup of $G(K_1/k)$.*

The field K_1 is the splitting field of a separable polynomial h over k. Since K_2 contains k, h can also be considered as a polynomial over K_2 and then we see that K_1K_2 is the splitting field of the polynomial h over K_2. From this it follows that K_1K_2/K_2 is a Galois extension.

Let σ be an element of $G(K_1K_2/K_2)$. Since $\sigma(x) = x$ for every $x \in K_2$, a fortiori $\sigma(x) = x$ for every $x \in k$. Further since K_1/k is a normal extension, $\sigma(K_1) = K_1$. We thus get a mapping $f\colon G(K_1K_2/K_2) \to G(K_1/k)$, namely if $\sigma \in G(K_1K_2/K_2)$, $f(\sigma)$ is the restriction of σ to K_1. Further if $\sigma \neq$ identity, $f(\sigma)$ is not the identity element of K_1/k, for then σ would be the identity automorphism of K_1K_2, since K_1K_2 is generated by K_1 and K_2. This completes the proof of the proposition.

Remark 4.6 In general f need not be onto; for example if $K_1 = K_2$, we have $K_1K_2 = K_2$. Then $G(K_1K_2/K_2)$ reduces to one element and we can choose K_1/K such that $G(K_1/k)$ consists of more than one element.

Theorem 4.7 *Let k be a finite field consisting of q elements and K a finite extension of k. Then K/k is a Galois extension and the Galois group $G(K/k)$ is cyclic. If $\sigma: K \to K$ is the mapping defined by $\sigma(a) = a^q,\ a \in K, \sigma$ is a k-automorphism and is a generator of $G(K/k)$.*

Let p be the characteristic of k and $\mathbf{Z}/(p)$ the prime field of characteristic p. We have $K \supset k \supset \mathbf{Z}/(p)$. We have seen that $K/\mathbf{Z}/(p)$ is a Galois extension (Section 4, Chapter 3). Therefore K/k is a Galois extension. Consider the mapping $\sigma: K \to K$ defined by $\sigma(a) = a^q$. If $a \in k,\ \sigma(a) = a$ since the multiplicative group k^* is of order $(q-1)$ and $a^{q-1} = 1,\ a \in k^*$, which gives $a^q = a$. If a is the zero element of k, we have obviously $a^q = a$. It is easily verified that σ is an automorphism of K. Let $m = (K : k)$. The group $G(K/k)$ is of order m and if we show that the element σ is of order m, it follows that $G(K/k)$ is cyclic and that σ is a generator of $G(K/k)$. We know that the multiplicative group K^* is cyclic (Proposition 3.32, Chapter 3); let α be a generator of K^*. Therefore the order of α is $(q^m - 1)$. We have $\sigma(\alpha) = \alpha^q$. Suppose that σ as an element of $G(K/k)$ is of order s i.e. $\alpha^{q^s} = \alpha$ and s is the least positive integer with this property. It follows that $s = m$ and therefore the theorem is proved.

Chapter 5

Applications of Galois Theory

NOTATION Let K be a field of characteristic p and m a positive integer. We write $[m, p] = 1$ if either of the following conditions is satisfied:

(1) $p = 0$ and m arbitrary,

(2) $p > 0$ and m and p are coprime.

5.1 Cyclic extensions

Let K be a field characteristic p and m an integer ≥ 1 such that $[m, p] = 1$.

Consider the polynomial $f = X^m - 1$ in $K[X]$. If ρ is any root of f, then $f'(\rho) = m\rho^{m-1} \neq 0$ so that all the roots of f are distinct (Proposition 3.22, Chapter 3). Let $\rho_1, \ldots, \rho_m$ be the roots of f. These are called the m-th *roots of unity.* They form an abelian group under multiplication. Let t be the exponent of this abelian group. Then $\rho_i^t = 1$ for $1 \leq i \leq m$ (Proposition 1.33, Chapter 1). Since $X^t - 1$ has only t roots in its splitting field over K, we see that $t = m$. This means that the ρ_i $(1 \leq i \leq m)$ form a cyclic group order m. Any generator of this group is called a *primitive m-th root of unity.* If ρ is primitive m-th root of unity, we have

$$f = X^m - 1 = \prod_{0 \leq i \leq m-1} (X - \rho^i),$$

and the field $L = K(\rho)$ is clearly the splitting field of f over K. The extension L/K is separable since all the roots of f are distinct. Thus L/K is a Galois extension.

Let G be the Galois group of L/K and $\sigma \in G$. If ρ is a primitive mth root of unity, so is $\sigma(\rho)$ and therefore $\sigma(\rho) = \rho^\nu$ where $(\nu, m) = 1$ and the integer ν is determined uniquely modulo m. Let R_m denote the multiplicative group of residue classes $\bmod\ m$ which are prime to m. It is easily verified that the map $\sigma \to \bar{\nu}$, where $\bar{\nu}$ is the residue class of $\nu \bmod\ m$, defines a homomorphism ϕ of G into R_m. If an element $\sigma \in G$ is such that $\sigma(\rho) = \rho$, we have $\sigma(\rho^i) = \rho^i,\ 0 \leq i \leq m-1$, and therefore σ is the identity element e of G. Thus $\ker\phi = (e)$ i.e. G is isomorphic to a subgroup of R_m. We have therefore proved the following.

Proposition 5.1 *Let L be the splitting field of $X^m - 1$ over K. Then $L = K(\rho)$ where ρ is a primitive m-th root of unity and L/K is a Galois extension whose Galois group is isomorphic to s subgroup of R_m.*

An extension F/E is called *cyclic* if it is a Galois extension with cyclic Galois group.

Remark 5.2 Let us assume that the integer m in Proposition 5.1 is a prime. Then R_m is cyclic (Proposition 3.32, Chapter 3). Hence G is also cyclic, i.e. L/K is cyclic.

Proposition 5.3 *Let the field K contain all the m-th roots of unity. Let L be the splitting field of the polynomial $f = X^m - \omega, \omega \in K$, over K. If $\alpha \in L$ is a root of f, we have $L = K(\alpha)$ and L/K is a cyclic extension. If m is a prime, either $L = K$ or $(L : K) = m$.*

Proof: We have

$$f = \prod_{0 \leq i \leq m-1} (X - \alpha\rho^i)$$

where ρ is a primitive mth root of unity. It follows that $L = K(\alpha)$. Since $[m, p] = 1,\ f$ is separable over K and thus L/K is a Galois extension.

Let G be the Galois group of L/K. We have, for any $\sigma \in G$, $\sigma(\alpha) = \alpha\rho^i$ for some integer i, which is determined uniquely modulo m. It is easily verified that the map $\sigma \to i(\text{modulo } m)$ defines a homomorphism ϕ of G into $\mathbf{Z}/(m)$ and that $\ker\phi = (e)$. Thus G is isomorphic to a subgroup of the cyclic group $\mathbf{Z}/(m)$ and hence G is cyclic. If m is a prime, $\mathbf{Z}/(m)$ has no subgroup other than (0) and $\mathbf{Z}/(m)$ so that $G = (e)$

or $G \approx \mathbf{Z}/(m)$. From this it follows that either $L = K$ or $(L : K) = m$ (Proposition 4.1, Chapter 4).

Proposition 5.4 *Let m be a prime and K contain all the m-th roots of unity. Let L/K be a cyclic extension such that $(L\colon K) = m$. Then there exists an element $\omega \in K$ such that L is the splitting field of $X^m - \omega$ over K.*

We require the following

Lemma 5.5 *Let ρ be a primitive m-th root of unity, m being a prime. Then, if a is an integer*

$$\sum_{0\le i\le m-1} \rho^{ia} = \begin{cases} 0 \text{ if } m \not| a \\ m \text{ if } m \mid a. \end{cases}$$

Proof of the Lemma If $m|a$, $\rho^{ia} = 1$ for every integer i. Hence $\sum_{0\le i\le m-1} \rho^{ia} = m$. If $m \not| a$, $\theta = \rho^a$ is again a primitive mth root of unity since m is prime. Therefore $\sum_{0\le i\le m-1} \rho^{ia} = \sum_{0\le i\le m-1} \theta^i =$ sum of the roots of the polynomial $X^m - 1$. Hence $\sum_{0\le i\le m-1} \rho^{ia} = 0$.

Proof of Proposition Since L/K is separable, $L = K(\beta)$ for some $\beta \in L$ (Theorem in Section 3.5, Chapter 3). Let f be the minimal polynomial of β over K. Then f splits into linear factors over L since L/K is normal; let $f = (X - \beta_1)\cdots(X - \beta_m)$, $\beta = \beta_1$. Let σ be a generator of the Galois group of L/K. We can assume, without loss of generality that $\sigma(\beta_i) = \beta_{i+1}$ for $1 \le i \le m-1$ and that $\sigma(\beta_m) = \beta_1$. Let $\alpha_k \in L$, $1 \le k \le m$, be defined as follows[1]

$$\alpha_k = \sum_{0\le i\le m-1} \rho^{ki}\beta_{i+1}.$$

By the above lemma, we have

$$\sum_{1\le k\le m} \alpha_k = \sum_{0\le i\le m-1} \beta_{i+1}\left(\sum_{1\le k\le m} \rho^{ki}\right) = m\beta_1.$$

Further $\alpha_m = \sum_{1\le i\le m} \beta_i$ and therefore belongs to K. Since $m\beta_1$ is not in K, it follows that there exists a k, $1 \le k \le m-1$ such that $\alpha_k \notin K$.

[1] The expression for α_k is called the *Lagrange resolvent*.

Let $\alpha = \alpha_k$. Now

$$\begin{aligned}
\sigma(\alpha) &= \sum_{0 \le i \le m-1} \rho^{ki} \sigma(\beta_{i+1}) \\
&= \sum_{0 \le i \le m-2} \rho^{ki} \beta_{i+2} + \rho^{k(m-1)} \beta_1 \\
&= \rho^{-k} \sum_{0 \le i \le m-1} \rho^{ki} \beta_{i+1} = \rho^{-k} \alpha.
\end{aligned}$$

so that $\sigma(\alpha^m) = (\sigma(\alpha))^m = \alpha^m$. Since σ generates G, $\tau(\alpha^m) = \alpha^m$ for every $\tau \in G$. Thus $\alpha^m = \omega \in K$. Since $(K(\alpha){:}\, K)$ divides m which is a prime, $(K(\alpha){:}\, K) = 1$ or m. Since $\alpha \notin K$, $(K(\alpha){:}\, K) = m$, so that $L = K(\alpha)$. It follows that L is the splitting field of $X^m - \omega$ over K, and our proposition is proved.

Corollary 5.6 *Let K be of characteristic $\neq 2$ and L/K an extension such that $(L{:}\, K) = 2$. Then there exists an element $\alpha \in L$ such that $\alpha^2 \in K$ and $L = K(\alpha)$.*

The proof is immediate.

Remark 5.7 Propositions 5.1 and 5.3 do not remain valid if we drop the condition that K all the mth roots of unity.

5.2 Solvability by radicals

Let K be a field of characteristic p. An extension L/K is said to be a *simple radical extension* if there exists an element α in L such that $\omega = \alpha^m \in K$, $[m, p] = 1$ and $L = K(\alpha)$. We sometimes write $\alpha = \omega^{1/m}$ and call α a *simple radical* over K. An extension L/K is said to be a *radical extension* if there exist subfields K_i $(1 \le i \le n)$ containing K such that $K_1 = K$, $K_n = L$, $K_{i+1} \supset K_i$ and K_{i+1}/K_i is a simple radical extension. Any element of L is called a *radical* over K.

If M/L and L/K are radical extensions then M/K is a radical extension. We note that a simple radical extension is finite and separable and therefore any radical extension is finite and separable. Let L/K be a radical extension, N/L any extension and F a subfield of N containing K. Then it is easily seen that LF/F is a radical extension, where LF is the field generated by L and F in N. From this it follows that if L/K is an extension and L_i $(i = 1, 2)$ are subfields of L containing K such that L_i/K is radical ($i = 1, 2$) then L_1L_2/K is a radical extension, since L_1L_2/L_1 and L_1/K are radical extensions. Now if L_i ($1 \leq i \leq l$) are a finite number of subfields of L containing K such that L_i/K is radical for $1 \leq i \leq l$, it is clear by induction on l that $(L_1L_2 \cdots L_l)/K$ is again a radical extension.

Proposition 5.8 *Let L/K be a radical extension. Then there exists an extension M/L such that M/K is a Galois radical extension.*

PROOF: Clearly it is sufficient to prove that there is a Galois radical extension M/K and a K-isomorphism of L onto a subfield of M.

The proof is by induction on $(L\colon K)$. If $(L\colon K) = 1$, there is nothing to prove. Suppose that $(L\colon K) = n > 1$. Then there exists a radical extension L_1/K such that $L = L_1(\alpha)$, $\alpha^m = a \in L_1$, $[m, p] = 1$ and $L \neq L_1$. Since $(L_1\colon K) < n$, by the induction hypothesis, there exists a Galois radical extension M_1/K such that L_1 is a subfield of M_1. Let G be the Galois group of M_1/K. Set

$$f = \prod_{\sigma \in G} (X^m - \sigma(a)).$$

Clearly $f \in K[X]$. Let M be the splitting field of f over M_1. It is obvious that M/M_1 is a radical extension an it follows that M/K is a radical extension. Further M/K is a Galois extension, for if M_1 is the splitting field of a polynomial ϕ over K, then M is the splitting field over K of the polynomial ϕf. The inclusion mapping of L_1 into M_1 can be extended to an isomorphism of $L = L_1(\alpha)$ into a subfield of M (cf. Section 2 of Chapter 3). This completes the proof of the proposition.

Proposition 5.9 *Let L/K be a Galois radical extension. Then the Galois group of L/K is solvable.*

PROOF: By the definition of a radical extension, there exist subfields K_i ($1 \leq i \leq n$) of L, such that $K_n = L$, $K_1 = K$ and $K_{i+1} = K_i(\beta_i)$, $\beta_i^{m_i} = a_i \in K_i$, $[m_i, p] = 1$ ($1 \leq i \leq n-1$). Let $m = \prod_{1 \leq i \leq n-1} m_i$. Clearly $[m, p] = 1$. Let L be the splitting field over K of a polynomial $f \in K[X]$. If M is splitting field over L of the polynomial $\phi = (X^m - 1)f$, it is also the splitting field of ϕ over K. Since ϕ is separable over K, it follows that M/K is a Galois extension. Let F be the subfield of M generated by K and the roots of $X^m - 1$. Let F_i ($1 \leq i \leq n$) be the subfield of M generated by F and K_i. We set $F_0 = K$. Clearly

$F_1 = F,\ F_n = M$ and $F_{i+1} = F_i(\beta_i)$ $(1 \leq i \leq n-1)$. Since F contains all the mth roots of unity, it follows that $F_{i+1}/F_i\,(1 \leq i \leq n-1)$ is a cyclic extension (Proposition 5.3).

We assert that the Galois group G of M/K is solvable. Let G_i be the subgroups of G having F_i, $1 \leq i \leq n$, as fixed fields. We have $G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_n = \{e\}$. Since $F_{i+1}/F_i\,(0 \leq i \leq n-1)$ are normal, it follows that G_{i+1} is a normal subgroup of G_i and that G_i/G_{i+1} can be identified with the Galois group of F_{i+1}/F_i, $0 \leq i \leq n-1$ (Corollary to Theorem 4.3, Chapter 4). By Proposition 5.1 G_0/G_1 is abelian and we have seen above that $G_i/G_{i+1}\,(1 \leq i \leq n-1)$ is cyclic. Thus we have a solvable series for G (Section 3, Chapter 1) so that G is solvable.

Since the Galois group of L/K can be identified with a quotient group of G (Corollaryto Theorem 4.3, Chapter 4), it follows that the Galois group of L/K is solvable (Proposition 1.56).

Proposition 5.10 *Let L/K be a Galois extension of degree n such that $G = G(L/K)$ is solvable. Suppose that $[n,p] = 1$. Then there exists an extension M/L such that M/K is a radical extension.*

Proof: We prove the proposition by induction on the order of G. If $G = \{e\}$, there is nothing to prove. Otherwise, there is a normal subgroup G_1 of G such that G/G_1 is cyclic of prime order (and the order of G_1 is then strictly less than that of G; Proposition 1.58, Chapter 1). Let L_1 be the fixed field of G_1. Then L/L_1 and L_1/K are Galois extension with Galois group G_1 and G/G_1 respectively (Theorem 4.3, Chapter 4). Let $m =$ order of G/G_1. Then $[m,p] = 1$. Let N be the splitting field of $X^m - 1$ over L and F the subfield of N generated by K and the roots of $X^m - 1$. Let L_1F (resp. LF) be the subfield of N generated by L_1 and F (resp. L and F).

Now L_1F/F is a Galois extension and $G(L_1F/F)$ is isomorphic to a subgroup of $G(L_1/K)$ (Proposition 4.5, Chapter 4). Since m is prime $G(L_1f/F) = \{e\}$ or it is a cyclic group of order m. Since F contains all the mth roots of unity, it follows that L_1F/F is a simple radical extension (Proposition 5.4.)

The extension LF/L_1F is Galois and $G(LF/L_1F)$ is isomorphic to a subgroup of $G(L/L_1)$ (Proposition 4.5, Chapter 4), since LF is the subfield of N generated by L and L_1F. It follows that $G(LF/L_1F)$ is solvable (Proposition 1.56, Chapter 1) and that if r is its order $[r,p] = 1$. Then, by the induction hypothesis, there is an extension M/LF such that M/L_1F is a radical extension. Since F/K is a radical extension, it follows that M/K is a radical extension. This completes the proof of the proposition.

Let $f \in K[X]$. Then f is said to be *solvable by radicals over* K if the splitting field of f over K is a subfield of a radical extension over K. It is easily seen that f is solvable by radicals over K if and only if every irreducible factor of f is solvable by radicals over K.

Theorem 5.11 *Let $f \in K[X]$ and L be the splitting field of f over K. Suppose that $[n,p] = 1$ where $n = (L\colon K)$. Then L/K is a Galois extension and f is solvable by radicals if and only if $G(L/K)$ is solvable.*

PROOF: Let α be any element of L. Let g be the minimal polynomial of α over K and m its degree. Since $m = (K(\alpha)\colon K)$, we have $m|n$ and $[m,p] = 1$. Therefore g is separable over K. Thus α is separable over K and it follows that L/K is a Galois extension. Suppose now that $G(L/K)$ is solvable. By Proposition 5.10, it follows that there exists an extension M/L such that M/K is a radical extension. Conversely let M/L be an extension such that M/K is a radical extension. Using Proposition 5.8, we may assume that M/K is a Galois radical extension. By Proposition 5.9, we see that $G(M/K)$ is solvable. Since $G(L/K)$ is isomorphic to a quotient group of $G(M/K)$, it follows that $G(L/K)$ is solvable.

Remark 5.12 If in the above theorem, f is such that $[m!, p] = 1$ where $m = \deg f$, it follows that $[n,p] = 1$.

5.3 Solvability of algebraic equations

Let H be a subgroup of the symmetric group S_n on the set $\{x_1, \ldots, x_n\}$. We say that H is *transitive* if given x_i, x_j there exists $\sigma \in H$ such that $\sigma(x_i) = x_j$.

Let $f \in K[X]$ and suppose that it is separable over K. Let L be the splitting field of f over K. Then L/K is a Galois extension. The group $G = G(L/K)$ is called the group of the polynomial f over K.

Suppose now that f is irreducible. Let $\alpha_1, \ldots, \alpha_n$ be its roots. For any root α_i of f and $\sigma \in G$, $\sigma(\alpha_i)$ is again a root of f, so that $\sigma(\alpha_i) = \alpha_j$ for some j. Thus σ induces a permutation $\bar{\sigma}$ of the set $\{\alpha_1, \ldots, \alpha_n\}$.

The map $\sigma \to \bar{\sigma}$ of G into the permutation group S_n as defined above, is clearly an isomorphism of G onto a subgroup of S_n. We identify G with its image under this mapping and thus regard G as a permutation group. The subgroup G of S_n is transitive, since given any two roots α_i, α_j there is a K-automorphism σ of L such that $\sigma(\alpha_i) = \alpha_j$ (Proposition 3.13, Chapter 3).

Theorem 5.13 *Let the characteristic p of the field K be different from 2 and 3 and $f \in K[X]$ be of degree ≤ 4. Then f is solvable by radicals over K.*

PROOF: We can assume that f is irreducible. If $n = \deg f$, we have $[n!, p] = 1$. Therefore, if L is the splitting field of f over K and $m = (L\colon K)$, we have $[m, p] = 1$. By what we have seen above, $G(L/K)$ can be identified with a subgroup of S_n, $n \leq 4$. Since S_n is solvable for $n \leq 4$ (Section 4, Chapter 1), it follows that $G(L/K)$ is solvable. (Proposition 1.56, Chapter 1). The theorem now follows from Theorem 5.11.

Given a field K, we ask the question whether there exists a separable polynomial over K which is not solvable by radicals over K. The answer is not always in the affirmative.

For instance, consider the following examples:

Example 5.14 Let $K = \mathbf{C}$, the field of complex numbers. The "Fundamental Theorem of Algebra" implies that any irreducible polynomial f over $\mathbf{C}$ is linear. This means that $\mathbf{C}$ is itself the splitting field of f over $\mathbf{C}$. Hence the group of f reduces to the identity element, in particular f is solvable by radicals!

Example 5.15 Let $K = \mathbf{R}$, the field of real numbers and f an irreducible polynomial over $\mathbf{R}$. Since $(\mathbf{C} : \mathbf{R}) = 2$ and f splits into linear factors in $\mathbf{C}$, it follows that the splitting of f over $\mathbf{R}$ is either $\mathbf{C}$ or $\mathbf{R}$. Hence the group of f is of order ≤ 2. Therefore f is solvable by radicals over $\mathbf{R}$.

Example 5.16 Let K be a finite field and L/K any finite extension. We know that L/K is cyclic (Theorem 4.7, Chapter 4). In particular $G(L/K)$ is solvable.

We shall now show, however, that there exist irreducible polynomials over the field $\mathbf{Q}$ of rational numbers such that their groups over $\mathbf{Q}$ are not solvable.

Proposition 5.17 *Let G be a transitive subgroup of the permutation group S_p, p being a prime. Suppose that G contains a transposition. Then $G = S_p$.*

Proof: We represent S_p as the permutation group of $I_p = \{1, 2, \dots, p\}$. Let H be the subgroup of G generated by the transpositions contained in G. Then $H \neq \{e\}$ and it is a normal subgroup of G, for if (i, j) is a transposition in G, we have $\sigma(i, j)\sigma^{-1} = (\sigma(i),\ \sigma(j))$ and if $\tau = \prod_{1\le k\le n} \tau_k$ where τ_k is a transposition in G, then $\sigma\tau\sigma^{-1} = \prod_{1\le k\le n}(\sigma\tau_k\sigma^{-1})$. We assert that H is a transitive subgroup of S_p. This fact is a consequence of the following.

Lemma 5.18 *Let G be a transitive subgroup of S_p, p being a prime. Then if H is a normal subgroup G such that $H \neq \{e\}$, it is also a transitive subgroup of S_p.*

Proof of the Lemma We introduce an equivalence relation in I_p as follows. We write $i \sim j$ if there exists $h \in H$ such that $h(i) = j$. Let $H(i)$ be the equivalence class containing $i \in I_p$. Then $H(i)$ is the subset $\{\sigma(i) \mid \sigma \in H\}$ of I_p. We assert that if i, j are in I_p, $H(i)$ and $H(j)$ have the same number of elements. In fact, there exist $\tau \in G$ such that $\tau(j) = i$ and we have $H(i) = H(\tau(j)) = \tau H(j)$ since H is normal. Since τ is a one-one mapping of I_p onto itself, $H(j)$ and $\tau H(j)$ have the same number of elements and the assertion follows. Since I_p is the disjoint union of the distinct equivalence classes $H(i)$, it follows that if m is the number of elements in $H(i)$, $m|p$. Since $H \neq \{e\}$, we have $m \neq 1$ and it follows that $m = p$. Hence $H(i) = I_p$, i.e. H is a transitive subgroup of G.

We now continue the proof of the proposition. There is a transposition $(i_1, i_2) \in H$. Let $i_2, \dots, i_q$ be these elements of I_p such that $(i_1, i_j) \in H,\ 2 \le j \le q$. We can assume without loss of generality, that $i_1 = 1,\ i_2 = 2, \dots i_q, = q$. If $q = p,\ H = S_p$ so that $G = S_p$ and the proposition is proved. Suppose that $q < p$. Then $(1, i) \in H$ for $1 \le i \le q$ and $(1, j) \notin H$ for $j > q$. Since H is transitive, there exists $\sigma \in H$ such that $\sigma(1) = p$. Now $\sigma = \tau_1 \dots \tau_h$ where $\tau_k, 1 \le k \le h$, are transpositions in H. Suppose that all the $\tau_k, 1 \le k \le h$, leave the set $\{1, \dots q\}$ invariant, i.e. if $1 \le i \le q$, then $1 \le \tau_k(i) \le q$ for every $k, 1 \le k \le h$. Then for every i with $1 \le i \le q$, we have $1 \le \sigma(i) \le q$, which is a contradiction. Therefore there is a $\tau_k, 1 \le k \le h$, which is of the form (i_1, i_2) with

$1 \le i_1 \le q$, and $i_2 > q$. Then we have

$$(1, i_1)(i_1, i_2)(1, i_1)^{-1} = (1, i_2) \in H$$

This leads to a contradiction. Thus $q = p$ and the proposition is proved.

Proposition 5.19 *Let $f \in \mathbf{Q}[X]$, where $\mathbf{Q}$ is the field of rational numbers such that* (1) $\deg f = p, p$ *being a prime,* (2)f *is irreducible and,* (3)f *has exactly* $(p-2)$ *real roots (in the field $\mathbf{C}$ of complex numbers). Then the group of f is S_p.*

PROOF: We assume that $p \ge 3$, since the proposition is trivial for $p = 2$. The map $\mathbf{C} \to \mathbf{C}$ defined by $z \to \bar{z}$, ($\bar{z}$ being the complex conjugate of z), is clearly an $\mathbf{R}$-automorphism of $\mathbf{C}$. Therefore if $\alpha \in \mathbf{C}$ is a root of a polynomial g with real coefficients, then $\bar{\alpha}$ is also a root of g.

Let $f = \prod_{1 \le i \le p}(X - \alpha_i)$ be such that α_i with $3 \le i \le p$ are real. We have $\alpha_2 = \bar{\alpha_1}$. Thus the mapping of $\mathbf{C}$ onto $\mathbf{C}$ defined by $z \to \bar{z}$ induces an automorphism σ of the splitting field of f over $\mathbf{R}$ and σ induces the transposition (α_1, α_2) on the set $\{\alpha_1, \dots \alpha_p\}$. Therefore the group of f contains a transposition and since it is transitive on $\{\alpha_1, \dots \alpha_p\}$ (f being irreducible), it follows that the group of f is S_p (Proposition 5.17).

Theorem 5.20 *For every prime p, there exists a polynomial $f \in \mathbf{Q}[X]$ whose group is S_p. In particular there exist polynomials over $\mathbf{Q}$ which cannot be solved by radicals over $\mathbf{Q}$.*

For $p = 2$, we may take f to be any irreducible polynomial of degree 2 over $\mathbf{Q}$ (for example $X^2 + 1$).

If $p \ge 3$, we construct an irreducible polynomial f of degree p over $\mathbf{Q}$ such that f has precisely $(p-2)$ real roots (in $\mathbf{C}$). Then by Proposition 5.19, it follows that the group of f is S_p.

If $p = 3$, we can take $f = X^3 - 2$. Clearly f is irreducible (for example, in view of Eisenstein's criterion (Proposition 2.39, Chapter 2)).

Let us assume that $p \ge 5$. Let $a_1, a_2, \dots, a_{p-2}$ be even integers such that

$$a_1 > a_2 > \cdots > a_{p-2}$$

and b a positive even integer. Let

$$g = (X^2 + b) \prod_{1 \le i \le p-2} (X - a_i).$$

Let $t_k = \frac{a_k + a_{k+1}}{2}$, $1 \le k \le p-3$. Clearly t_k is an integer. Also $(t_k^2 + b) \ge 2$. Further $|t_k - a_i| \ge 1 (1 \le i \le p-2)$ and at least for one i, $|t_k - a_i| > 1$, so that we have $g(t_k) > 2$, $1 \le k \le p-3$. Now, if $a_i > x > a_{i+1} (1 \le i \le p-3)$, $g(x) > 0$ or $g(x) < 0$ according as i is even or odd. Therefore $(g(t_k) - 2) > 0$ or $g(t_k) - 2 < 0$ according as k is even or odd $(1 \le k \le p-3)$. Now if x is sufficiently large, $g(x) - 2 > 0$ and $g(x) - 2 < 0$ for $x \le a_{p-2}$.

Thus if $f = g - 2$, f has at least $(p-2)$ real roots $\alpha_1, \dots, \alpha_{p-2}$ such that $\alpha_1 > t_1$, $t_i > \alpha_{i+1} > t_{i+1} (1 \le i \le p-4)$ and $t_{p-3} > \alpha_{p-2}$.

Let α_{p-1}, α_p be the remaining roots of f (in $\mathbf{C}$). We have

$$\begin{aligned} \sum_{1 \le i \le p} \alpha_i &= \sum_{1 \le i \le p-2} a_i = t \text{ (say)}; \\ \sum_{1 \le i < j \le p} \alpha_i \alpha_j &= b + \sum_{1 \le i < j \le p-2} a_i a_j = b + m \text{ (say)}. \end{aligned}$$

Then

$$\sum_{1 \le i \le p} \alpha_i^2 = t^2 - 2(b+m).$$

We now choose b such that $t^2 - 2(b+m) < 0$. Then f has only $(p-2)$ real roots.

We show now that f is irreducible. If $f = X^p + \sum_{1 \le i \le p} c_i X^{p-i}$, clearly $2 | c_i (1 \le i \le p)$ and $4 \nmid c_p$. The irreducibility of f is now a consequence of Eisenstein's criterion (Proposition 2.39, Chapter 2).

Finally, since for $p \ge 5$, S_p is not solvable, it follows that there exist polynomials over $\mathbf{Q}$ which are not solvable by radicals over $\mathbf{Q}$.

Remark 5.21 If $p = 5$, an example of a polynomial f over $\mathbf{Q}$ with S_5 as its group is obtained as follows. With the notation as in the proof of the theorem, we can take $a_1 = 2, a_2 = 0, a_3 = -2$ and $b = 6$. Then

$$g = (X^2 + 6)(X-2)X(X+2) \quad \text{and}$$

$$f = X^5 + 2X^3 - 24X - 2.$$

5.4 Construction with ruler and compass

Let $\mathbf{E}$ the plane, i.e. the set $\mathbf{R} \times \mathbf{R}$. We fix a system of rectangular axes for $\mathbf{E}$ and by the coordinates (x, y) of a point of $\mathbf{E}$, we mean the coordinates with respect to these axes. If S is a subset of $\mathbf{E}$, we set

$X(S) = \{x \in \mathbf{R} \mid (x, y) \in S \text{ for some } y \in \mathbf{R}\}$ and $Y(S) = \{y \in \mathbf{R} \mid (x, y) \in S \text{ for some } x \in \mathbf{R}\}$. We denote by $K(S)$ the subfield of $\mathbf{R}$ generated by $X(S) \cup Y(S)$.

Let S be a subset of $\mathbf{E}$ consisting of at least two points. We may assume, without loss of generality, that S contains $(0, 0)$ and $(1, 0)$. We say that S *is stable under constructions with ruler and compass (or S is stable)* if the following conditions are satisfied.

(1) If the line through A, B meets another line through C, D where $A, B, C, D \in S$ at a point E, then E is in S;

(2) If a point E of $\mathbf{E}$ is in the intersection of a circle with centre A passing through B, and the line through C and $D(A, B, C, D \in S)$, then E is in S.

(3) If a point E of $\mathbf{E}$ is in the intersection of circles with centres A and C passing through B and D respectively $(A, B, C, D, \in S)$, then E is in S.

Let S be *any* subset of the plane containing (0,0) and (1,0). Then the intersection of all stable subsets of $\mathbf{E}$ containing S is again stable. This set is called the *stable closure* of S and is denoted by $C(S)$.

Let K be a subfield of $\mathbf{R}$. It is said to be stable if i the square root of every positive element of K is in K is again stable. If K is *any* subfield of $\mathbf{R}$ the intersection of all stable subfields of $\mathbf{R}$ containing K is again stable. This field is called the stable closure of K and is denoted by $C(K)$.

Proposition 5.22 *Let S be a stable subset of $\mathbf{E}$. Then we have $X(S) = Y(S) = K(S)$ and $K(S)$ is a stable subfield of $\mathbf{R}$. Further, $(x, y) \in S$ if and only if x, y are in $X(S)$.*

Conversely, if K is a stable subfield of $\mathbf{R}$, the subset S of $\mathbf{E}$ defined by $S = \{(x, y) \mid x, y \in K\}$ is stable.

Proof: By the well-known constructions with ruler and compass, we see that (1) $(x, y) \in S$ if and only if $(x, 0), (0, x), (0, y), (y, 0)$ are in S; (2) if x, y are in $X(S)$, then $x - y$ and xy^{-1} (if $y \neq 0$) are in $X(S)$; and (3) if $x > 0$, and x is in $X(S)$, then $\sqrt{x}$ is in $X(S)$. The first part of the proposition is an easy consequence of these properties. The converse is an immediate consequence of the following:

(1) if the line through A, B intersects another line through C, D (where $A, B, C, D \in S$), at a point E, the coordinates of E are in $K(T)$; T being the subset of S consisting of A, B, C, D;

(2) if E belongs to the intersection of the circle with centre A passing through B, and the line through C, D (where $A, B, C, D \in S$), the coordinates of E are in an extension L of $K(T)$ such that $(L : K(T)) \leq 2$.

(3) if any point $E \in \mathbf{E}$ is in the intersection of circles with centres A and C, passing through B and D respectively, (where $A, B, C, D \in S$) then the coordinates of E are in an extension L of $K(T)$ such that $(L : K(T)) \leq 2$.

Remark 5.23 (1) Let S be the subset of $\mathbf{E}$ consisting of the two points (0,0) and (1,0). Then $C(S)$ is the set of points which is usually referred to as being constructible by ruler and compass given the unit length. In this case, we have $\mathbf{Q} = K(S)$.

(2) Let S be a subset of $\mathbf{E}$ containing (0,0) and (1,0). Then we have $K(C(S)) = C(K(S))$.

Let N/K be a radical extension. It is said to be of *type* 2 if there exist subfields N_i $(0 \leq i \leq n)$ of N containing K such that $N_0 = K, N_n = N, N_i \subset N_{i+1}$ and $(N_{i+1} : N_i) \leq 2$ $(0 \leq i \leq n-1)$. We note that if M/K is any extension and M_j $(1 \leq j \leq m)$ are subfields of M containing K such that $M_j/K (1 \leq j \leq m)$ are radical extensions of type 2, then the extension $(M_1 \ldots M_m)/K$ is again a radical extension of type 2.

Proposition 5.24 *Let K be a subfield of* $\mathbf{R}$ *and $x \in C(K)$. Then there exists a subfield L of $C(K)$ containing x and K such that L/K is a radical extension of type* 2.

PROOF: For every integer $i \geq 0$, we define inductively subfields K_i of $C(K)$ as follows : $K_0 = K, K_{i+1}$ is the subfield of $C(K)$ generated by K_i and the square roots of all the positive elements of K_i. Clearly $C(K) = \bigcup_{i \geq 0} K_i$.

The element $x \in K_i$ for some i. We prove the proposition by induction on i. Let us assume that the proposition is proved for all y in K_{i-1}. There exist elements $\theta_1, \ldots \theta_n$ in K_i such that $\theta_j^2 \in K_{i-1} (1 \leq j \leq n)$ and $x \in K_{i-1}(\theta_1, \ldots \theta_n)$. Then $x = f(\theta_1, \ldots, \theta_n)/g(\theta_1, \ldots, \theta_n)$, where

$$\begin{aligned} f(\theta_1, \ldots, \theta_n) &= \sum a_{i_1, \ldots, i_n} \theta_1^{i_1} \ldots \theta_n^{i_n}, \\ g(\theta_1, \ldots, \theta_n) &= \sum b_{j_1, \ldots, j_n} \theta_1^{j_1} \ldots \theta_n^{j_n}, g(\theta_1, \ldots, \theta_n) \neq 0 \end{aligned}$$

and $a_{i_1, \ldots, i_n}, b_{j_1, \ldots, j_n}$ are in K_{i-1}. By the induction hypothesis every one of the elements $a_{i_1, \ldots, i_n}, b_{j_1, \ldots, j_n}$ is contained in a subfield of $C(K)$ which is a radical extension of K of type 2. Thus, there exists a radical extension of L_1/K of type 2 containing all the $a_{i_1,\ldots,i_n}, b_{j_1,\ldots,j_n}$. We have $x \in L_1(\theta_1, \ldots, \theta_n)$ and $\theta_i^2 \in L_1 (1 \leq i \leq n)$. We take $L = L_1(\theta_1, \ldots, \theta_n)$; obviously L/L_1 is a radical extension of type 2 and thus L/K is a radical extension of type 2.

Theorem 5.25 *Let K be a subfield of $\mathbf{R}$. Then an element y of $\mathbf{R}$ is in $C(K)$ if and only if there is a Galois extension N/K such that $(N : K) = 2^m$ (for some integer m) and $y \in N$.*

PROOF: Let $y \in C(K)$. Then by Proposition 5.24, there exists a subfield M of $\mathbf{R}$ such that M/K is a radical extension of type 2 and y is in M. We assert that if M is any radical extension of type 2, there exists an extension N/M such that N/K is Galois and $(N : K) = 2^m$ for some m. In fact the required Galois extension is obtained by repeating the proof of Proposition 5.8 for this particular case.

Let now N/K be a Galois extension of degree 2^m such that y is in N. We can assume that N is a subfield of $\mathbf{C}$; for, N is the splitting field of a polynomial f over $K(y)$ and by the fundamental theorem of algebra, f splits into linear factors in $\mathbf{C}$, so that there is a $K(y)$-isomorphism of σ of N onto the subfield N' of $\mathbf{C}$ generated by $K(y)$ and the roots of f in $\mathbf{C}$. The group $G(N/K)$ has a solvable series:

$$G(N/K) = G_0 \supset G_1 \supset G_2 \cdots \supset G_n = (e)$$

such that G_{i+1} is a normal subgroup of G_i and G_i/G_{i+1} is of order 2 $(0 \leq i \leq n-1)$ (Propositions 1.57 and 1.58, Chapter 1). If K_i are the fixed fields of G_i we have $K_0 = K$, $K_n = N$ and $(K_{i+1} \colon K_i) = 2$. We prove by induction on i that $K_i \cap \mathbf{R} \subset C(K)$ for every i. Assume that $K_{i-1} \cap \mathbf{R} \subset C(K)$. We have $K_i = K_{i-1}(x)$, $x \in K_i$ and $x^2 \in K_{i-1}$. Therefore every element of K_i is of the form $a + bx$, $a, b \in K_{i-1}$. By the induction assumption, the real and imaginary parts of a, b and x^2 are in $C(K)$. Moreover if x is any complex number such that the real and imaginary parts of x^2 are in $C(K)$, it is easy to see that the real and imaginary parts of x are also in $C(K)$. Thus $K_i \cap \mathbf{R} \subset C(K)$. Since $y \in N \cap \mathbf{R}$, we have y is in $C(K)$ and the theorem is proved.

Example 5.26 *Trisection of an angle.* Let S be the set consisting of points $O = (0, 0), P = (1, 0)$ and $Q = (x, y)$ such that P and Q lie on the same circle C with centre O. Let θ be the angle $P\hat{O}Q$ and R be the point on C such that $P\hat{O}R$ is $\theta/3$. The problem is to decide whether any point on the line through O and R is in $C(S)$, or equivalently, whether

R is in $C(S)$. We have $R = (\cos\theta/3,\ \sin\theta/3)$ and R is in $C(S)$ if and only if $\cos\theta/3$ is in $C(K(S))$. Now $\cos\theta/3$ is a root of the polynomial $f = 4X^3 - 3X - \alpha$, where $\alpha = \cos\theta$. We can choose α such that $\alpha \in Q,\ 0 \le \alpha \le 1$ and f irreducible over Q (for example $\theta = \pi/3$). It is easy to see that f is irreducible also over $K(S)$. Then $\cos\theta/3$ for such a choice of α is not in $C(K(S))$, since $(K(S)(\cos\theta/3)\colon K(S)) = 3$.

Example 5.27 *Squaring the circle.* Let S be the set consisting of $O = (0,0)$ and $P = (1,0)$. Let $R = (x,0)$ be a point such that the area of the square whose base is OR, is equal to that of the circle with centre O and passing through P. The problem is to decide whether $R \in C(S)$ or, equivalently whether $x \in C(\mathbf{Q})$. We have $X^2 = \pi$. It is known that π is not algebraic over $\mathbf{Q}$. Since every element of $C(\mathbf{Q})$ is algebraic over $\mathbf{Q}$, $R \notin C(S)$; thus the unit circle cannot be squared.

Example 5.28 *Doubling the cube.* Let S consist of the points $O = (0,0)$ and $P = (1,0)$. Let $R = (x,0)$ be such that the volume of the cube with OR as an edge is equal to twice the volume of the cube with OP as an edge. The problem is to decide whether R is in $C(S)$ or, equivalently, whether $x \in C(\mathbf{Q})$. Clearly x is a root of the polynomial $f = X^3 - 2$. Since the group of f over $\mathbf{Q}$ is S_3, we have $R \notin C(S)$.

Example 5.29 *Construction of regular polygons with a given number of sides.* Let S be the set consisting of the points $O = (0,0)$ and $P = (1,0)$. Let Δ be a regular polygon with h sides, one of whose vertices is P and which is inscribed in the circle with centre O and radius OP. The problem is to decide whether the vertices of Δ are in $C(S)$; clearly this is equivalent to finding if $R = (\cos 2\pi/h,\ \sin 2\pi/h)$ is in $C(S)$. Let $\rho = \exp(2\pi i/h),\ i = \sqrt{-1}$. We have $\cos 2\pi/h = (\rho + \rho^{-1})/2$. Thus $(\mathbf{Q}(\rho) : (\cos 2\pi/h)) = 2$. Now $\mathbf{Q}(\rho)/\mathbf{Q}$ is a Galois extension since ρ is a primitive hth root of unity. Because of Theorem 5.25, we see that $R \in C(S)$ if and only if $(\mathbf{Q}(\rho) : \mathbf{Q}) = 2^m$ for some integer m.

Let us now suppose that h is a *prime*. We shall show that the vertices of Δ are in $C(S)$ if and only if h is a Fermat prime, i.e. $h = 2^{2^\lambda} + 1$ for some integer λ. Since

$$1 - X^h = (1 - X)(1 + X + \cdots + X^{h-1}),$$

ρ is a root of the polynomial $f = 1 + X \cdots + X^{h-1}$.

Set $X = Y + 1$. Then $f(X) = g(Y)$, where

$$g(Y) = Y^{h-1} + \binom{h}{1} Y^{h-2} + \cdots \binom{h}{h-1}.$$

Since h is a prime, h divides $\binom{h}{j}$, $1 \leq j \leq (h-1)$ and h^2 does not divide $\binom{h}{h-1} = h$. Hence by Eisenstein's criterion (Proposition 2.39, Chapter 2), g and hence f, is irreducible over $\mathbf{Q}$. Therefore, $(\mathbf{Q}(\rho) : \mathbf{Q}) = (h-1)$. Thus R is in $C(S)$ if and only if $h = 1 + 2^m$. It is easy to see (since h is a prime) that m is of the form 2^λ for some integer i.e. h is a Fermat prime. Setting $\lambda = 0, 1, 2$ we get $h = 3, 5, 17$ which are primes. Thus, an equilateral triangle, a pentagon and a 17-gon can be constructed by ruler and compass.

It is not known whether there exists an infinity of Fermat primes.

Bibliography

[1] E. ARTIN *Galois theory*, Notre Dame, Indiana, (1959).

[2] N. BOURBAKI *Algébre*, Chap. V, Hermann, Paris, (1950).

[3] N. JACOBSON *Lectures in Abstract Algebra*, Vol, III, Van Nostrand, Princeton, (1964).

[4] K. G. RAMANATHAN *Lectures on the Algebraic Theory of Fields*, Tata Institute of Fundamental Research, (1954).

[5] B. L. VAN DER WAERDEN *Modern Algebra*, Vol. I, Ungar, New York, (1948).