FIELDS AND GALOIS THEORY

J.S. MILNE

ABSTRACT. These are the notes for the second part of Math 594, University of Michigan, Winter 1994, exactly as they were handed out during the course except for some minor corrections.

Please send comments and corrections to me at jmilne@umich.edu using "Math594" as the subject.

v2.01 (August 21, 1996). First version on the web.

v2.02 (May 27, 1998). About 40 minor corrections (thanks to Henry Kim).

CONTENTS

1. Extensions of Fields

1.1. **Definitions.** A *field* is a set F with two composition laws $+$ and $\cdot$ such that

(a) $(F, +)$ is an abelian group;
(b) let $F^{\times} = F - \{0\}$; then $(F^{\times}, \cdot)$ is an abelian group;
(c) (distributive law) for all $a, b, c \in F$, $(a+b)c = ac + bc$ (hence also $a(b+c) = ab + ac$).

Equivalently, a field is a nonzero commutative ring (meaning with 1) such that every nonzero element has an inverse. A field contains at least two distinct elements, 0 and 1. The smallest, and one of the most important, fields is $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} = \{0, 1\}$.

Lemma 1.1. *A commutative ring R is a field if and only if it has no ideals other than* (0) *and R.*

Proof. Suppose R is a field, and let I be a nonzero ideal in R. If a is a nonzero element of I, then $1 = a^{-1}a \in I$, and so $I = R$. Conversely, suppose R is a commutative ring with no nontrivial ideals; if $a \neq 0$, then $(a) = R$, which means that there is a b in F such that $ab = 1$. □

Example 1.2. The following are fields: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

A *homomorphism* of fields $\alpha : F \to F'$ is simply a homomorphism of rings, i.e., it is a map with the properties

$$\alpha(a+b) = \alpha(a) + \alpha(b), \quad \alpha(ab) = \alpha(a)\alpha(b), \quad \alpha(1) = 1, \quad \text{all } a, b \in F.$$

Such a homomorphism is always injective, because the kernel is a proper ideal (it doesn't contain 1), which must therefore be zero.

1.2. **The characteristic of a field.** The map

$$\mathbb{Z} \to F, \quad n \mapsto 1_F + 1_F + \cdots + 1_F \quad (n\text{times}),$$

is a homomorphism of rings.

Case 1: Kernel $= (0)$; then $n \cdot 1_F = 0 \implies n = 0$ (in $\mathbb{Z}$). The map $\mathbb{Z} \to F$ extends to a homomorphism $\mathbb{Q} \hookrightarrow F$, $\frac{m}{n} \mapsto (m \cdot 1_F)(n \cdot 1_F)^{-1}$. Thus F contains a copy of $\mathbb{Q}$. In this case, we say that F has *characteristic zero.*

Case 2: Kernel $\neq (0)$, i.e., $n \cdot 1_F = 0$ some $n \neq 1$. The smallest such n will be a prime p (else F will have nonzero zero-divisors), and p generates the kernel. In this case, $\{m \cdot 1_F \mid m \in \mathbb{Z}\} \approx \mathbb{F}_p$, and F contains a copy of $\mathbb{F}_p$. We say that F has *characteristic* p.

The fields $\mathbb{F}_p$, p prime, and $\mathbb{Q}$ are called the *prime fields.* Every field contains a copy of one of them.

Remark 1.3. The binomial theorem

$$(a+b)^m = a^m + \binom{m}{1}a^{m-1}b + \cdots + \binom{m}{r}a^{m-r}b^r + \cdots + b^m$$

holds in any ring. If p is prime, then $p|\binom{p}{r}$ for all r, $1 \leq r \leq p-1$. Therefore, when F has characteristic p, $(a+b)^p = a^p + b^p$. Hence $a \mapsto a^p$ is a homomorphism $F \to F$, called the *Frobenius endomorphism* of F. When F is finite, it is an isomorphism, called the *Frobenius automorphism.*

1.3. **The polynomial ring $F[X]$.** I shall assume everyone knows the following (see Jacobson Chapter II, or Math 593).

(a) Let I be a nonzero ideal in $F[X]$. If $f(X)$ is a nonzero polynomial of least degree in I, then $I = (f(X))$. When we choose f to be monic, i.e., to have leading coefficient one, it is uniquely determined by I. There is a one-to-one correspondence between the nonzero ideals of $F[X]$ and the monic polynomials in $F[X]$. The prime ideals correspond to the irreducible monic polynomials.

(b) *Division algorithm*: given $f(X)$ and $g(X) \in F[X]$ with $g \neq 0$, we can find $q(X)$ and $r(X) \in F[X]$ with $\deg(r) < \deg(g)$ such that $f = gq + r$; moreover, $q(X)$ and $r(X)$ are uniquely determined. Thus the ring $F[X]$ is a Euclidean domain.

(c) *Euclid's algorithm*: Let f and $g \in F[X]$ have gcd $d(X)$; the algorithm gives polynomials $a(X)$ and $b(X)$ such that

$$a(X) \cdot f(X) + b(X) \cdot g(X) = d(X), \quad \deg(a) \leq \deg(g), \quad \deg(b) \leq \deg(f).$$

Recall how it goes. Using the division algorithm, we construct a sequence of quotients and remainders:

$$\begin{aligned} f &= q_0 g + r_0 \\ g &= q_1 r_0 + r_1 \\ r_0 &= q_2 r_1 + r_2 \\ &\cdots \\ r_{n-2} &= q_n r_{n-1} + r_n \\ r_{n-1} &= q_{n+1} r_n. \end{aligned}$$

Then $r_n = \gcd(f, g)$, and

$$r_n = r_{n-2} - q_n r_{n-1} = r_{n-2} - q_n(r_{n-3} - q_{n-1} r_{n-2}) = \cdots = af + bg.$$

Maple knows Euclid's algorithm—to learn its syntax, type "?gcdex;".

(d) Since $F[X]$ is an integral domain, we can form its field of fractions $F(X)$. It consists of quotients $f(X)/g(X)$, f and g polynomials, $g \neq 0$.

1.4. **Factoring polynomials.** It will frequently be important for us to know whether a polynomial is irreducible and, if it isn't, what its factors are. The following results help.

PROPOSITION 1.4. *Suppose $r = \frac{c}{d}$, $c, d \in \mathbb{Z}$, $\gcd(c, d) = 1$, is a root of a polynomial*

$$a_m X^m + a_{m-1} X^{m-1} + \cdots + a_0, \quad a_i \in \mathbb{Z}.$$

Then $c | a_0$ and $d | a_m$.

PROOF. It is clear from the equation

$$a_m c^m + a_{m-1} c^{m-1} d + \cdots + a_0 d^m = 0$$

that $d | a_m c^m$, and therefore, $d | a_m$. The proof that $c | a_0$ is similar. □

EXAMPLE 1.5. The polynomial $X^3 - 3X - 1$ is irreducible in $\mathbb{Q}[X]$ because its only possible roots are ± 1 (and they aren't).

PROPOSITION 1.6. *Let $f(X) \in \mathbb{Z}[X]$ be such that its coefficients have greatest common divisor* 1. *If $f(X)$ factors nontrivially in $\mathbb{Q}[X]$, then it factors nontrivially in $\mathbb{Z}[X]$; moreover, if $f(X) \in \mathbb{Z}[X]$ is monic, then any monic factor of $f(X)$ in $\mathbb{Q}[X]$ lies in $\mathbb{Z}[X]$.*

PROOF. Use Gauss's lemma (see Jacobson, 2.16, or Math 593). □

PROPOSITION 1.7. *(Eisenstein criterion) Let*

$$f = a_m X^m + a_{m-1} X^{m-1} + \cdots + a_0, \quad a_i \in \mathbb{Z};$$

suppose that there is a prime p such that:

p does not divide a_m,
p divides $a_{m-1}, ..., a_0$,
p^2 does not divide a_0.

Then f is irreducible in $\mathbb{Q}[X]$.

PROOF. We may remove any common factor from the coefficients f, and hence assume that they have gcd $= 1$. Therefore, if $f(X)$ factors in $\mathbb{Q}[X]$, it factors in $\mathbb{Z}[X]$:

$$a_m X^m + a_{m-1} X^{m-1} + \cdots + a_0 = (b_n X^n + \cdots + b_0)(c_r X^r + \cdots + c_0), \quad b_i, c_i \in \mathbb{Z}, \quad n, r < m.$$

Since p, but not p^2, divides $a_0 = b_0 c_0$, p must divide exactly one of b_0, c_0, say p divides b_0. Now from the equation

$$a_1 = b_0 c_1 + b_1 c_0,$$

we see that $p|b_1$. Now from the equation

$$a_2 = b_0 c_2 + b_1 c_1 + b_2 c_0,$$

we see that $p|b_2$. By continuing in this way, we find that p divides $b_0, b_1, \ldots, b_n$, which contradicts the fact that p does not divide a_m. □

The above three propositions hold with $\mathbb{Z}$ replaced by any unique factorization domain.

PROPOSITION 1.8. *There is an algorithm for factoring a polynomial in $\mathbb{Q}[X]$.*

PROOF. Consider $f(X) \in \mathbb{Q}[X]$. Multiply $f(X)$ by an integer, so that it is monic, and then replace it by $D^{\deg(f)} f(\frac{X}{D})$, $D =$ a common denominator for the coefficients of f, to obtain a monic polynomial with integer coefficients. Thus we need consider only polynomials

$$f(X) = X^m + a_1 X^{m-1} + \cdots + a_m, \quad a_i \in \mathbb{Z}.$$

From the fundamental theorem of algebra (see later), we know that f splits completely in $\mathbb{C}[X]$:

$$f(X) = \prod_{i=1}^{m} (X - \alpha_i), \quad \alpha_i \in \mathbb{C}.$$

From the equation $f(\alpha_i) = 0$, it follows that $|\alpha_i|$ is less than some bound M depending on $a_1, \ldots, a_m$. Now if $g(X)$ is a monic factor of $f(X)$, then its roots in $\mathbb{C}$ are certain of the α_i, and its coefficients are symmetric polynomials in its roots. Therefore the absolute values of the coefficients of $g(X)$ are bounded. Since they are also integers (by 1.6), we see that there are only finitely many possibilities for $g(X)$. Thus, to find the factors of $f(X)$ we (better Maple) only have to do a finite amount of checking. □

One other observation is sometimes useful: Suppose that the leading coefficient of $f(X) \in \mathbb{Z}[X]$ is not divisible by the prime p; if $f(X)$ is irreducible in $\mathbb{F}_p[X]$, then it is irreducible in $\mathbb{Z}[X]$. Unfortunately, this test is not always effective: for example, $X^4 - 10X^2 + 1$ is reducible[1] modulo every prime, but it is irreducible in $\mathbb{Q}[X]$.

[1] I don't know an elementary proof of this. One proof uses that its Galois group is $\approx (\mathbb{Z}/2\mathbb{Z})^2$.

Maple knows how to factor polynomials in $\mathbb{Q}[X]$ and in $\mathbb{F}_{|}[X]$. For example

`>factor(6*X^2+18*X-24)`; will find the factors of $6X^2 + 18X - 24$, and

`>Factor(X^2+3*X+3) mod 7`; will find the factors of X^2+3X+3 modulo 7, i.e., in $\mathbb{F}_7[X]$. Thus, we need not concern ourselves with the problem of factorizing polynomials in $\mathbb{Q}[X]$ or $\mathbb{F}_p[X]$.

1.5. **Extension fields; degrees.** A field E containing a field F is called an *extension (field)* of F. Such an E can be regarded (in an obvious fashion) as an F-vector space. We write $[E : F]$ for the dimension (possibly infinite) of E as an F-vector space, and call $[E : F]$ the *degree* of E over F. We often say that E is *finite* over F when it has finite degree over F.

Example 1.9. (a) The field of complex numbers $\mathbb{C}$ has degree 2 over $\mathbb{R}$ (basis $\{1, i\}$).

(b) The field of real numbers $\mathbb{R}$ has infinite degree over $\mathbb{Q}$. (We know $\mathbb{Q}$ is countable, which implies that any finite-dimensional vector space over $\mathbb{Q}$ is countable; but $\mathbb{R}$ is not countable. More explicitly, one can find real numbers α such that $1, \alpha, \alpha^2, \dots$ are linearly independent (see section 1.9 below)).

(c) The field of *Gaussian numbers* $\mathbb{Q}(i) =_{df} \{a + bi \in \mathbb{C} \mid a, b \in \mathbb{Q}\}$ has degree 2 over $\mathbb{Q}$ (basis $\{1, i\}$).

(d) The field $F(X)$ has infinite degree over F. (It contains the F-subspace $F[X]$, which has the infinite basis $\{1, X, X^2, \dots\}$.)

Proposition 1.10. *Let $L \supset E \supset F$ (all fields). Then L/F is of finite degree $\iff$ L/E and E/F are both of finite degree, in which case*

$$[L : F] = [L : E][E : F].$$

Proof. Assume that L/E and E/F are of finite degree, and let $\{e_i\}$ be a basis for E/F and $\{\ell_j\}$ a basis for L/E. I claim that $\{e_i\ell_j\}$ is a basis for L over F. I first show that it spans L. Let $\gamma \in L$. Then, because $\{\ell_j\}$ spans L as an E-vector space,

$$\gamma = \sum \alpha_j \ell_j, \qquad \text{some } \alpha_j \in E,$$

and because $\{e_i\}$ spans E as an F-vector space, for each j,

$$\alpha_j = \sum a_{ij} e_i, \qquad \text{some } a_{ij} \in F.$$

On putting these together, we find that

$$\gamma = \sum a_{ij} e_i \ell_j.$$

Next I show that $\{e_i\ell_j\}$ is linearly independent. A linear relation $\sum a_{ij}e_i\ell_j = 0$ can be rewritten $\sum_j(\sum_i a_{ij}e_i)\ell_j = 0$. The linear independence of the ℓ_j's now shows that $\sum_i a_{ij}e_i = 0$ for each j, and the linear independence of the e_i's now shows that each $a_{ij} = 0$.

Conversely, if L is of finite degree over F, then it is certainly of finite degree over E. Moreover, E, being a subspace of a finite dimensional F-space, is also finite dimensional. □

1.6. **Construction of some extensions.** Let $f(X) \in F[X]$ be a monic polynomial of degree m, and let (f) be the ideal generated by f. Consider the quotient ring $F[X]/(f(X))$, and write x for the image of X in $F[X]/(f(X))$, i.e., x is the coset $X + (f(X))$. Then:

(a) The map

$$P(X) \mapsto P(x) : F[X] \to F[x]$$

is a surjective homomorphism; we have $f(x) = 0$.

(b) From the division algorithm, we know each element g of $F[X]/(f)$ is represented by a unique polynomial r of degree $< m$. Hence each element of $F[x]$ can be written uniquely as a sum

$$a_0 + a_1 x + \cdots + a_{m-1}x^{m-1}, \qquad a_i \in F, \qquad (*).$$

(c) The addition of two elements, written in the form (*), is obvious.

(d) To multiply two elements in the form (*), multiply in the usual way, and use the relation $f(x) = 0$ to express the monomials of degree $\geq m$ in x in terms of lower degree monomials.

(e) Now assume $f(X)$ is irreducible. To find the inverse of an element $\alpha \in F[x]$, write α in the form (*), i.e., set $\alpha = g(x)$ where $g(X)$ is a polynomial of degree $\leq m-1$. Then use Euclid's algorithm in $F[X]$ to obtain polynomials $a(X)$ and $b(X)$ such that

$$a(X)f(X) + b(X)g(X) = d(X)$$

with $d(X)$ the gcd of f and g. In our case, $d(X)$ is 1 because $f(X)$ is irreducible and $\deg g(X) < \deg f(X)$. On replacing X with x in the equation, we find $b(x)g(x) = 1$. Hence $b(x)$ is the inverse of $g(x)$.

Conclusion: For any monic irreducible polynomial $f(X) \in F[X]$, $F[x] = F[X]/(f(X))$ is a field of degree m over F. Moreover, if we know how to compute in F, then we know how to compute in $F[x]$.

Example 1.11. Let $f(X) = X^2 + 1 \in \mathbb{R}[X]$. Then $\mathbb{R}[x]$ has:

elements: $a + bx$, $a, b \in \mathbb{R}$;

addition: obvious;

multiplication: $(a+bx)(a'+b'x) = (aa' - bb') + (ab' + a'b)x$.

We usually write i for x and $\mathbb{C}$ for $\mathbb{R}[x]$.

Example 1.12. Let $f(X) = X^3 - 3X - 1 \in \mathbb{Q}[X]$. This is irreducible over $\mathbb{Q}$, and so $\mathbb{Q}[x]$ has basis $\{1, x, x^2\}$ as a $\mathbb{Q}$-vector space. Let

$$\beta = x^4 + 2x^3 + 3 \in \mathbb{Q}[x].$$

Then using that $x^3 - 3x - 1 = 0$, we find that $\beta = 3x^2 + 7x + 5$. Because $X^3 - 3X - 1$ is irreducible,

$$\gcd(X^3 - 3X - 1,\, 3X^2 + 7X + 5) = 1.$$

In fact, Euclid's algorithm (courtesy of Maple) gives

$$(X^3 - 3X - 1)(\tfrac{-7}{37}X + \tfrac{29}{111}) + (3X^2 + 7X + 5)(\tfrac{7}{111}X^2 - \tfrac{26}{111}X + \tfrac{28}{111}) = 1.$$

Hence

$$(3x^2 + 7x + 5)(\tfrac{7}{111}x^2 - \tfrac{26}{111}x + \tfrac{28}{111}) = 1;$$

we have found the inverse of β.

1.7. **Generators of extension fields.** Let E be an extension field of F, and let S be a subset of E. The intersection of all the subrings of E containing F and S is again a subring of E (containing F and S). We call it the subring of E *generated by* F and S, and we write it $F[S]$.

LEMMA 1.13. *The ring $F[S]$ consists of all the elements of E that can be written as finite sums of the form*

$$\sum a_{i_1 \cdots i_n} \alpha_1^{i_1} \cdots \alpha_n^{i_n}, \quad a_{i_1 \cdots i_n} \in F, \quad \alpha_i \in S. \qquad (*)$$

PROOF. Let R be the set of all such elements; it is easy to check that R is a ring containing F and S, and that any ring containing F and S contains R; therefore R equals $F[S]$. □

Note that the expression of an element in the form (*) will *not* be unique in general. When $S = \{\alpha_1, ..., \alpha_n\}$, we write $F[\alpha_1, ..., \alpha_n]$ for $F[S]$.

LEMMA 1.14. *Let $E \supset R \supset F$ with E and F fields and R a ring. If R is finite-dimensional when regarded as an F-vector space, then it is a field.*

PROOF. Let α be a nonzero element of R—we have to show that α is invertible. The map $x \mapsto \alpha x : R \to R$ is an injective F-linear map, and is therefore surjective. In particular, there is an element $\beta \in R$ such that $\alpha\beta = 1$. □

EXAMPLE 1.15. An element of $\mathbb{Q}[\pi]$, $\pi = 3.14159...$, can be written uniquely as a finite sum

$$a_0 + a_1\pi + a_2\pi^2 + \cdots, \quad a_i \in \mathbb{Q}.$$

An element of $\mathbb{Q}[i]$ can be written uniquely in the form $a + bi$, $a, b \in \mathbb{Q}$. (Everything considered in $\mathbb{C}$.)

Let E again be an extension field of F and S a subset of E. The subfield $F(S)$ of E *generated by* F and S is the intersection of all subfields of E containing F and S. It is equal to the field of fractions of F[S] (since this is a field containing F and S, and is the smallest such field). Lemma 1.14 shows that $F[S]$ is sometimes already a field, in which case $F(S) = F[S]$. We write $F(\alpha_1, ..., \alpha_n)$ for $F(S)$ when $S = \{\alpha_1, ..., \alpha_n\}$.

Thus: $F[\alpha_1, \ldots, \alpha_n]$ consists of all elements of E that can be expressed as polynomials in the α_i with coefficients in F, and $F(\alpha_1, \ldots, \alpha_n)$ consists of all elements of E that can be expressed as quotients of two such polynomials.

EXAMPLE 1.16. An element of $\mathbb{Q}(\pi)$ can be expressed as a quotient

$$g(\pi)/h(\pi), \quad g(X), h(X) \in \mathbb{Q}[X], \quad h(\pi) \neq 0.$$

The ring $\mathbb{Q}[i]$ is already a field.

An extension E of F is said to be *simple* if $E = F(\alpha)$ some $\alpha \in E$. For example, $\mathbb{Q}(\pi)$ and $\mathbb{Q}[i]$ are simple extensions of $\mathbb{Q}$.

When F and F' are subfields of E, then we write $F \cdot F'$ for $F(F')(= F'(F))$, and we call it the *composite* of F and F'. It is the smallest subfield of E containing both F and F'.

1.8. **Algebraic and transcendental elements.** Let E be an extension field of F, and let $\alpha \in E$. Then we have a homomorphism

$$f(X) \mapsto f(\alpha) : F[X] \to E.$$

There are two possibilites.

Case 1: The kernel of the map is (0), i.e.,

$$f(\alpha) = 0, \quad f(X) \in F[X] \implies f(X) = 0.$$

In this case we say that α *transcendental* over F. The isomorphism $F[X] \to F[\alpha]$ extends to an isomorphism $F(X) \to F(\alpha)$.

Case 2: The kernel is $\neq (0)$, i.e., $g(\alpha) = 0$ for some nonzero $g(X) \in F[X]$. We then say that α is *algebraic* over F. Let $f(X)$ be the monic polynomial generating the kernel of the map. It is irreducible (if $f = gh$ is a proper factorization, then $g(\alpha)h(\alpha) = f(\alpha) = 0$, but $g(\alpha) \neq 0 \neq h(\alpha)$). We call f the *minimum polynomial* of α over F. It is characterized as an element of $F[X]$ by each of the following sets of conditions:

f is monic; $f(\alpha) = 0$; $g(\alpha) = 0$ and $g \in F[X] \implies f|g$;

f is the monic polynomial of least degree such $f(\alpha) = 0$;

f is monic, irreducible, and $f(\alpha) = 0$.

Note that $g(X) \mapsto g(\alpha)$ induces an isomorphism $F[X]/(f) \to F[\alpha]$. Since the first is a field, so also is the second: $F(\alpha) = F[\alpha]$. Moreover, each element of $F[\alpha]$ has a unique expression

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{m-1}\alpha^{m-1}, \qquad a_i \in F,$$

where $m = \deg(f)$. In other words, $1, \alpha, \ldots, \alpha^{m-1}$ is a basis for $F[\alpha]$ over F. Hence $[F(\alpha) : F] = m$. Since $F[x] \approx F[\alpha]$, arithmetic in $F[\alpha]$ can be performed using the same rules as in $F[x]$.

EXAMPLE 1.17. Let $\alpha \in \mathbb{C}$ be such that $\alpha^3 - 3\alpha - 1 = 0$. The minimum polynomial of α over $\mathbb{Q}$ is $X^3 - 3X - 1$ (because this polynomial is monic, irreducible, and has α as a root). The set $\{1, \alpha, \alpha^2\}$ is a basis for $\mathbb{Q}[\alpha]$ over $\mathbb{Q}$. The calculations in an example above show that if β is the element $\alpha^4 + 2\alpha^3 + 3$ of $\mathbb{Q}[\alpha]$, then $\beta = 3\alpha^2 + 7\alpha + 5$, and

$$\beta^{-1} = \tfrac{7}{111}\alpha^2 - \tfrac{26}{111}\alpha + \tfrac{28}{111}.$$

REMARK 1.18. Maple knows how to compute in $\mathbb{Q}[\alpha]$. For example,

`factor(X^4+4);` returns the factorization

$$(X^2 - 2X + 2)(X^2 + 2X + 2).$$

Now type: `alias(c=RootOf(X^2+2*X+2);`. Then

`factor(X^4+4,c);` returns the factorization

$$(X + c)(X - 2 - c)(X + 2 + c)(X - c),$$

i.e., Maple has factored $X^4 + 4$ in $\mathbb{Q}[c]$ where c has minimum polynomial $X^2 + 2X + 2$.

An extension E/F is *algebraic* if all elements of E are algebraic over F; otherwise it is *transcendental* over F.

PROPOSITION 1.19. *(a) If $[E : F]$ is finite, then E is algebraic over F.*

(b) If E is algebraic over F and finitely generated (as a field), then $[E : F]$ is finite.

PROOF. (a) If α were transcendental over F, then $1, \alpha, \alpha^2, \ldots$ would be linearly independent over F.

(b) Let $E = F[\alpha_1, ..., \alpha_n]$; then $F[\alpha_1]$ is finite over F (because α_1 is algebraic over F); $F[\alpha_1, \alpha_2]$ is finite over $F[\alpha_1]$ (because α_2 is algebraic over F, and hence $F[\alpha_1]$). Hence $F[\alpha_1, \alpha_2]$ is finite over F. This argument can be continued. □

COROLLARY 1.20. *If E is algebraic over F then any subring R of E containing F is a field.*

Proof. Let $\alpha \in R$; then $F[\alpha]$ is a field and $F[\alpha] \subset R$. Therefore α has an inverse in R. □

A field F is said to be *algebraically closed* if E algebraic over F implies $E = F$. Equivalent condition: the only irreducible polynomials in $F[X]$ are of degree one; every nonconstant polynomial in $F[X]$ has a root in F.

Example 1.21. The field of complex numbers $\mathbb{C}$ is algebraically closed. The set of all complex numbers algebraic over $\mathbb{Q}$ is an algebraically closed field. Every field F has an algebraically closed algebraic extension field (which is unique up to a *nonunique* isomorphism). All these statements will be proved later.

1.9. **Transcendental numbers.** A complex number is said to be *algebraic* or *transcendental* according as it is algebraic or transcendental over $\mathbb{Q}$. First some history:

1844: Liouville showed that certain numbers (now called Liouville numbers) are transcendental.

1873: Hermite showed that e is transcendental.

1873: Cantor showed that the set of algebraic numbers is countable, but that $\mathbb{R}$ is not countable. [Thus almost all numbers are transcendental, but it is usually very difficult to prove that a particular number is transcendental.]

1882: Lindemann showed that π is transcendental.

1934: Gelfond-Schneider showed that if α and β are algebraic, $\alpha \neq 0, 1$, and $\beta \notin \mathbb{Q}$, then α^{β} is transcendental. (This was one of Hilbert's famous problems)

1994: Euler's constant

$$\gamma = \lim_{n\to\infty} (\sum_{k=1}^{n} 1/k - \log n)$$

has not yet been proven to be transcendental.

1994: The numbers $e + \pi$ and $e - \pi$ are surely transcendental, but they have not even been proved to be irrational!

Proposition 1.22. *The set of algebraic numbers is countable.*

Proof. Define the height $h(r)$ of a rational number to be $\max(|m|, |n|)$, where $r = m/n$ is the expression of r in its lowest terms. There are only finitely many rational numbers with height less than a fixed number N. Let $A(N)$ be the set of algebraic numbers whose minimum equation over $\mathbb{Q}$ is of degree $\leq N$ and has coefficients of height $< N$. Then $A(N)$ is finite for each N. Count the elements of $A(10)$; then count the elements of $A(100)$; then count the elements of $A(1000)$, and so on. □

A typical Liouville number is $\sum_{n=0}^{\infty} \frac{1}{10^{n!}}$—in its decimal expansion there are increasingly long strings of zeros. We prove that the analogue of this number in base 2 is transcendental.

THEOREM 1.23. *The number $\alpha = \sum \frac{1}{2^{n!}}$ is transcendental.*

PROOF. Suppose not, and let

$$f(X) = X^d + a_1 X^{d-1} + \cdots + a_d, \quad a_i \in \mathbb{Q},$$

be the minimum polynomial of α over $\mathbb{Q}$. Thus $[\mathbb{Q}[\alpha] : \mathbb{Q}] = d$. Let

$$f(X) = \prod_{i=1}^{d} (X - \alpha_i), \quad \alpha_i \in \mathbb{C}, \quad \alpha_1 = \alpha,$$

and choose a nonzero integer D such that $Df(X) \in \mathbb{Z}[X]$. Let $\Sigma_N = \sum_{n=0}^{N} \frac{1}{2^{n!}}$, so that $\Sigma_N \to \alpha$ as $N \to \infty$, and let $x_N = f(\Sigma_N)$.

Because $f(X)$ is irreducible in $\mathbb{Q}[X]$, it has no rational root, except possibly α; but $\Sigma_N \neq \alpha$, and so $x_N \neq 0$. (In fact α is obviously nonrational because its expansion to base 2 is not periodic.)

Clearly $x_N \in \mathbb{Q}$; in fact $(2^{N!})^d D x_N \in \mathbb{Z}$, and so

$$|(2^{N!})^d D x_N| \geq 1.$$

On the other hand,

$$|x_N| = \prod |\Sigma_N - \alpha_i| \leq |\alpha_1 - \Sigma_N| (M + \Sigma_N)^{d-1}, \quad \text{where } M = \max_{i \neq 1} |\alpha_i|,$$

and

$$|\alpha_1 - \Sigma_N| = \sum_{n=N+1}^{\infty} \frac{1}{2^{n!}} \leq \frac{2}{2^{(N+1)!}}$$

Hence

$$|(2^{N!})^d D x_N| \leq 2 \cdot \frac{2^{d \cdot N!} D}{2^{(N+1)!}} \cdot (M + \Sigma_N)^{d-1} \to 0 \quad \text{as } N \to \infty$$

because $\frac{2^{d \cdot N!}}{2^{(N+1)!}} = \left(\frac{2^d}{2^{N+1}}\right)^{N!} \to 0$. We have a contradiction. □

1.10. **Constructions with straight-edge and compass.** The Greeks understood that integers and the rational numbers. They were surprised to find that the length of the diagonal of a square of side 1, namely $\sqrt{2}$, is not rational. They thus realized that they needed to extend their number system. They then hoped that the "constructible" numbers would suffice. Suppose we are given a length, which we call 1, a straight-edge, and a compass (device for drawing circles). A number (better a length) is *constructible* if it can be constructed by forming successive intersections of

- lines drawn through two points already constructed, and
- circles with centre a point already constructed and radius a constructed length.

This led them to three famous problems that they were unable to solve: is it possible to duplicate the cube, trisect an angle, or square the circle by straight-edge and compass constructions? We'll see that the answer to all three is negative.

Let F be a subfield of $\mathbb{R}$. The F-plane is $F \times F \subset \mathbb{R} \times \mathbb{R}$. We make the following definitions:

A line in the F-plane is a line through two points in the F-plane. Such a line is given by an equation:

$$ax + by + c = 0, \quad a, b, c \in F.$$

A circle in the F-plane is a circle with centre an F-point and radius an element of F. Such a circle is given by an equation:

$$(x-a)^2+(y-b)^2=c^2, \quad a,b,c \in F.$$

LEMMA 1.24. *Let $L \neq L'$ be F-lines, and let $C \neq C'$ be F-circles.*

(a) *$L \cap L' = \emptyset$ or consists of a single F-point.*
(b) *$L \cap C = \emptyset$ or consists of one or two points in the $F[\sqrt{e}]$-plane, some $e \in F$.*
(c) *$C \cap C' = \emptyset$ or consists of one or two points in the $F[\sqrt{e}]$-plane, some $e \in F$.*

PROOF. The points in the intersection are found by solving the simultaneous equations, and hence by solving (at worst) a quadratic equation with coefficients in F. □

LEMMA 1.25. *(a) If c and d are constructible, then so also are $c \pm d$, cd, and $\frac{c}{d}$ $(d \neq 0)$.*

(b) If $c > 0$ is constructible, then so also is $\sqrt{c}$.

PROOF. First show that it is possible to construct a line perpendicular to a given line through a given point, and then a line parallel to a given line through a given point. Hence it is possible to construct a triangle similar to a given one on a side with given length. By an astute choice of the triangles, one constructs cd and c^{-1}. For (b), draw a circle of radius $\frac{c+1}{2}$ about $(\frac{c+1}{2},0)$, and draw a vertical line through the point $A=(1,0)$ to meet the circle at P. The length AP is $\sqrt{c}$. (For more details, see for example, Rotman, Galois Theory, Appendix 3.) □

THEOREM 1.26. *(a) The set of constructible numbers is a field.*

(b) A number α is constructible if and only if it is contained in field of the form

$$\mathbb{Q}[\sqrt{a_1},\ldots,\sqrt{a_r}], \quad a_i \in \mathbb{Q}[\sqrt{a_1},\ldots,\sqrt{a_{i-1}}].$$

PROOF. (a) Immediate from (a) of Lemma 1.25.

(b) From (a) we know that the set of constructible numbers is a field containing $\mathbb{Q}$, and it follows from (a) and Lemma 1.25 that every number in $\mathbb{Q}[\sqrt{a_1},\ldots,\sqrt{a_r}]$ is constructible. Conversely, it follows from Lemma 1.24 that every constructible number is in a field of the form $\mathbb{Q}[\sqrt{a_1},\ldots,\sqrt{a_r}]$. □

Now we can apply the (not quite elementary) result Proposition 1.10 to obtain:

COROLLARY 1.27. *If α is constructible, then α is algebraic over $\mathbb{Q}$, and $[\mathbb{Q}[\alpha]:\mathbb{Q}]$ is a power of 2.*

PROOF. We know that $[\mathbb{Q}[\alpha]:\mathbb{Q}]$ divides $[\mathbb{Q}[\sqrt{a_1},\ldots,\sqrt{a_r}]:\mathbb{Q}]=2^r$. □

COROLLARY 1.28. *It is impossible to duplicate the cube by straight-edge and compass constructions.*

PROOF. The problem is to construct a cube with volume 2. This requires constructing a root of the polynomial $X^3-2=0$. But this polynomial is irreducible (by Eisenstein's criterion for example), and so $[\mathbb{Q}[\sqrt[3]{2}]:\mathbb{Q}]=3$. □

COROLLARY 1.29. *In general, it is impossible to trisect an angle by straight-edge and compass constructions.*

Proof. Knowing an angle is equivalent to knowing the cosine of the angle. Therefore, to trisect 3α, we have to construct a solution to

$$\cos 3\alpha = 4\cos^3\alpha - 3\cos\alpha.$$

For example, take $3\alpha = 60$; to construct α, we have to solve $8x^3 - 6x - 1 = 0$, which is irreducible. □

Corollary 1.30. *It is impossible to square the circle by straight-edge and compass constructions.*

Proof. A square with the same area as a circle of radius r has side $\sqrt{\pi}r$. Since π is transcendental, so also is $\sqrt{\pi}$. □

We now consider another famous old problem, that of constructing a regular polygon. Note that $X^m - 1$ is not irreducible; in fact

$$X^m - 1 = (X-1)(X^{m-1} + X^{m-2} + \cdots + 1).$$

Lemma 1.31. *If p is prime then $X^{p-1} + \cdots + 1$ is irreducible; hence $\mathbb{Q}[e^{2\pi i/p}]$ has degree $p-1$ over $\mathbb{Q}$.*

Proof. Consider

$$f(X+1) = \frac{(X+1)^p - 1}{X} = X^{p-1} + \cdots + a_2X^2 + a_1X + p,$$

with $a_i = \binom{p}{i+1}$. Since $p|a_i$, $i = 1, ..., p-2$, $f(X+1)$ is irreducible by Eisenstein's criterion. □

In order to construct a regular p-gon, p an odd prime, we need to construct $\cos\frac{2\pi}{p}$. But $\mathbb{Q}[e^{\frac{2\pi i}{p}}] \supset \mathbb{Q}[\cos\frac{2\pi}{p}] \supset \mathbb{Q}$. The degree of $\mathbb{Q}[e^{\frac{2\pi i}{p}}]$ over $\mathbb{Q}[\cos\frac{2\pi}{p}]$ is 2—the equation

$$\alpha^2 - 2\cos\frac{2\pi}{p}\cdot\alpha + 1 = 0, \quad \alpha = e^{\frac{2\pi i}{p}},$$

shows that it is ≤ 2, and it is not 1 because $\mathbb{Q}[e^{\frac{2\pi i}{p}}]$ is not contained in $\mathbb{R}$. Hence $[\mathbb{Q}[\cos\frac{2\pi}{p}] : \mathbb{Q}] = \frac{p-1}{2}$.

Thus if the regular p-gon is constructible, then $(p-1)/2 = 2^k$ some k (later, we shall see a converse), which imples $p = 2^{k+1} + 1$. But $2^r + 1$ can only be a prime if r is a power of 2, because otherwise r has an odd factor t, and for t odd,

$$Y^t + 1 = (Y+1)(Y^{t-1} - Y^{t-2} + \cdots + 1).$$

Thus if the regular p-gon is constructible, then $p = 2^{2^k} + 1$ for some k. Fermat conjectured that all numbers of the form $2^{2^k} + 1$ are prime, and claimed to show that this is true for $k \leq 5$—for this reason primes of this form are called *Fermat primes.* For $0 \leq k \leq 4$, the numbers $p = 3, 5, 17, 257, 65537$, are prime but Euler showed that $2^{32} + 1 = 641 \cdot 6700417$, and we don't know of any more Fermat primes.

Gauss showed that

$$\cos\frac{2\pi}{17} = -\frac{1}{16} + \frac{1}{16}\sqrt{17} + \frac{1}{16}\sqrt{34 - 2\sqrt{17}} + \frac{1}{8}\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}}$$

when he was 18 years old. This success encouraged him to become a mathematician.

2. Splitting Fields; Algebraic Closures

2.1. Maps from simple extensions.

Let E and E' be fields containing F. An *F-homomorphism* is a homomorphism $\varphi : E \to E'$ such that $\varphi(a) = a$ for all $a \in F$. Thus an F-homorphism maps a polynomial $\sum a_{i_1\cdots i_m}\alpha_1^{i_1}\cdots\alpha_m^{i_m}$, $a_{i_1\cdots i_m} \in F$, to

$$\sum a_{i_1\cdots i_m}\varphi(\alpha_1)^{i_1}\cdots\varphi(\alpha_m)^{i_m}.$$

An *F-isomorphism* is a bijective F-homomorphism. Note that if E and E' have the same finite degree over F, then an F-homomorphism is automatically an F-isomorphism.

Proposition 2.1. *Let $F(\alpha)$ be a simple field extension of a field F, and let Ω be a second field containing F.*

(a) *Assume α is transcendental over F; then for any F-homomorphism $\varphi : F(\alpha) \to \Omega$, $\varphi(\alpha)$ is transcendental over F, and the map $\varphi \mapsto \varphi(\alpha)$ defines a one-to-one correspondence*

$$\{F\text{-homomorphisms } \varphi : F(\alpha) \to \Omega\} \leftrightarrow \{\text{ elements of } \Omega \text{ transcendental over } F\}.$$

(b) *Assume α is algebraic over F, with minimum polynomial $f(X)$; then for any F-homomorphism $\varphi : F[\alpha] \to \Omega$, $\varphi(\alpha)$ is a root of $f(X)$ in Ω, and the map $\varphi \mapsto \varphi(\alpha)$ defines a one-to-one correspondence*

$$\{F\text{-homomorphisms } \varphi : F[\alpha] \to \Omega\} \leftrightarrow \{\text{ distinct roots of } f(X) \text{ in } \Omega\}.$$

In particular, the number of such maps is the number of distinct roots of f in Ω.

Proof. (a) Let $\gamma \in \Omega$. To say that α is transcendental over F means that $F[\alpha]$ is the ring of polynomials in α (as variable). By the universal property of polynomial rings, there is a unique F-homomorphism $\varphi : F[\alpha] \to \Omega$ sending α to γ. This extends to $F(\alpha)$ if and only if all nonzero elements of $F[\alpha]$ are sent to invertible (i.e., nonzero) elements of Ω, which is so if and only if γ is transcendental.

(b) Let $f(X) = \sum a_i X^i$, and consider an F-homomorphism $\varphi : F[\alpha] \to \Omega$. On applying φ to the equation $\sum a_i\alpha^i = 0$, we obtain the equation $\sum a_i\varphi(\alpha)^i = 0$, which shows that $\gamma =_{df} \varphi(\alpha)$ is a root of $f(X)$ in Ω. Conversely, let $\gamma \in \Omega$ be a root of $f(X)$. The map $F[X] \to \Omega$, $g(X) \mapsto g(\gamma)$, factors through $F[X]/(f(X))$. When composed with the inverse of the isomorphism $F[X]/(f(X)) \to F[\alpha]$, it becomes a homomorphism $F[\alpha] \to \Omega$ sending α to γ. □

We shall need a slight generalization of this result.

Proposition 2.2. *Let $F(\alpha)$ be a simple field extension of a field F, and let $\varphi_0 : F \to \Omega$ be a homomorphism of F into a second field Ω.*

(a) *Assume α is transcendental over F; then the map $\varphi \mapsto \varphi(\alpha)$ defines a one-to-one correspondence*

$$\{\text{extensions } \varphi : F(\alpha) \to \Omega \text{ of } \varphi_0\} \leftrightarrow \{\text{elements of } \Omega \text{ transcendental over } \varphi_0(F)\}.$$

(b) *Assume α is algebraic over F, with minimum polynomial $f(X)$; then the map $\varphi \mapsto \varphi(\alpha)$ defines a one-to-one correspondence*

$$\{\text{extensions } \varphi : F[\alpha] \to \Omega \text{ of } \varphi_0\} \leftrightarrow \{\text{ distinct roots of } (\varphi_0 f)(X)\text{in } \Omega\}.$$

In particular, the number of such maps is the number of distinct roots of $\varphi_0 f$ in Ω.

Proof. The proof is essentially the same as that of the preceding proposition. □

By $\varphi_0 f$ we mean the polynomial obtained by applying φ_0 to the coefficients of f, i.e., $f = \sum a_i X^i \implies \varphi_0 f = \sum \varphi(a_i) X^i$.

2.2. Splitting fields.

Let f be a polynomial with coefficients in F. A field E containing F is said to *split* f if f splits in $E[X]$, i.e., if $f(X) = \prod(X - \alpha_i)$ with $\alpha_i \in E$. If E is also generated by the α_i, then it is called a *splitting field* for f.

Note that if $f(X) = \prod f_i(X)^{m_i}$, then a splitting field for $\prod f_i(X)$ is also a splitting field for f (and conversely).

Example 2.3. (a) Let $f(X) = aX^2 + bX + c \in \mathbb{Q}[X]$ be irreducible, and let $\alpha = \sqrt{b^2 - 4ac}$; then the subfield $\mathbb{Q}[\alpha]$ of $\mathbb{C}$ generated by α is a splitting field for f.

(b) Let $f(X) = X^3 + aX^2 + bX + c \in \mathbb{Q}[X]$ be irreducible, and let $\alpha_1, \alpha_2, \alpha_3$ be its roots in $\mathbb{C}$. Then $\mathbb{Q}[\alpha_1, \alpha_2, \alpha_3] = \mathbb{Q}[\alpha_1, \alpha_2]$ is a splitting field for $f(X)$. Note that $[\mathbb{Q}[\alpha_1] : \mathbb{Q}] = 3$ and that $[\mathbb{Q}[\alpha_1, \alpha_2] : \mathbb{Q}[\alpha_1]] = 1$ or 2, and so $[\mathbb{Q}[\alpha_1, \alpha_2] : \mathbb{Q}] = 3$ or 6. We'll see later that the degree is 3 if and only if the discriminant of $f(X)$ is a square in F. For example, the discriminant of $X^3 + bX + c$ is $-4b^3 - 27c^2$, and so the splitting field of $X^3 + 10X + 1$ has degree 6 over $\mathbb{Q}$.

Proposition 2.4. *Every polynomial has a splitting field.*

Proof. Let $f \in F[X]$. Let g_1 be an irreducible factor of $f(X)$, and let $F_1 = F[X]/(g_1(X)) = F[\alpha_1]$, $\alpha_1 = X + (g_1)$. Then α_1 is a root of $f(X)$ in F_1, and we define $f_1(X)$ to be the quotient $f(X)/(X - \alpha_1)$ (in $F_1[X]$). Then $f_1 \in F_1[X]$, and the same construction gives us a field $F_2 = F_1[\alpha_2]$ with α_2 a root of f_1. By continuing in this fashion, we obtain a splitting field. □

Remark 2.5. Let $n = \deg f$. In the proof, $[F_1 : F] \leq n$, $[F_2 : F_1] \leq n - 1, ...,$ and so the degree of the splitting field over F is $\leq n!$. Whether or not there exist polynomials of degree n in $F[X]$ whose splitting field has degree $n!$ depends on F. For example, there don't for $n > 1$ if $F = \mathbb{C}$ or $\mathbb{F}_p$, nor for $n > 2$ if $F = \mathbb{R}$. However, later we shall see how to write down large numbers (in fact infinitely many) polynomials of degree n in $\mathbb{Q}[X]$ whose splitting fields have degree $n!$.

Example 2.6. (a) Let $f = (X^p - 1)/(X - 1)$; any field generated by a root of f is a splitting field (if ζ is one root, the remainder are $\zeta^2, \zeta^3, \ldots, \zeta^{p-1}$).

(b) Suppose F is of characteristic p, and let $f = X^p - X - a$; any field generated by a root of f is a splitting field (if α is one root, the remainder are $\alpha + 1, ..., \alpha + p - 1$).

(c) If α is one root of $X^n - a$, then the remaining roots are all of the form $\zeta\alpha$, where $\zeta^n = 1$. Therefore, if F contains all the n^{th} roots of 1, i.e., if $X^n - 1$ splits in $F[X]$, then $F[\alpha]$ is a splitting field for $X^n - a$. Note that if p is the characteristic of F, then $X^p - 1 = (X - 1)^p$, and so F automatically contains all the p^{th} roots of 1.

Proposition 2.7. *Let $f \in F[X]$, and let E be a splitting field for f, and let $\Omega \supset F$ be a second field splitting f.*

(a) *There exists at least one F-homomorphism $\varphi : E \to \Omega$.*

(b) *The number of F-homomorphisms $E \to \Omega$ is $\leq [E:F]$, and $= [E:F]$ if f has* $\deg(f)$ *distinct roots in Ω.*

(c) *If Ω is also a splitting field for f, then each F-homomorphism $E \to \Omega$ is an isomorphism. In particular, any two splitting fields for f are F-isomorphic.*

Proof. Write $E = F[\alpha_1, ..., \alpha_m]$, $m \leq \deg(f)$, with the α_i the distinct roots of $f(X)$. The minimum polynomial of α_1 is an irreducible polynomial f_1 dividing f. As f (hence f_1) splits in Ω, Proposition 2.1 shows that there exists an F-homomorphism $\varphi_1 : F[\alpha_1] \to \Omega$, and the number of φ_1's is $\leq \deg(f_1) = [F[\alpha_1] : F]$, with equality holding when f (hence also f_1) has distinct roots in Ω.

Next, the minimum polynomial of α_2 over $F[\alpha_1]$ is an irreducible factor f_2 of $f(X)$ in $F[\alpha_1][X]$. According to Proposition 2.2, each φ_1 extends to a homomorphism $\varphi_2 : F[\alpha_1, \alpha_2] \to \Omega$, and the number of extensions is $\leq \deg(f_2) = [F[\alpha_1, \alpha_2] : F[\alpha_1]]$, with equality holding when f (hence also f_2) has distinct roots in Ω.

On combining these statements we conclude that there exists an F-homomorphism $\varphi : F[\alpha_1, \alpha_2] \to \Omega$, and the number of such homomorphisms is $\leq [F[\alpha_1, \alpha_2] : F]$, with equality holding when f has $\deg(f)$ distinct roots in Ω.

After repeating the argument m times, we obtain (a) and (b). For (c), note that, because an F-homomorphism $E \to \Omega$ is injective, we must have $[E : F] \leq [\Omega : F]$. If Ω is also a splitting field, then we obtain the reverse inequality also. We therefore have equality, and so any F-homomorphism $E \to \Omega$ is an isomorphism. □

Corollary 2.8. *Let E and L be extension fields of F, with E finite over F; then there exists an extension field Ω of L and an F-homomorphism $E \to \Omega$.*

Proof. Write $E = F[\alpha_1, \ldots, \alpha_m]$, and let f_i be the minimum polynomial of α_i over F. Let E' be a splitting field of $f =_{df} \prod f_i$ regarded as an element of $E[X]$, and replace E with the subfield of E' generated by F and all the roots of $f(X)$. Thus E is now the splitting field of $f(X) \in F[X]$. Let Ω be a splitting field for f regarded as an element of $L[X]$. The proposition shows that there is an F-homomorphism $E \to \Omega$. □

Remark 2.9. After replacing E by its (isomorphic) image in Ω, we will have that E and L are subfields of Ω. This will allow us to assume that E and L are subfields of a common field.

Warning! If E and E' are splitting fields of $f(X) \in F[X]$, then we know there is an F-isomorphism $E \to E'$, but there will in general be no *preferred* such isomorphism. Error and confusion can result if you simply identify the fields.

2.3. **Algebraic closures.**

Recall that Ω is said to be algebraically closed if every nonconstant polynomial $f(X) \in \Omega[X]$ has a root in Ω (and hence splits in $\Omega[X]$); equivalently, if the only irreducible polynomials in $\Omega[X]$ are those of degree 1. Recall also that a field Ω containing F is said to be an algebraic closure of F if it is algebraic over F and it is algebraically closed. We want to show that (assuming the axiom of choice) every field has an algebraic closure. The following criterion suggests how this might be done.

Lemma 2.10. *Suppose that Ω is algebraic over F and every polynomial $f \in F[X]$ splits in $\Omega[X]$; then Ω is an algebraic closure of F.*

PROOF. Let $f \in \Omega[X]$. We know (see §1.6) how to construct a finite extension E of Ω containing a root α of f. We want to show that α in fact lies in Ω. Write $f = a_nX^n + \cdots + a_0$, $a_i \in \Omega$, and consider the sequence of fields $F \subset F[a_1, \ldots, a_n] \subset F[a_1, \ldots, a_n, \alpha]$. Because each a_i is algebraic over F, $F[a_1, \ldots, a_n]$ is a finite field extension of F, and because $f \in F[a_1, \ldots, a_n][X]$, α is algebraic over $F[a_1, \ldots, a_n]$. Therefore α lies in a finite extension of F, and is therefore algebraic over F, i.e., it is the root of a polynomial with coefficients in F. But, by assumption, this polynomial splits in $\Omega[X]$, and so all its roots lie in Ω. In particular, $\alpha \in \Omega$. □

LEMMA 2.11. *Let $\Omega \supset F$; then*

$$E = \{\alpha \in \Omega \mid \alpha \text{ algebraic over } F\}$$

is a field.

PROOF. If α and β are algebraic over F, then $F[\alpha, \beta]$ is of finite degree over F, and so is a field (see 1.14). Every element of $F[\alpha, \beta]$ is algebraic over F, including $\alpha \pm \beta$, α/β, $\alpha\beta, \ldots$. □

The field E constructed in the lemma is called the *algebraic closure of F in Ω*. The preceding lemma shows that if every polynomial in $F[X]$ splits in $\Omega[X]$, then E is an algebraic closure of F. Thus to construct an algebraic closure of F, it suffices to construct an extension in which every polynomial in $F[X]$ splits. We know how to do this for a single polynomial, but passing from there to all polynomials causes set-theoretic problems.

THEOREM 2.12 (*). [2]*Every field has an algebraic closure.*

Once we have proved the fundamental theorem of algebra, that $\mathbb{C}$ is algebraically closed, then we will know that the algebraic closure in $\mathbb{C}$ of any subfield F of $\mathbb{C}$ is an algebraic closure of F. This proves the theorem for such fields. We sketch three proofs of the general result. The first doesn't assume the axiom of choice, but does assume that F is countable.

PROOF. (First proof of 2.12) Because F is countable, it follows that $F[X]$ is countable, i.e., we can list its elements $f_1(X), f_2(X), \ldots$. Define the fields E_i inductively as follows: $E_0 = F$; E_i is the splitting field of f_i over E_{i-1}. Note that $E_0 \subset E_1 \subset E_2 \subset \cdots$. Define $\Omega = \cup E_i$; it is obviously an algebraic closure of F. □

REMARK 2.13. Since the E_i are not subsets of a fixed set, forming the union requires explanation: define Ω^* to be the disjoint union of the E_i; let a, $b \in \Omega^*$, say $a \in E_i$ and $b \in E_j$; write $a \sim b$ if $a = b$ when regarded as elements of the larger of E_i or E_j; verify that $\sim$ is an equivalence relation, and let $\Omega = \Omega^*/\sim$.

PROOF. (Second proof of 2.12) If A and B are rings containing a field F, then $A \otimes_F B$ is a ring containing F, and there are F-homomorphisms A, $B \to A \otimes_F B$. More generally, if $(A_i)_{i \in I}$ is some family of rings each of which contains F, then $\otimes_F A_i$ is a ring containing F, and there are F-homomorphisms $A_j \to \otimes_F A_i$ for each $j \in I$. It is defined to be the quotient of the F-vector space with basis ΠA_i by the subspace generated by elements of the form:

- $(x_i) + (y_i) - (z_i)$ with $x_j + y_j = z_j$ for one $j \in I$ and $x_i = y_i = z_i$ for all $i \neq j$.
- $(x_i) - a(y_i)$ with $x_j = ay_j$ for one $j \in I$ and $x_i = y_i$ for all $i \neq j$.

[2] Results marked with an asterisk require the axiom of choice for their proof.

It can be made into a ring in an obvious fashion (see Bourbaki, Algèbre, Chapt 3, Appendix).

For each polynomial $f \in F[X]$, choose a splitting field E_f, and let $\Omega = (\otimes_f E_f)/M$ where M is a maximal ideal in $\otimes_f E_f$—Zorn's lemma implies that M exists (see below). Then Ω is a field (see 1.1), and there are F-homomorphisms $E_f \to \Omega$ (which must be injective) for each $f \in F[X]$. Since f splits in E_f, it must also split in the larger field Ω. The algebraic closure of F in Ω is therefore an algebraic closure of F. (Actually, Ω itself is an algebraic closure of F.) □

Lemma 2.14 (Zorn's). *Let $(S, \leq)$ be a nonempty partially ordered set (reflexive, transitive, anti-symmetric, i.e., $a \leq b$ and $b \leq a \implies a = b$). Suppose that every totally ordered subset T of S (i.e., for all $s, t \in T$, either $s \leq t$ or $t \leq s$) has an upper bound in S (i.e., there exists an $s \in S$ such that $t \leq s$ for all $t \in T$). Then S has a maximal element (i.e., an element s such that $s \leq s' \implies s = s'$).*

Zorn's lemma is equivalent to the Axiom of Choice.

Lemma 2.15 (*). *Every nonzero commutative ring A has a maximal ideal.*

Proof. Let S be the set of all proper ideals in A, partially ordered by inclusion. If T is a totally ordered set of ideals, then $J = \bigcup_{I \in T} I$ is again an ideal, and it is proper because if $1 \in J$ then $1 \in I$ for some I in T. Thus J is an upper bound for T. Now Zorn's lemma implies that S has a maximal element, which is a maximal ideal in A. □

Proof. (Third proof of 2.12) First show that the cardinality of any field algebraic over F is the same as that of F. Next choose an uncountable set Ξ of cardinality greater than that of F, and identify F with a subset of Ξ. Let S be the set triples $(E, +, \cdot)$ with $E \subset S$ and $(+, \cdot)$ a field structure on E such that $(E, +, \cdot)$ contains F as a subfield and is algebraic over it. Write $(E, +, \cdot) \leq (E', +', \cdot')$ if the first is a subfield of the second. Apply Zorn's lemma to show that S has maximal elements, and then show that a maximal element is algebraically closed. (See Jacobson, Lectures in Algebra, III, p144 for the details.) □

There do exist naturally occurring fields, not contained in $\mathbb{C}$, that are uncountable. For example, for any field F there is a ring $F[[T]]$ of formal power series $\sum_{i \geq 0} a_i T^i$, $a_i \in F$, and its field of fractions is uncountable even if F is finite.

Theorem 2.16 (*). *Let Ω be an algebraic closure of F, and let E be an algebraic extension of F; then there is an F-homomorphism $E \to \Omega$. If E is also an algebraic closure of F, then any such map is an isomorphism.*

Proof. Suppose first that E is countably generated over F, i.e., $E = F[\alpha_1, ..., \alpha_n, \ldots]$. Then we can extend the inclusion map $F \to \Omega$ to $F[\alpha_1]$ (map α_1 to any root of its minimal polynomial in Ω), then to $F[\alpha_1, \alpha_2]$, and so on.

The uncountable case is a straightforward application of Zorn's lemma.

Let S be the set of pairs (M, φ_M) with M a field $F \subset M \subset E$ and φ_M an F-homomorphim $M \to \Omega$. Write $(M, \varphi_M) \leq (N, \varphi_N)$ if $M \subset N$ and $\varphi_N | M = \varphi_M$. This makes S into a partially ordered subset. Let T be a totally ordered subset of S. Then $M' = \cup_{M \in T} M$ is a subfield of E, and we can define a homomorphism $\varphi' : M' \to \Omega$ by requiring that $\varphi'(x) = \varphi_M(x)$ if $x \in M$. The pair (M', φ') is an upper bound for T in S. Hence Zorn's lemma gives us a maximal element (M, φ) in S. Suppose that $M \neq E$. Then there exists an element $\alpha \in E$, $\alpha \notin M$. Since α is algebraic over M, we can apply (2.2) to extend φ to $M[\alpha]$, contradicting the maximality of M. Hence $M = E$, and the proof of the first statement is complete.

If E is algebraically closed, then every polynomial $f \in F[X]$ splits in E and hence in $\varphi(E)$, i.e., $f(X) = \prod(X - \alpha_i)$, $\alpha_i \in \varphi(E)$. Let $\alpha \in \Omega$, and let $f(X)$ be the minimum polynomial of α. Then $X - \alpha$ is a factor of $f(X)$ in $\Omega[X]$, but, as we just observed, $f(X)$ splits in $\varphi(E)[X]$. Because of unique factorization, this implies that $\alpha \in \varphi(E)$. □

The above proof is a typical application of Zorn's lemma: once we know how to do something in a finite (or countable) situation, Zorn's lemma allows us to do it in general.

Remark 2.17. Even for a finite field F, there will exist uncountably many isomorphisms from one algebraic closure to a second, none of which is to be preferred over any other. Thus it is (uncountably) sloppy to say that the algebraic closure of F is unique. All one can say is that, given two algebraic closures Ω, Ω' of F, then, thanks to the axiom of choice, there exists an F-isomorphism $\Omega \rightarrow \Omega'$.

3. The Fundamental Theorem of Galois Theory

In this section, we prove the fundamental theorem of Galois theory, which gives a one-to-one correspondence between the subfields of the splitting field of a separable polynomial and the subgroups of the Galois group of f.

3.1. **Multiple roots.**

Let $f, g \in F[X]$. Even when f and g have no common factor in $F[X]$, you might expect that they could acquire a common factor in $\Omega[X]$ for some $\Omega \supset F$. In fact, this doesn't happen—gcd's don't change when the field is extended.

Proposition 3.1. *Let f and g be polynomials in $F[X]$, and let $\Omega \supset F$. If $r(X)$ is the gcd of f and g computed in $F[X]$, then it is also the gcd of f and g in $\Omega[X]$. In particular, if f and g are monic and irreducible and $f \neq g$, then they do not have a common root in any extension field of F.*

Proof. Let $r_F(X)$ and $r_\Omega(X)$ be the greatest common divisors of f and g in $F[X]$ and $\Omega[X]$ respectively. Certainly $r_F(X)|r_\Omega(X)$ in $\Omega[X]$. The Euclidean algorithm shows that there are polynomials a and b in $F[X]$ such that

$$a(X)f(X) + b(X)g(X) = r_F(X).$$

Since $r_\Omega(X)$ divides f and g in $\Omega[X]$, it divides the left-hand side of the equation, and therefore also the right. Hence $r_\Omega = r_F$.

For the second statement, note that the hypotheses imply that $\gcd(f, g) = 1$ (in $F[X]$). Hence they can't have a common factor $X - \alpha$ in any extension field. □

The proposition allows us to write $\gcd(f, g)$, without reference to a field.

Let $f \in F[X]$, and let $f(X) = \prod(X - \alpha_i)^{m_i}$, α_i distinct, be a splitting of f over some large field $\Omega \supset F$. We then say that α_i is a root of *multiplicity* m_i. A root of multiplicity one is said to be *simple*.

We say that f *has multiple roots* if it has roots of multiplicity > 1 in some big field Ω. It then has multiple roots in the subfield of Ω generated by its roots, and because any two splitting fields are F-isomorphic, this shows that f will have roots of multiplicity > 1 in every field containing F in which it splits.

If f has multiple factors in $F[X]$, say $f = \prod f_i(X)^{m_i}$ with some $m_i > 1$, then obviously it will have multiple roots. If $f = \prod f_i$ with the f_i distinct monic irreducible polynomials, then the proposition shows that f can only have multiple roots if one of the f_i has multiple roots. Thus it remains to examine irreducible polynomials for multiple roots.

Example 3.2. Let F be of characteristic p, and assume that F has an element a that is not a p^{th}-power (e.g., $F = \mathbb{F}_p(T)$; $a = T$). Then $X^p - a$ is irreducible in $F[X]$, but $X^p - a = (X - \alpha)^p$ in its splitting field. Thus an irreducible polynomial can have multiple roots.

We define the derivative $f'(X)$ of a polynomial $f(X) = \sum a_i X^i$ to be $\sum i a_i X^{i-1}$. When $F = \mathbb{R}$, this agrees with the usual definition. The usual rules for differentiating sums and products still hold, but note that the derivative of X^p is zero in characteristic p.

Proposition 3.3. *Let f be a (monic) irreducible polynomial in $F[X]$. The following statements are equivalent:*

(a) *f has at least one multiple root (in a splitting field);*
(b) $\gcd(f, f') \neq 1$;
(c) *F has characteristic $p \neq 0$ and $f(X) = g(X^p)$, some $g \in F[X]$;*
(d) *all the roots of f are multiple.*

PROOF. (a) $\implies$ (b). Let α be a multiple root of f, and write $f = (X-\alpha)^m g(X)$, $m > 1$, in some splitting field. Then

$$f'(X) = m(X-\alpha)^{m-1}g(X) + (X-\alpha)^m g'(X).$$

Hence $f'(\alpha) = 0$, and so $\gcd(f, f') \neq 1$.

(b) $\implies$ (c). Since f is irreducible and $\deg(f') < \deg(f)$,

$$\gcd(f, f') \neq 1 \implies f' = 0 \implies f = g(X^p).$$

(c) $\implies$ (d). Suppose $f(X) = g(X^p)$, and let $g(X) = \prod(X - a_i)^{m_i}$ in some splitting field. Then

$$f(X) = g(X^p) = \prod(X^p - a_i)^{m_i} = \prod(X - \alpha_i)^{pm_i}$$

where $\alpha_i^p = a_i$ (in some big field). Hence every root of $f(X)$ has multiplicity at least p.

(d) $\implies$ (a). Every root multiple $\implies$ at least one root multiple (I hope). □

DEFINITION 3.4. A polynomial $f \in F[X]$ is said to be *separable* if all its irreducible factors have simple roots.

Note that the preceding discussion shows that f is not separable if and only if

(a) the characteristic of F is $p \neq 0$, and
(b) at least one of the irreducible factors of f is a polynomial in X^p.

A field F is said to be *perfect* if all polynomials in $F[X]$ are separable.

PROPOSITION 3.5. *A field F is perfect if and only if it either*

- *has characteristic* 0*, or*
- *it has characteristic p and $F = F^p$ (i.e., every element of F is a p^{th} power).*

PROOF. $\implies$: If char $F = p$ and it contains an element a that is not a p^{th} power, then $F[X]$ contains a nonseparable polynomial, namely, $X^p - a$.

$\impliedby$: If char $F = p$ and $F = F^p$, then every polyonomial in X^p is a p^{th} power—$\sum a_i X^p = (\sum b_i X)^p$ if $a_i = b_i^p$—and so can't be irreducible. □

EXAMPLE 3.6. (a) All finite fields are perfect (because $a \mapsto a^p$ is an injective homomorphism $F \to F$, which must be surjective if F is finite). In fact, any field algebraic over $\mathbb{F}_p$ is perfect.

(b) If F_0 has characteristic p, then $F = F_0(X)$ is not perfect (because X is not a p^{th} power).

3.2. **Groups of automorphisms of fields.**

Consider fields $E \supset F$. We write $\operatorname{Aut}(E/F)$ for the group of F-automorphisms of E, i.e., automorphisms $\sigma : E \to E$ such that $\sigma(a) = a$ for all $a \in F$.

Example 3.7. (a) There are two obvious automorphisms of $\mathbb{C}$, namely, the identity map and complex conjugation. We'll see later (last section) that by using the Axiom of Choice, one can construct uncountably many more. They are all noncontinuous and (I've been told) nonmeasurable—hence they *require* the Axiom of Choice for their construction.

(b) Let $E = \mathbb{C}(X)$. Then $\mathrm{Aut}(E/\mathbb{C})$ consists of the maps $X \mapsto \frac{aX+b}{cX+d}$, $ad - bc \neq 0$ (Jacobson, Lectures III, p158), and so $\mathrm{Aut}(E/\mathbb{C}) = \mathrm{PGL}_2(\mathbb{C})$. Analysts will note that this is the same as the automorphism group of the Riemann sphere. This is not a coincidence: the field of meromorphic functions on the Riemann sphere $\mathbb{P}^1_{\mathbb{C}}$ is $\mathbb{C}(z) \approx \mathbb{C}(X)$, and so there is a map $\mathrm{Aut}(\mathbb{P}^1_{\mathbb{C}}) \to \mathrm{Aut}(\mathbb{C}(z)/\mathbb{C})$, which one can show is an isomorphism.

(c) The group $\mathrm{Aut}(\mathbb{C}(X_1, X_2)/\mathbb{C})$ is quite complicated—there is a map

$$\mathrm{PGL}_3(\mathbb{C}) = \mathrm{Aut}(\mathbb{P}^2_{\mathbb{C}}) \hookrightarrow \mathrm{Aut}(\mathbb{C}(X_1, X_2)/\mathbb{C}),$$

but this is very far from being surjective. When there are more X's, the group is unknown. (The group $\mathrm{Aut}(\mathbb{C}(X_1, \ldots, X_n)/\mathbb{C})$ is the group of *birational* automorphisms of $\mathbb{P}^n_{\mathbb{C}}$. It is called the *Cremona group.* Its study is part of algebraic geometry.)

In this section, we shall be concerned with the groups $\mathrm{Aut}(E/F)$ when E is a finite extension of F.

Proposition 3.8. *If E is a splitting field of a monic separable polynomial $f \in F[X]$, then* $\mathrm{Aut}(E/F)$ *has order* $[E : F]$.

Proof. Let $f = \prod f_i^{m_i}$, with the f_i monic irreducible and distinct. The splitting field of f is the same as the splitting field of $\prod f_i$. Hence we may assume f is a product of distinct monic separable irreducible polynomials, and hence has $\deg f$ distinct roots in E. Now Proposition 2.7b shows that there are $[E : F]$ distinct F-homomorphisms $E \to E$; they are automatically isomorphisms. □

Example 3.9. (a) Let $E = F[\alpha]$, $f(\alpha) = 0$; if f has no other root in E than α, then $\mathrm{Aut}(E/F) = 1$. For example, if $\sqrt[3]{2}$ denotes the real cube root of 2, then $\mathrm{Aut}(\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}) = 1$. Thus, in the proposition, it is essential that E be a *splitting* field.

(b) Let F be a field of characteristic $p \neq 0$, and let a be an element of F that is not a p^{th} power. The splitting field of $f = X^p - a$ is $F[\alpha]$ where α is the unique root of f. Then $\mathrm{Aut}(E/F) = 1$. Thus, in the proposition, it is essential that E be the splitting field of a *separable* polynomial.

When G is a group of automorphisms of a field E, we write

$$E^G = \mathrm{Inv}(G) = \{\alpha \in E \mid \sigma\alpha = \alpha, \text{ all } \sigma \in G\}.$$

It is a subfield of E, called the subfield of *G-invariants* of E or the subfield of E *fixed by* G.

We have maps

$$G \mapsto \mathrm{Inv}(G) \qquad F \mapsto \mathrm{Aut}(E/F).$$

Goal: Show that when E is the splitting field of a separable polynomial in $F[X]$ and $G = \mathrm{Aut}(E/F)$, then

$$H \mapsto \mathrm{Inv}(H), \qquad M \mapsto \mathrm{Aut}(E/M)$$

give a one-to-one correspondence between the set of intermediate fields M, $F \subset M \subset E$, and the set of subgroups H of G.

LEMMA 3.10 (E. Artin). *Let G be a finite group of automorphisms of a field E, and let $F = E^G$; then $[E:F] \leq (G:1)$.*

PROOF. Let $G = \{\sigma_1 = 1, \ldots, \sigma_m\}$, and let $\alpha_1, \ldots, \alpha_n$ be $n > m$ elements of E. We shall show that the α_i are linearly dependent over F. In the system

$$\begin{array}{rcl} \sigma_1(\alpha_1)x_1 + \cdots + \sigma_1(\alpha_n)x_n & = & 0 \\ \cdots \quad \cdots & & \\ \sigma_m(\alpha_1)x_1 + \cdots + \sigma_m(\alpha_n)x_n & = & 0 \end{array}$$

there are m equations and $n > m$ unknowns, and hence there are nontrivial solutions (in E). Choose a nontrivial solution $(c_1, \ldots, c_n)$ with the fewest nonzero elements. After renumbering the α_i's, we may suppose that $c_1 \neq 0$, and then (after multiplying by a scalar) that $c_1 = 1$. With these normalizations, we'll see that all $c_i \in F$. Hence the first equation (recall $\sigma_1 = 1$)

$$\alpha_1 c_1 + \cdots + \alpha_n c_n = 0$$

shows that the α_i are linearly dependent over F.

If not all c_i are in F, then $\sigma_k(c_i) \neq c_i$ for some i, k. On apply σ_k to the equations

$$\begin{array}{rcl} \sigma_1(\alpha_1)c_1 + \cdots + \sigma_1(\alpha_n)c_n & = & 0 \\ \cdots \quad \cdots & & \\ \sigma_m(\alpha_1)c_1 + \cdots + \sigma_m(\alpha_n)c_n & = & 0 \end{array}$$

and using that $\{\sigma_k\sigma_1, \ldots, \sigma_k\sigma_m\}$ is a permutation of $\{\sigma_1, \ldots, \sigma_m\}$, we find that $(1, \ldots, \sigma_k(c_i), \ldots)$ is also a solution to the system of equations. On subtracting it from the first, we obtain a solution $(0, \ldots, c_i - \sigma_k(c_i), \ldots)$, which is nonzero (look at the i^{th} coordinate), but has more zeros than the first solution (look at the first coordinate)—contradiction. □

3.3. **Separable, normal, and Galois extensions.**

An algebraic extension E/F is said to be *separable* if the minimum polynomial of every element of E is separable, i.e., doesn't have multiple roots (in a splitting field); equivalently, if every irreducible polynomial in $F[X]$ having a root in E is separable. Thus E/F is *inseparable* if and only if

(a) F is nonperfect, and in particular has characteristic $p \neq 0$, *and*
(b) there is an element α of E whose minimal polynomial is of the form $g(X^p)$, $g \in F[X]$.

For example, $E = \mathbb{F}_p(T)$ is an inseparable extension of $\mathbb{F}_p(T^p)$.

An algebraic extension E/F is *normal* if the minimum polynomial of every element of E splits in E; equivalently, if every irreducible polynomial $f \in F[X]$ having a root in E splits in E.

Thus if $f \in F[X]$ is irreducible of degree m and has a root in E, then

$$\left.\begin{array}{ccc} E/F \text{ separable} & \Longrightarrow & \text{roots of } f \text{ distinct} \\ & & \\ E/F \text{ normal} & \Longrightarrow & f \text{ splits in } E \end{array}\right\} \Longrightarrow f \text{ has } m \text{ distinct roots in } E.$$

Therefore, E/F is normal and separable if and only if, for each $\alpha \in E$, the minimum polynomial of α has $[F[\alpha]:F]$ distinct roots in E.

EXAMPLE 3.11. (a) The field $\mathbb{Q}[\sqrt[3]{2}]$, where $\sqrt[3]{2}$ is the real cube root of 2, is separable but not normal over $\mathbb{Q}$ (X^3-2 doesn't split in $\mathbb{Q}[\alpha]$).

(b) The field $\mathbb{F}_p(T)$ is normal but not separable over $\mathbb{F}_p(T^p)$—it is the splitting field of the inseparable polynomial $X^p - T^p$.

THEOREM 3.12. *Let E be an extension field of F. The following statements are equivalent:*

(a) *E is the splitting field of a separable polynomial $f \in F[X]$;*
(b) *$F = E^G$ for some finite group of automorphisms of E;*
(c) *E is normal and separable, and of finite degree, over F.*

Moreover, if E is as in (a), then $F = E^{\mathrm{Aut}(E/F)}$; if G and F are as in (b) then $G = \mathrm{Aut}(E/F)$.

PROOF. (a) $\implies$ (b). Let $G = \mathrm{Aut}(E/F)$, and let $F' = E^G \supset F$. Then E is also the splitting field of $f \in F'[X]$, and f is still separable when regarded as a polynomial over F'. Hence Proposition 3.8 shows that

$$[E:F'] = \#\,\mathrm{Aut}(E/F')$$

$$[E:F] = \#\,\mathrm{Aut}(E/F).$$

Since $\mathrm{Aut}(E/F') = \mathrm{Aut}(E/F) = G$, we conclude that $F = F'$, and so $F = E^{\mathrm{Aut}(E/F)}$.

(b) $\implies$ (c). By Artin's lemma, we know that $[E:F] \le (G:1)$; in particular, it is finite. Let $\alpha \in E$ and let f be the minimum polynomial of α; we have to prove that f splits into distinct factors in E. Let $\{\alpha_1 = \alpha, ..., \alpha_m\}$ be the orbit of α under G, and let

$$g(X) = \prod (X - \alpha_i) = X^m + a_1 X^{m-1} + \cdots + a_m.$$

Any $\sigma \in G$ merely permutes the α_i. Since the a_i are symmetric polynomials in the α_i, we find that $\sigma a_i = a_i$ for all i, and so $g(X) \in F[X]$. It is monic, and $g(\alpha) = 0$, and so $f(X)|g(X)$ (see p7). But also $g(X)|f(X)$, because each α_i is a root of $f(X)$ (if $\alpha_i = \sigma\alpha$, then applying σ to the equation $f(\alpha) = 0$ gives $f(\alpha_i) = 0$). We conclude that $f(X) = g(X)$, and so $f(X)$ splits into distinct factors in E.

(c) $\implies$ (a). Because E has finite degree over F, it is generated over F by a finite number of elements, say, $E = F[\alpha_1, ..., \alpha_m]$, $\alpha_i \in E$, α_i algebraic over F. Let f_i be the minimum polynomial of α_i over F. Because E is normal over F, each f_i splits in E, and so E is the splitting field of $f = \prod f_i$. Because E is separable over F, f is separable.

Finally, we have to show that if G is a finite group acting on a field E, then $G = \mathrm{Aut}(E/E^G)$. We know that:

- $[E:E^G] \le (G:1)$ (Artin),
- $G \subset \mathrm{Aut}(E/E^G)$, and,
- E is the splitting field of a separable polynomial in $E^G[X]$ (because $b \implies a$), and so (by 3.8) the order of $\mathrm{Aut}(E/E^G)$ is $[E:E^G]$.

Now the inequalities

$$[E:E^G] \le (G:1) \le (\mathrm{Aut}(E/E^G):1) = [E:E^G]$$

must be equalities, and so $G = \mathrm{Aut}(E/E^G)$. □

An extension of fields $E \supset F$ satisfying the equivalent conditions of the proposition is called a *Galois extension*, and $\mathrm{Aut}(E/F)$ is called the *Galois group* $\mathrm{Gal}(E/F)$ of E over F. Note that we have shown that $F = E^{\mathrm{Gal}(E/F)}$.

Remark 3.13. Let E be Galois over F with Galois group G, and let $\alpha \in E$. The elements $\alpha_1 = \alpha$, $\alpha_2, ..., \alpha_m$ of the orbit of α are called the *conjugates* of α. In the course of the proof of the the above theorem we showed that the minimum polynomial of α is $\prod(X - \alpha_i)$.

Corollary 3.14. *Every finite separable extension E of F is contained in a finite Galois extension.*

Proof. Let $E = F[\alpha_1, ..., \alpha_m]$. Let $f_i =$ minimum polynomial of α_i over F, and take E' to be the splitting field of $\prod f_i$ over F. □

Corollary 3.15. *Let $E \supset M \supset F$; if E is Galois over F, then it is Galois over M.*

Proof. We know E is the splitting field of some $f \in F[X]$; it is also the splitting field of f regarded as an element of $M[X]$. □

Remark 3.16. When we drop the assumption that E is separable over F, we can still say something. Let E be a finite extension of F. An element $\alpha \in E$ is said to be *separable* over F if its minimum polynomial over F is separable. The elements of E separable over F form a subfield E' of E that is separable over F; write $[E : F]_{\mathrm{sep}} = [E' : F]$ (*separable degree* of E over F). If Ω is an algebraically closed field containing F, then there are exactly $[E : F]_{\mathrm{sep}}$ F-homomorphisms $E \to \Omega$. When $E \supset M \supset F$ (finite extensions),

$$[E : F]_{\mathrm{sep}} = [E : M]_{\mathrm{sep}}[M : F]_{\mathrm{sep}}.$$

In particular,

$$E \text{ is separable over } F \iff E \text{ is separable over } M \text{ and } M \text{ is separable over } F.$$

3.4. The fundamental theorem of Galois theory.

Theorem 3.17 (Fundamental theorem of Galois theory). *Let E be a Galois extension of F, and let $G = \mathrm{Gal}(E/F)$. The maps $H \mapsto E^H$ and $M \mapsto \mathrm{Gal}(E/M)$ are inverse bijections between the set of subgroups of G and the set of intermediate fields between E and F:*

$$\{\text{subgroups of } G\} \leftrightarrow \{\text{intermediate fields } F \subset M \subset E\}.$$

Moreover:

(a) *The correspondence is inclusion-reversing, i.e., $H_1 \supset H_2 \iff E^{H_1} \subset E^{H_2}$.*
(b) *Indexes equal degrees, i.e., $(H_1 : H_2) = [E^{H_2} : E^{H_1}]$.*
(c) *The group $\sigma H \sigma^{-1} \leftrightarrow \sigma M$, i.e., $E^{\sigma H \sigma^{-1}} = \sigma(E^H)$; $\mathrm{Gal}(E/\sigma M) = \sigma \,\mathrm{Gal}(E/M)\sigma^{-1}$.*
(d) *The group H is normal in $G \iff E^H$ is normal (hence Galois) over F, in which case*

$$\mathrm{Gal}(E^H/F) = G/H.$$

Proof. Let H be a subgroup of G. We first have to show that $\mathrm{Gal}(E/E^H) = H$. But we have already observed that E is Galois over E^H, and Theorem 3.12 shows that $\mathrm{Gal}(E/E^H) = H$.

Next let M be an intermediate field, and let $H = \mathrm{Gal}(E/M)$. We have to show that $E^H = M$, but this is again proved in Theorem 3.12.

Thus we have proved that $\mathrm{Inv}(\cdot)$ and $\mathrm{Gal}(E/\cdot)$ are inverse bijections.

(a) We have the obvious implications:

$$H_1 \supset H_2 \implies E^{H_1} \subset E^{H_2} \implies \mathrm{Gal}(E/E^{H_1}) \supset \mathrm{Gal}(E/E^{H_2}).$$

But $\mathrm{Gal}(E/E^{H_i}) = H_i$.

(b) In the case $H_2 = 1$, the first equality follows from (3.8) and (3.12). The general case follows, using that

$$(H_1 : 1) = (H_1 : H_2)(H_2 : 1) \quad \text{and} \quad [E : E^{H_1}] = [E : E^{H_2}][E^{H_2} : E^{H_1}].$$

(c) If $H = \{\tau \in G \mid \tau\alpha = \alpha, \text{ all } \alpha \in M\}$, i.e., $H = \mathrm{Gal}(E/M)$, then $\sigma H \sigma^{-1} = \{\tau \in G \mid \tau\sigma\alpha = \sigma\alpha, \text{ all } \alpha \in M\}$, i.e., $\sigma H \sigma^{-1} = \mathrm{Gal}(E/\sigma M)$.

(d) Assume H to be normal in G, and let $M = E^H$. Because $\sigma H \sigma^{-1} = H$ for all $\sigma \in G$, we must have $\sigma M = M$ for all $\sigma \in G$, i.e., the action of G on E stabilizes M. We therefore have a homomorphism

$$\sigma \mapsto \sigma|M : G \to \mathrm{Aut}(M/F)$$

with kernel H. Let G' be the image. Then $F = M^{G'}$, and so M is Galois over F with Galois group G' (by Theorem 3.12).

Conversely, assume that M is normal over F, and write $M = F[\alpha_1, ..., \alpha_m]$. For $\sigma \in G$, $\sigma\alpha_i$ is a root of the minimum polynomial of α_i over F, and so lies in M. Hence $\sigma M = M$, and this implies that $\sigma H \sigma^{-1} = H$ (by (c)). □

Remark 3.18. The theorem shows that there is an order reversing bijection between the intermediate fields of E/F and the subgroups of G. Using this we can read off more results. For example let $M_1, M_2, \ldots, M_r$ be intermediate fields, and let H_i be the subgroup corresponding to M_i (i.e., $H_i = \mathrm{Gal}(E/M_i)$). Then (by definition) $M_1 M_2 \cdots M_r$ is the smallest field containing all M_i; hence it must correspond to the largest subgroup contained in all H_i, which is $\bigcap H_i$. Therefore

$$\mathrm{Gal}(E/M_1 \cdots M_r) = H_1 \cap ... \cap H_r.$$

We mention two further results (they are not difficult to prove):

1. Let E/F be Galois, and let L be any field containing F. Assume L and E are contained in some large field Ω. Then EL is Galois over L, E is Galois over $E \cap L$, and the map $\sigma \mapsto \sigma|E : \mathrm{Gal}(EL/L) \to \mathrm{Gal}(E/E \cap L)$ is an isomorphism.
2. Let E_1/F and E_2/F be Galois, with E_1 and E_2 subfields of some field Ω. Then E_1E_2 is Galois over F, and

$$\sigma \mapsto (\sigma|E_1, \sigma|E_2) : \mathrm{Gal}(E_1E_2/F) \to \mathrm{Gal}(E_1/F) \times \mathrm{Gal}(E_2/F)$$

   is injective with image $\{(\sigma_1, \sigma_2) \mid \sigma_1|E_1 \cap E_2 = \sigma_2|E_1 \cap E_2\}$.

Example 3.19. We analyse the extension $\mathbb{Q}[\zeta]/\mathbb{Q}$, where ζ is the primitive 7^{th} root of 1, say $\zeta = e^{2\pi i/7}$. Then $\mathbb{Q}[\zeta]$ is the splitting field of the irreducible polynomial

$$X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$$

(see 1.31), and so is Galois of degree 6 over $\mathbb{Q}$. For any $\sigma \in G$, $\sigma\zeta = \zeta^i$, some i, $1 \le i \le 6$, and the map $\sigma \mapsto i$ defines an isomorphism $\mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q}) \to (\mathbb{Z}/7\mathbb{Z})^\times$. Let σ be the element of $\mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q})$ such that $\sigma\zeta = \zeta^3$. Then σ generates $\mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q})$ because the class of 3 in $(\mathbb{Z}/7\mathbb{Z})^\times$ generates it (the powers of 3 mod 7 are 3, 2, 6, 4, 5, 1). We investigate the subfields of $\mathbb{Q}[\zeta]$ corresponding to the subgroups $< \sigma^3 >$ and $< \sigma^2 >$.

Note that $\sigma^3\zeta = \zeta^6 = \bar{\zeta}$ (complex conjugate of ζ). The subfield of $\mathbb{Q}[\zeta]$ corresponding to $<\sigma^3>$ is $\mathbb{Q}[\zeta+\bar{\zeta}]$, and $\zeta+\bar{\zeta} = 2\cos\frac{2\pi}{7}$. Since $<\sigma^3>$ is a normal subgroup of $<\sigma>$, $\mathbb{Q}[\zeta+\bar{\zeta}]$ is Galois over $\mathbb{Q}$, with Galois group $<\sigma> / <\sigma^3>$. The conjugates of $\alpha_1 = \zeta+\bar{\zeta}$ are $\alpha_3 = \zeta^3+\zeta^{-3}$, $\alpha_2 = \zeta^2+\zeta^{-2}$. Direct calculation shows that

$$\sum \alpha_i = \sum_{i=1}^{6} \zeta^i = -1,$$

$$\alpha_1\alpha_2\alpha_3 = (\zeta+\zeta^6)(\zeta^2+\zeta^5)(\zeta^3+\zeta^4) = (\zeta+\zeta^3+\zeta^4+\zeta^6)(\zeta^3+\zeta^4) = (\zeta^4+\zeta^6+1+\zeta^2+\zeta^5+1+\zeta+\zeta^3) = 1.$$

$$\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3 = -2.$$

Hence the minimum polynomial of $\zeta+\bar{\zeta}$ is

$$g(X) = X^3+X^2-2X-1.$$

The minimum polynomial of $\cos\frac{2\pi}{7} = \frac{\alpha_1}{2}$ is therefore

$$\frac{g(2X)}{8} = X^3+X^2/2-X/2-1/8.$$

The subfield of $\mathbb{Q}[\zeta]$ corresponding to $<\sigma^2>$ is generated by $\beta = \zeta+\zeta^2+\zeta^4$. Let $\beta' = \sigma\beta$. Then $(\beta-\beta')^2 = -7$. Hence the field fixed by $<\sigma^2>$ is $\mathbb{Q}[\sqrt{-7}]$.

Example 3.20. We compute the Galois group of the splitting field E of $X^5-2 \in \mathbb{Q}[X]$. Recall (from the Homework) that $E = \mathbb{Q}[\zeta,\alpha]$ where ζ is a primitive 5^{th} root of 1, and α is a root of X^5-2. For example, we could take E to be the splitting field of X^5-2 in $\mathbb{C}$, with $\zeta = e^{2\pi i/5}$ and α equal to the real 5^{th} root of 2. We have the picture:

$$\begin{tikzcd}[column sep=small] & \mathbb{Q}[\zeta,\alpha] \arrow[dl, dash, "N"'] \arrow[dr, dash, "H"] & \\ \mathbb{Q}[\zeta] \arrow[dr, dash, "G/N"'] & & \mathbb{Q}[\alpha] \arrow[dl, dash] \\ & \mathbb{Q} & \end{tikzcd}$$

The degrees

$$[\mathbb{Q}[\zeta]:\mathbb{Q}] = 4, \quad [\mathbb{Q}[\alpha]:\mathbb{Q}] = 5.$$

Because 4 and 5 are relatively prime,

$$[\mathbb{Q}[\zeta,\alpha]:\mathbb{Q}] = 20.$$

Hence $G = \mathrm{Gal}(\mathbb{Q}[\zeta,\alpha]/\mathbb{Q})$ has order 20, and the subgroups N and H corresponding to $\mathbb{Q}[\zeta]$ and $\mathbb{Q}[\alpha]$ have orders 5 and 4 respectively (because $N = \mathrm{Gal}(\mathbb{Q}[\zeta,\alpha]/\mathbb{Q}[\zeta]\ldots)$. Because $\mathbb{Q}[\zeta]$ is normal over $\mathbb{Q}$ (it is the splitting field of X^5-1), N is normal in G. Because $\mathbb{Q}[\zeta]\cdot\mathbb{Q}[\alpha] = \mathbb{Q}[\zeta,\alpha]$, we have $H\cap N = 1$ (see 3.18), and so $G = N \rtimes_\theta H$. We have $H \approx G/N \approx (\mathbb{Z}/5\mathbb{Z})^\times$, which is cyclic, being generated by the class of 2. Let τ be the generator of H corresponding to 2 under this isomorphism, and let σ be a generator of N. Thus $\sigma(\alpha)$ is another root of X^5-2, which we can take to be $\zeta\alpha$ (after possibly replacing σ by a power). Hence:

$$\begin{cases} \tau\zeta &= \zeta^2 \\ \tau\alpha &= \alpha \end{cases} \begin{cases} \sigma\zeta &= \zeta \\ \sigma\alpha &= \zeta\alpha. \end{cases}$$

Note that $\tau\sigma\tau^{-1}(\alpha) = \tau\sigma\alpha = \tau(\zeta\alpha) = \zeta^2\alpha$ and it fixes ζ; therefore $\tau\sigma\tau^{-1} = \sigma^2$. Thus G has generators σ and τ and defining relations

$$\sigma^5 = 1, \quad \tau^4 = 1, \quad \tau\sigma\tau^{-1} = \sigma^2.$$

The subgroup H has five conjugates, which correspond to the five fields $\mathbb{Q}[\zeta^i\alpha]$,

$$\sigma^i H\sigma^{-i} \leftrightarrow \sigma^i\mathbb{Q}[\alpha] = \mathbb{Q}[\zeta^i\alpha], \qquad 1 \leq i \leq 5.$$

Definition 3.21. An extension $E \supset F$ is called a *cyclic*, *abelian, ...,* *solvable* extension if it is Galois with cyclic, abelian, ..., solvable Galois group.

3.5. Constructible numbers revisited.

Earlier, we showed that a number α is constructible if and only if it is contained in a field $\mathbb{Q}[\sqrt{a_1}]\cdots[\sqrt{a_r}]$. In particular

$$\alpha \text{ constructible } \implies [\mathbb{Q}[\alpha]:\mathbb{Q}] = 2^s \text{ some } s.$$

Now we can prove a partial converse to this last statement.

Theorem 3.22. *If α is contained in a Galois extension of $\mathbb{Q}$ of degre 2^r then it is constructible.*

Proof. Suppose $\alpha \in E$ where E is Galois over $\mathbb{Q}$ of degree 2^r, and let $G = \mathrm{Gal}(E/\mathbb{Q})$. From a theorem on the structure of p-groups, we know there will be a sequence of groups

$$\{1\} \subset G_1 \subset G_2 \subset \cdots \subset G_r = G$$

with G_i/G_{i-1} of order 2. Correspondingly, there will be a sequence of fields,

$$\mathbb{Q} \subset E_1 \subset E_2 \subset \cdots \subset E_r = E$$

with E_i of degree 2 over E_{i-1}.

But (see below), every quadratic extension is obtained by extracting a square root, and we know that square roots can be constructed using only a ruler and compass. This proves the theorem. □

Lemma 3.23. *Let E/F be a quadratic extension of fields of characteristic $\neq 2$. Then $E = F[\sqrt{d}]$ for some $d \in F$.*

Proof. Let $\alpha \in E$, $\alpha \notin F$, and let $X^2 + bX + c$ be the minimum polynomial of α. The $\alpha = \frac{-b\pm\sqrt{b^2-4c}}{2}$, and so $E = F[\sqrt{b^2-4c}]$. □

Corollary 3.24. *If p is a prime of the form 2^k+1, then $\cos\frac{2\pi}{p}$ is constructible.*

Proof. The field $\mathbb{Q}[e^{2\pi i/p}]$ is Galois over $\mathbb{Q}$ with Galois group $G \approx (\mathbb{Z}/p\mathbb{Z})^\times$, which has order $p-1 = 2^k$. □

Thus a regular p-gon, p prime, is constructible if and only if p is a Fermat prime, i.e., of the form $2^{2^r}+1$. For example, we have proved that the regular 65537-polygon is constructible, without (happily) having to exhibit an explicit formula for $\cos\frac{2\pi}{65537}$.

3.6. Galois group of a polynomial.

If the polynomial $f \in F[X]$ is separable, then its splitting field E is Galois over F, and we call $\mathrm{Gal}(E/F)$ the *Galois group G_f* of f.

Let $f = \prod_{i=1}^n (X-\alpha_i)$ in the splitting field E. We know elements of $\mathrm{Gal}(E/F)$ map roots of f to roots of f, i.e., they map the set $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ into itself. Since they are automorphisms, they define permutations of $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$. As $E = F[\alpha_1, ..., \alpha_n]$, an element of $\mathrm{Gal}(E/F)$ is uniquely determined by its action on $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$. Thus G_f can be identified with a subset of $\mathrm{Sym}(\{\alpha_1, \alpha_2, \ldots, \alpha_n\}) \approx S_n$. From the definitions, one sees that G_f consists of the permutations σ of $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ with the property

$$P \in F[X_1, \ldots, X_n], \quad P(\alpha_1, \ldots, \alpha_n) = 0 \implies P(\sigma\alpha_1, \ldots, \sigma\alpha_n) = 0.$$

This gives a description of G_f without mentioning fields or abstract groups (neither of which were available to Galois).

Note that $(G_f : 1) \leq \deg(f)!$.

3.7. **Solvability of equations.**

Let f be a polynomial. We say the equation $f(X) = 0$ is *solvable* (by extracting radicals) if there is a tower

$$F = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_m$$

such that

(a) $F_i = F_{i-1}[\alpha_i]$, $\alpha_i^{m_i} \in F_{i-1}$;
(b) F_m contains a splitting field for f.

THEOREM 3.25. *(Galois, 1832) Let F be a field of characteristic zero. The equation $f = 0$ is solvable if and only if the Galois group of f is solvable.*

We shall prove this later. Also we shall exhibit polynomials $f(X) \in \mathbb{Q}[X]$ with Galois group S_n, which therefore are not solvable when $n \geq 5$.

REMARK 3.26. If F has characteristic p, then the theorem fails for two reasons:

(i) f may not be separable, and so not have a Galois group;
(ii) $X^p - X - a$ is not solvable by radicals.

If the definition of solvable is changed to allow extensions of the type in (ii) in the chain, and f is required to be separable then the theorem becomes true in characteristic p.

4. Computing Galois Groups.

In this section, we investigate general methods for computing Galois groups.

4.1. When is $G_f \subset A_n$?

Consider a polynomial

$$f(X) = X^n + a_1X^{n-1} + \cdots + a_n$$

and let $f(X) = \prod_{i=1}^n (X - \alpha_i)$ in some splitting field. Set

$$\Delta(f) = \prod_{1\leq i<j\leq n} (\alpha_i - \alpha_j), \qquad D(f) = \Delta(f)^2 = \prod_{1\leq i<j\leq n} (\alpha_i - \alpha_j)^2.$$

Note that $D(f) \neq 0$ if f has a only simple roots, i.e., if f is separable with no multiple factors. Identify G_f with a subgroup of $\mathrm{Sym}(\{\alpha_1, \ldots, \alpha_n\})$ (as in §3.6).

Proposition 4.1. *Assume f is separable, and let $\sigma \in G_f$.*

(a) $\sigma\Delta(f) = \mathrm{sign}(\sigma)\Delta(f)$*, where* $\mathrm{sign}(\sigma)$ *is the signature of* σ*.*
(b) $\sigma D(f) = D(f)$*.*

Proof. The first equation follows immediately from the definition of the signature of σ (see Groups, p31), and the second equation is obtained by squaring the first. □

Corollary 4.2. *Let $f(X) \in F[X]$ be of degree n and have only simple roots. Let F_f be a splitting field for f, so that $G_f = \mathrm{Gal}(F_f/F)$.*

(a) *The discriminant $D(f) \in F$.*
(b) *The subfield of F_f corresponding to $A_n \cap G_f$ is $F[\Delta(f)]$. Hence*

$$G_f \subset A_n \iff \Delta(f) \in F \iff D(f) \text{ is a square in } F.$$

Proof. (a) We know that $D(f)$ is an element of F_f fixed by $G_f =_{df} \mathrm{Gal}(F_f/F)$. Therefore it lies in F (by the Fundamental Theorem of Galois Theory).

(b) Because f has simple roots, $\Delta(f) \neq 0$, and so the formula $\sigma\Delta(f) = \mathrm{sign}(\sigma)\Delta(f)$ shows that σ fixes $\Delta(f) \iff \sigma \in A_n$. Therefore $G_f \cap A_n$ is the subgroup of G_f corresponding to $F[\Delta(f)]$, and so $G_f \cap A_n = G_f \iff F[\Delta(f)] = F$. □

The discriminant of f can be expressed as a universal polynomial in the coefficients of f—we shall prove this later. For example:

$$\begin{aligned} D(aX^2 + bX + c) &= b^2 - 4ac \\ D(X^3 + bX + c) &= -4b^3 - 27c^2. \end{aligned}$$

By completing the cube, one can put any cubic polynomial in this form.

The formulas for the discriminant rapidly become very complicated, for example, that for $X^5 + aX^4 + bX^3 + cX^2 + dX + e$ has about 60 terms. Fortunately, Maple knows them: the syntax is "`discrim(f,X);`" where f is a polynomial in the variable X.

Remark 4.3. Suppose $F \subset \mathbb{R}$. Then $D(f)$ will not be a square if it is negative. It is known that the sign of $D(f)$ is $(-1)^s$ where $2s$ is the number of nonreal roots of f in $\mathbb{C}$. Thus if s is odd, then G_f is not contained in A_n. This can be proved more directly by noting that complex conjugation will act on the roots as the product of s transpositions (cf. the proof of Proposition 4.13). Of course the converse is not true: when s is even, G_f is not necessarily contained in A_n.

4.2. When is G_f transitive?

PROPOSITION 4.4. *Let $f(X) \in F[X]$ have only simple roots. Then $f(X)$ is irreducible if and only if G_f permutes the roots of f transitively.*

PROOF. $\Longrightarrow$: If α and β are two roots of $f(X)$ in a splitting field F_f for f, then they both have $f(X)$ as their minimum polynomial, and so there is a natural F-isomorphism $F[\alpha] \to F[\beta]$, namely,

$$F[\alpha] \approx F[X]/(f(X)) \approx F[\beta], \qquad \alpha \leftrightarrow X \leftrightarrow \beta.$$

Write $F_f = F[\alpha_1, \alpha_2, ...]$ with $\alpha_1 = \alpha$ and $\alpha_2, \alpha_3, \ldots$ the other roots of $f(X)$. Then the F-isomorphism $F[\alpha] \to F[\beta]$ extends (step by step) to a homomorphism $F[\alpha_1, \alpha_2, ...] \to F_f$ (see 2.7), which must be an isomorphism.

$\Longleftarrow$: Let $g(X) \in F[X]$ be an irreducible factor of f, and let α be one of its roots. If β is a second root of f, then (by assumption) $\beta = \sigma\alpha$ for some $\sigma \in G_f$. Now the equation

$$0 = \sigma g(\alpha) \overset{g(X)\in F[X]}{=} g(\sigma\alpha)$$

shows that β is also a root of g, and we see that we must have $f(X) = g(X)$. □

Note that when $f(X)$ is irreducible of degree n, then $n|(G_f : 1)$ because $[F[\alpha] : F] = n$ and $[F[\alpha] : F]|[F_f : F] = (G_f : 1)$. Thus G_f is a transitive subgroup of S_n whose order is divisible by n.

4.3. Polynomials of degree ≤ 3.

EXAMPLE 4.5. Let $f(X) \in F[X]$ be a polynomial of degree 2. Then f is inseparable $\Longleftrightarrow$ F has characteristic 2 and $f(X) = X^2 - a$ for some $a \in F \setminus F^2$. If f is separable, then $G_f = 1 (= A_2)$ or S_2 according as $D(f)$ is a square in F or not.

EXAMPLE 4.6. Let $f(X) \in F[X]$ be a polynomial of degree 3. We can assume f to be irreducible, for otherwise we are essentially back in the previous case. Then f is inseparable $\Longleftrightarrow$ F has characteristic 3 and $f(X) = X^3 - a$ some $a \in F \setminus F^3$. If f is separable, then G_f is a transitive subgroup of S_3 whose order is divisible by 3. There are only two possibilities: $G_f = A_3 (=< (123) >)$ or S_3 according as $D(f)$ is a square in F or not.

For example, $X^3 - 3X + 1 \in \mathbb{Q}[X]$ is irreducible (apply 1.4), its discriminant is $-4(-3)^3 - 27 = 81 = 9^2$, and so its Galois group is A_3.

On the other hand, $X^3 + 3X + 1 \in \mathbb{Q}[X]$ is also irreducible (apply 1.4), but its discriminant is -135 which is not a square in $\mathbb{Q}$, and so its Galois group is S_3.

4.4. Quartic polynomials.

Let $f(X)$ be a quartic polynomial, and assume that the roots of f are simple. In order to determine G_f we shall exploit the fact that S_4 has

$$V = \{1, (12)(34), (13)(24), (14)(23)\}$$

as a normal subgroup—it is normal because it contains all elements of type 2+2—see Groups p34. Let E be the splitting field of f, and let $f(X) = \prod(X - \alpha_i)$ in E. We identify the

Galois group G_f of f with a subgroup of the symmetric group $S_4 = \mathrm{Sym}(\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\})$. Consider the partially symmetric elements

$$\begin{aligned} \alpha &= \alpha_1\alpha_2 + \alpha_3\alpha_4 \\ \beta &= \alpha_1\alpha_3 + \alpha_2\alpha_4 \\ \gamma &= \alpha_1\alpha_4 + \alpha_2\alpha_3. \end{aligned}$$

They are distinct elements of E because the α_i are distinct, e.g.,

$$\alpha - \beta = \alpha_1(\alpha_2 - \alpha_3) + \alpha_4(\alpha_3 - \alpha_2) = (\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3).$$

The group $\mathrm{Sym}(\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\})$ permutes $\{\alpha, \beta, \gamma\}$ transitively. The stabilizer of each of α, β, γ must therefore be a subgroup of index 3 in S_4, and hence has order 8. For example, the stabilizer of β is $< (1234), (13) >$. Groups of order 8 in S_4 are Sylow 2-subgroups. There are three of them, all isomorphic to D_4. By the Sylow theorems, V is contained in a Sylow 2-subgroup, and, because they are conjugate and it is normal, it must be contained in all three. It follows that V is the intersection of the three Sylow 2-subgroups. Each Sylow 2-subgroup stabilizes exactly one of α, β, or γ, and therefore their intersection V is the subgroup of S_4 fixing α, β, and γ.

Lemma 4.7. *The field $M = F[\alpha, \beta, \gamma]$ corresponds to $G_f \cap V$. Hence M is Galois over F, with Galois group $G/G \cap V$.*

Proof. The first statement follows from the above discussion, and the second follows from the Fundamental Theorem of Galois Theory. □

Picture:

$$\begin{tikzcd} E \arrow[d, dash, "G\cap V"'] & 1 \arrow[d, dash] \\ M \arrow[d, dash, "G/G\cap V"'] & G\cap V \arrow[d, dash] \\ F & G \end{tikzcd}$$

Let $g(X) = (X - \alpha)(X - \beta)(X - \gamma) \in M[X]$—it is called the *resolvant cubic* of f. Any permutation of the α_i (*a fortiori,* any element of G_f) merely permutes α, β, γ, and so fixes $g(X)$. Therefore (by the Fundamental Theorem) $g(X)$ has coefficients in F. More explicitly, we have:

Lemma 4.8. *If $f = X^4+bX^3+cX^2+dX+e$, then $g = X^3-cX^2+(bd-4e)X-b^2e+4ce-d^2$. The discriminants of f and g are equal.*

Proof. Compute everything in terms of the α_i's. (Cf. Hungerford, V.4.10.) □

Now let f be an irreducible separable quartic. Then $G = G_f$ is a transitive subgroup of S_4 whose order is divisible by 4. There are the following possibilities:

G	$(G \cap V : 1)$	$(G : V \cap G)$
S_4	4	6
A_4	4	3
V	4	1
D_4	4	2
C_4	2	2

$$(G \cap V : 1) = [E : M], \quad (G : V \cap G) = [M : F].$$

Note that G can't, for example, be the group generated by (12) and (34) because this is not transitive. The groups of type D_4 are the Sylow 2-subgroups discussed above, and the groups of type C_4 are those generated by cycles of length 4.

We can compute $(G : V \cap G)$ from the resolvant cubic g, because $G/V \cap G = \mathrm{Gal}(M/F)$, and M is the splitting field of g. Once we know $(G : V \cap G)$, we can deduce G except in the case that it is 2. If $[M : F] = 2$, then $G \cap V = V$ or C_2. Only the first group acts transitively on the roots of f, and so (from 4.4) we see that (in this case) $G = D_4$ or C_4 according as f is irreducible or not in $M[X]$.

Example 4.9. Consider $f(X) = X^4 + 4X^2 + 2 \in \mathbb{Q}[X]$. It is irreducible by Eisenstein's criterion, and its resolvant cubic is $(X - 4)(X^2 - 8)$; thus $M = \mathbb{Q}[\sqrt{2}]$. Note that f, when regarded as a polynomial in X^2, factors over M; hence $G_f = C_4$.

Example 4.10. Consider $f(X) = X^4 - 10X^2 + 4 \in \mathbb{Q}[X]$. One can check directly (using 1.6) that it is irreducible, and its resolvant cubic is $(X + 10)(X + 4)(X - 4)$. Hence $G_f = V$.

Example 4.11. Consider $f(X) = X^4 - 2 \in \mathbb{Q}[X]$. It is irreducible by Eisenstein's criterion, and its resolvant cubic is $g(X) = X^3 + 8X$. Hence $M = \mathbb{Q}[i\sqrt{2}]$. One can check that f is irreducible over M, and so its Galois group is D_4.

Alternatively, analyze the equation as in (3.20).

Maple knows how to factor polynomials over $\mathbb{Q}$ and over $\mathbb{Q}[\alpha]$ where α is a root of an irreducible polynomial. To learn the syntax, type: `?Factor`.

4.5. Examples of polynomials with S_p as Galois group over $\mathbb{Q}$.

The next lemma gives a criterion for a subgroup of S_p to be the whole of S_p.

Lemma 4.12. *Let p be a prime number. Then S_p is generated by any transposition and any p-cycle.*

Proof. After renumbering, we may assume that the transposition is $\tau = (12)$. Let the p-cycle be $\sigma = (i_1 \cdots i_p)$; we may choose to write σ so that 1 occurs in the first position, $\sigma = (1\, i_2 \cdots i_p)$. Now some power of σ will map 1 to 2 and will still be a p-cycle (here is where we use that p is prime). After replacing σ with the power, we may suppose $\sigma = (1\, 2\, j_3\, \ldots j_p)$, and after renumbering again, we may suppose $\sigma = (1\,2\,3 \ldots p)$. Then we'll have $(2\,3)$, $(3\,4)$, $(4\,5), \ldots$ in the group generated by σ and τ, and these elements generated S_p. □

Proposition 4.13. *Let f be an irreducible polynomial of prime degree p in $\mathbb{Q}[X]$. If f splits in $\mathbb{C}$ and has exactly two nonreal roots, then $G_f = S_p$.*

Proof. Let $E \subset \mathbb{C}$ be the splitting field of f, and let $\alpha \in E$ be a root of f. Because f is irreducible, $[\mathbb{Q}[\alpha] : \mathbb{Q}] = \deg f = p$, and so $p | [E : \mathbb{Q}] = (G_f : 1)$. Therefore G_f contains an element of order p (Cauchy's theorem), but the only elements of order p in S_p are p-cycles (here we use that p is prime again).

Let σ be complex conjugation on $\mathbb{C}$. Then σ transposes the two nonreal roots of $f(X)$ and fixes the rest. Therefore $G_f \subset S_p$ contains a transposition and a p-cycle, and so is the whole of S_p. □

It remains to construct polynomials satisfying the conditions of the Proposition.

EXAMPLE 4.14. Let $p \geq 5$ be a prime number. Choose a positive even integer m and even integers

$$n_1 < n_2 < \cdots < n_{p-2}.$$

Let $f(X) = g(X) - 2$, where

$$g(X) = (X^2 + m)(X - n_1)...(X - n_{p-2}).$$

When we write $f(X) = X^p + a_1 X^{p-1} + \cdots + a_p$, then all a_i are even, and $a_p = -(m \prod n_i) - 2$ is not divisible by 4. Hence Eisenstein's criterion implies that $f(X)$ is irreducible.

The polynomial $g(X)$ certainly has exactly two nonreal roots. Its graph crosses the x-axis exactly $p-2$ times, and its maxima and minima all have absolute value > 2 (because its values at odd integers have absolute value > 2). Hence the graph of $f(X) = g(X) - 2$ also crosses the x-axis exactly $p-2$ times.

4.6. **Finite fields.**

Let $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, the field of p elements. As we noted in §1.2, any other field E of characteristic p contains a copy of $\mathbb{F}_p$, namely, $\{m1_E \mid m \in \mathbb{Z}\}$. No harm results if we identify $\mathbb{F}_p$ with this subfield of E.

Let E be a field of degree n over $\mathbb{F}_p$. Then E has $q = p^n$ elements, and so $E^\times$ is a group of order $q - 1$. Hence the nonzero elements of E are roots $X^{q-1} - 1$, and all elements of E (including 0) are roots of $X^q - X$. Hence E is a splitting field for $X^q - X$, and so any two fields with q elements are isomorphic.

Now let E be the splitting field of $f(X) = X^q - X$, $q = p^n$. The derivative $f'(X) = -1$, which is relatively prime to $f(X)$ (in fact, to every polynomial), and so $f(X)$ has q distinct roots in E. Let S be the set of its roots. Then S is obviously closed under multiplication and the formation of inverses, but it is also closed under subtraction: if $a^q - a = 0$ and $b^q - b = 0$, then

$$(a - b)^q = a^q - b^q = a - b.$$

Hence S is a field, and so $S = E$. In particular, E has p^n elements.

PROPOSITION 4.15. *For each power $q = p^n$ there is a field $\mathbb{F}_q$ with q elements. It is the splitting field of $X^q - X$, and hence any two such fields are isomorphic. Moreover, $\mathbb{F}_q$ is Galois over $\mathbb{F}_p$ with cyclic Galois group generated by the Frobenius automorphism $\sigma(a) = a^p$.*

PROOF. Only the final statement remains to be proved. The field $\mathbb{F}_q$ is Galois over $\mathbb{F}_p$ because it is the splitting field of a separable polynomial. We noted in (1.3) that $\sigma = (x \mapsto x^p)$ is an automorphism of $\mathbb{F}_q$. It has order n, and $a \in \mathbb{F}_q$ is fixed by σ if and only if $a^p = a$. But $\mathbb{F}_p$ consists exactly of such elements, and so the fixed field of $< \sigma >$ is $\mathbb{F}_p$. This proves that $< \sigma >= \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$. □

COROLLARY 4.16. *Let E be a field with p^n elements. Then E contains exactly one field with p^m elements for each $m|n$, $m \geq 0$, and E is Galois over that field.*

PROOF. We know that E is Galois over $\mathbb{F}_p$ and that $\mathrm{Gal}(E/\mathbb{F}_p)$ is the cyclic group of order n generated by σ. The subgroups of $< \sigma >$ are the groups $< \sigma^m >$ with $m|n$. The fixed field of $< \sigma^m >$ is $\mathbb{F}_{p^m}$. □

COROLLARY 4.17. *Every extension of finite fields is simple.*

Proof. Consider $E \supset F$. Then $E^{\times}$ is a finite subgroup of the multiplicative group of a field, and hence is cyclic (see Exercise 3). If ζ generates $E^{\times}$ as a multiplicative group, then clearly $E = \mathbb{F}_p[\zeta]$. □

Corollary 4.18. *Each monic irreducible polynomial of degree $d|n$ in $\mathbb{F}_p[X]$ occurs exactly once as a factor of $X^{p^n} - X$.*

Proof. First, the factors of $X^{p^n} - X$ are distinct because it has no common factor with its derivative. If $f(X)$ is irreducible of degree d, then $f(X)$ has a root in a field of degree d over $\mathbb{F}_p$. But the splitting field of $X^{p^n} - X$ contains a copy of every field of degree d over $\mathbb{F}_p$ with $d|n$. Hence some root of $X^{p^n} - X$ is also a root of $f(X)$, and therefore $f(X)|X^{p^n} - X$. □

Maple factors polynomials modulo p very quickly. The syntax is "`Factor(f(X)) mod p;`". Thus, for example, to obtain a list of all monic polynomials of degree $1, 2$, or 4 over $\mathbb{F}_5$, ask Maple to factor $X^{625} - X$.

Let $\mathbb{F}$ be an algebraic closure of $\mathbb{F}_p$. Then $\mathbb{F}$ contains one field $\mathbb{F}_{p^n}$ for each integer $n \geq 1$—it consists of all roots of $X^{p^n} - X$—and $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n} \iff m|n$. The partially ordered set of finite subfields of $\mathbb{F}$ is isomorphic to the set of integers $n \geq 1$ partially ordered by divisibility.

Finite fields were sometimes called *Galois fields,* and $\mathbb{F}_q$ used to be denoted $GF(q)$ (it still is in Maple). Maple contains a "Galois field package" to do computations in finite fields. For example, it can find a primitive element for $\mathbb{F}_q$ (i.e., a generator for $\mathbb{F}_q^{\times}$). To start it, type: `readlib(GF);`.

4.7. **Computing Galois groups over $\mathbb{Q}$.**

We sketch a practical method for computing Galois groups over $\mathbb{Q}$ and similar fields. Our first result generalizes Proposition 4.4.

Proposition 4.19. *Let $f(X)$ be a monic separable polynomial in $F[X]$ of degree m with distinct roots, and suppose that $G_f \subset S_m$ has r orbits with $m_1, \ldots, m_r$ elements respectively (so that $m = m_1 + \cdots + m_r$); then f factors as $f = f_1 \cdots f_r$ with f_i irreducible of degree m_i.*

Proof. Let $\alpha_1, \ldots, \alpha_m$ be the distinct roots of $f(X)$. For $S \subset \{1, 2, \ldots, m\}$, consider $f_S = \prod_{i \in S}(X - \alpha_i)$. This polynomial divides $f(X)$ in $F_f[X]$, and it is fixed under the action of G_f (and hence has coefficients in F) if and only if S is stable under G_f. Therefore the irreducible factors are the polynomials f_S corresponding to minimal subsets S of $\{1, \ldots, m\}$ stable under G, but such sets S are precisely the orbits of G in $\{1, \ldots, m\}$. □

Now suppose F is finite, with p^n elements say, and let E be the splitting field of f. The Galois group of E over F is generated by the Frobenius automorphism $\sigma : x \mapsto x^{p^n}$. When we regard σ as a permutation of the roots of f, then its factors in the cycle decomposition of σ correspond to the distinct orbits of σ. Hence, if the degrees of the distinct irreducible factors of f are $m_1, m_2, \ldots, m_r$, then σ has a cycle decompostion of type

$$m_1 + \cdots + m_r = m.$$

Lemma 4.20. *Let R be a unique factorization domain with field of fractions F, and let f be a monic polynomial in $R[X]$. Let P be a prime ideal in R, and let $\bar{f}$ be the image of f in $(R/P)[X]$. Assume neither f nor $\bar{f}$ has a multiple root. Then the roots $\alpha_1, \ldots, \alpha_m$ of f lie in R, and their reductions $\bar{\alpha}_i$ modulo P are the roots of $\bar{f}$. Moreover $G_{\bar{f}} \subset G_f$ when both are identified with subgroups of* $\mathrm{Sym}\{\alpha_1, \ldots, \alpha_m\} = \mathrm{Sym}\{\bar{\alpha}_1, \ldots, \bar{\alpha}_m\}$.

PROOF. Omitted—see van der Waerden, Modern Algebra, I, §61 (second edition) or Math 676 (Algebraic Number Theory). □

On combining these results, we obtain the following theorem.

THEOREM 4.21 (Dedekind). *Let $f(X) \in \mathbb{Z}[X]$ be a monic polynomial of degree m, and let p be a prime such that $f \mod p$ has simple roots (equivalently, $D(f)$ is not divisible by p). Suppose that $\bar{f} = \prod f_i$ with f_i irreducible of degree m_i in $\mathbb{F}_p[X]$. Then G_f contains an element whose cycle decomposition corresponds to the partition:*

$$m = m_1 + \cdots + m_r.$$

EXAMPLE 4.22. Consider X^5-X-1. Modulo 2, this factors as $(X^2+X+1)(X^3+X^2+1)$, and modulo 3 it is irreducible. Hence G_f contains (12345) and $(ik)(lmn)$, and hence also $((ik)(lmn))^3 = (ik)$. Therefore $G_f = S_5$.

LEMMA 4.23. *A transitive subgroup of $H \subset S_n$ containing a transposition and an $(n-1)$-cycle is equal to S_n.*

PROOF. Let $(123\ldots n-1)$ be the $(n-1)$-cycle. By virtue of the transitivity, the transposition can be transformed into (in), some $1 \leq i \leq n-1$. Now the $(n-1)$-cycle and its powers will transform this into $(1n), (2n), \ldots, (n-1\, n)$, and these elements obviously generate S_n. □

EXAMPLE 4.24. Select monic polynomials of degree n, f_1, f_2, f_3 with coefficients in $\mathbb{Z}$ such that:

(a) f_1 is irreducible modulo 2;
(b) $f_2 =$ (degree 1)(irreducible of degree $n-1$) mod 3;
(c) $f_3 =$ (irreducible of degree 2)(product of 1 or 2 irreducible polys of odd degree) mod 5.

We choose them to have distinct roots. Take

$$f = -15f_1 + 10f_2 + 6f_3.$$

Then

(i) G_f is transitive (it contains an n-cycle because $f \equiv f_1 \mod 2$);
(ii) G_f contains a cycle of length $n-1$ (because $f \equiv f_2 \mod 3$);
(iii) G_f contains a transposition (because $f \equiv f_3 \mod 5$, and so it contains the product of a transposition with a commuting element of odd order; on raising this to an appropriate odd power, we are left with the transposition). Hence G_f is S_n.

This gives the following strategy for computing Galois groups over $\mathbb{Q}$. Factor f modulo a sequence of primes p not dividing $D(f)$ to determine the cycle types of the elements in G_f—a difficult theorem in number theory, the effective Chebotarev density theorem, says that if a cycle type occurs in G_f, then this will be seen by looking modulo a set of prime numbers of positive density, and will occur for a prime less than some bound. Now look up a table of transitive subgroups of S_n with order divisible by n and their cycle type. If this doesn't suffice to determine the group, then look at its action on the set of subsets of r roots for some r.

See, Butler and McKay, *The transitive groups of degree up to eleven,* Comm. Algebra 11 (1983), 863–911. This lists all transitive subgroups of S_n, $n \leq 11$, and gives the cycle types of their elements and the orbit lengths of the subgroup acting on the r-sets of roots; with few exceptions, these invariants are sufficient to determine the subgroup up to isomorphism.

Maple can compute Galois groups for polynomials of degree ≤ 7 over $\mathbb{Q}$. To learn the syntax, type `?galois;`. Magma (the replacement for Cayley) probably knows much more, but my efforts to obtain a manual for it have been unsuccessful.

See also, Soicher and McKay, *Computing Galois groups over the rationals*, J. Number Theory, 20 (1985) 273–281.

5. Applications of Galois Theory

In this section, we apply the Fundamental Theorem of Galois Theory to obtain other results about polynomials and extensions of fields.

5.1. **Primitive element theorem.**

Recall that a finite extension of fields E/F is simple if $E = F[\alpha]$ for some element α of E. Such an α is called a *primitive element* of E. We shall show that (at least) all separable extensions have primitive elements.

Consider for example $\mathbb{Q}[\sqrt{2}, \sqrt{3}]/\mathbb{Q}$. We know (see Exercise 13) that its Galois group over $\mathbb{Q}$ is a 4-group $<\sigma, \tau>$, where

$$\begin{cases} \sigma\sqrt{2} &= -\sqrt{2} \\ \sigma\sqrt{3} &= \sqrt{3} \end{cases}, \quad \begin{cases} \tau\sqrt{2} &= \sqrt{2} \\ \tau\sqrt{3} &= -\sqrt{3}. \end{cases}$$

Note that

$$\begin{aligned} \sigma(\sqrt{2}+\sqrt{3}) &= -\sqrt{2}+\sqrt{3}, \\ \tau(\sqrt{2}+\sqrt{3}) &= \sqrt{2}-\sqrt{3}, \\ (\sigma\tau)(\sqrt{2}+\sqrt{3}) &= -\sqrt{2}-\sqrt{3}. \end{aligned}$$

These all differ from $\sqrt{2}+\sqrt{3}$, and so only the identity element of $\mathrm{Gal}(\mathbb{Q}[\sqrt{2}, \sqrt{3}]/\mathbb{Q})$ fixes the elements of $\mathbb{Q}[\sqrt{2}+\sqrt{3}]$. According to the Fundamental Theorem, this implies that $\sqrt{2}+\sqrt{3}$ is a primitive element:

$$\mathbb{Q}[\sqrt{2}, \sqrt{3}] = \mathbb{Q}[\sqrt{2}+\sqrt{3}].$$

It is clear that this argument should work much more generally.

We say that an element α algebraic over a field F is *separable* over F if its minimum polynomial over F has no multiple roots. Thus a finite extension E of F is separable if and only if all its elements are separable over F.

Theorem 5.1. *Let $E = F[\alpha_1, ..., \alpha_r]$ be a finite extension of F, and assume that $\alpha_2, ..., \alpha_r$ are separable over F (but not necessarily α_1). Then there is an element $\gamma \in E$ such that $E = F[\gamma]$.*

Proof. For finite fields, we proved this in (4.16). Hence we may assume F to be infinite. It suffices to prove the statement for $r = 2$. Thus let $E = F[\alpha, \beta]$ with β separable over $F[\alpha]$. Let f and g be the minimum polynomials of α and β over F. Let $\alpha_1 = \alpha, \ldots, \alpha_s$ be the roots of f in some field containing E, and let $\beta_1 = \beta$, $\beta_2, \ldots, \beta_t$ be the roots of g. For $j \neq 1$, $\beta_j \neq \beta_1$, and so the the equation

$$\alpha_i + X\beta_j = \alpha_1 + X\beta_1, \qquad j \neq 1,$$

has exactly one solution, namely, $X = \frac{\alpha_i - \alpha_1}{\beta_1 - \beta_j}$. If we choose a c different from any of these solutions (using that F is infinite), then

$$\alpha_i + c\beta_j \neq \alpha + c\beta \text{ unless } i = 1 = j.$$

I claim that $\gamma = \alpha + c\beta$ generates E over F.

The polynomials $g(X)$ and $f(\gamma - cX)$ have coefficients in $F[\gamma][X]$, and have β as a root:

$$g(\beta) = 0, \quad f(\gamma - c\beta) = f(\alpha) = 0.$$

In fact, β is their only common root, because the roots of g are $\beta_1, ..., \beta_t$, and we chose c so that $\gamma - c\beta_j \neq \alpha_i$ unless $i = 1 = j$. Therefore $\gcd(g(X), f(\gamma - cX))$ computed in some field splitting fg is $X-\beta$, but we have seen (Proposition 3.1) that the gcd of two polynomials has coefficients in the same field as the coefficients of the polynomials. Hence $\beta \in F[\gamma]$, and then $\alpha = \gamma - c\beta$ also lies in $F[\gamma]$. □

Remark 5.2. Assume F to be infinite. The proof shows that γ can be chosen to be of the form

$$\gamma = \alpha_1 + c_2\alpha_2 + \cdots + c_r\alpha_r, \quad c_i \in F.$$

In fact, all but a finite number of elements of this form will serve. If $E = F[\alpha_1, \ldots, \alpha_r]$ is Galois over F, then an element of this form will be a primitive element provided it is moved by every element of $\mathrm{Gal}(E/F)$ except 1. These remarks make it very easy to write down primitive elements.

Our hypotheses are minimal: if *two* of the α's are not separable, then the extension need not be simple. Before proving this, we need another result.

Proposition 5.3. *Let $E = F[\gamma]$ be a simple algebraic extension of F. Then there are only finitely many intermediate fields M,*

$$F \subset M \subset E.$$

Proof. Let M be such a field, and let $g(X)$ be the minimum polynomial of γ over M. Let M' be the subfield of E generated over F by the coefficients of $g(X)$. Clearly $M' \subset M$, but (equally clearly) $g(X)$ is the minimum polynomial of γ over M'. Hence

$$[E : M'] = \deg g = [E : M],$$

and so $M = M'$: M is generated by the coefficients of $g(X)$.

Let $f(X)$ be the minimum polynomial of γ over F. Then $g(X)$ divides $f(X)$ in $M[X]$, and hence also in $E[X]$. Therefore, there are only finitely many possible g's, and consequently only finitely many possible M's. □

Remark 5.4. (a) Note that the proposition in fact gives a description of all the intermediate fields: each is generated over F by the coefficients of a factor $g(X)$ of $f(X)$ in $E[X]$. The coefficients of such a $g(X)$ are partially symmetric polynomials in the roots of $f(X)$ (i.e., fixed by some, but not necessarily all, of the permutations of the roots).

(b) The proposition has a converse: if E is a finite extension of F and there are only finitely many intermediate fields M, $F \subset M \subset E$, then E is a simple extension of F (see Dummit, p508). This gives another proof of the theorem when E is separable over F, because Galois theory shows that there are only finitely many intermediate fields in this case (embed E in a Galois extension of F).

(c) The simplest nonsimple extension is $k(X,Y) \supset k(X^p, Y^p) = F$, where k is an algebraically closed field of characteristic p. For any $c \in k$, we have

$$k(X,Y) = F[X,Y] \supset F[X+cY] \supset F$$

with the degree of each extension equal to p. If $F[X+cY] = F[X+c'Y]$, $c \neq c'$, then $F[X+cY]$ would contain both X and Y, which is impossible because $[k(X,Y) : F] = p^2$. Hence there are infinitely many distinct intermediate fields.[3]

[3] Zariski showed that there is even an intermediate field M that is not isomorphic to $F(X,Y)$, and Piotr Blass showed in his UM thesis, 1977, using the methods of algebraic geometry, that there is an infinite sequence of intermediate fields, no two of which are isomorphic.

5.2. **Fundamental Theorem of Algebra.**

We finally prove the misnamed[4] fundamental theorem of algebra.

THEOREM 5.5. *The field $\mathbb{C}$ of complex numbers is algebraically closed.*

PROOF. Define $\mathbb{C}$ to be the splitting field of $X^2+1 \in \mathbb{R}[X]$, and let i be a root of X^2+1 in $\mathbb{C}$; thus $\mathbb{C} = \mathbb{R}[i]$. We have to show (see 2.10) that every $f(X) \in \mathbb{R}[X]$ has a root in $\mathbb{C}$.

The two facts we need to assume about $\mathbb{R}$ are:

- Positive real numbers have square roots.
- Every polynomial of odd degree with real coefficients has a real root.

Both are immediate consequences of the Intermediate Value Theorem, which says that a continuous function on a closed interval takes every value between its maximum and minimum values (inclusive). (Intuitively, this says that, unlike the rationals, the real line has no "holes".)

We first show that every element of $\mathbb{C}$ has a square root. Write $\alpha = a + bi$, with $a, b \in \mathbb{R}$, and choose c, d to be real numbers such that

$$c^2 = \frac{(a + \sqrt{a^2+b^2})}{2}, \quad d^2 = \frac{(-a + \sqrt{a^2+b^2})}{2}.$$

Then $c^2 - d^2 = a$ and $(2cd)^2 = b^2$. If we choose the signs of c and d so that cd has the same sign as b, then $(c+di)^2 = \alpha$.

Let $f(X) \in \mathbb{R}[X]$, and let E be a splitting field for $f(X)(X^2+1)$—we have to show that $E = \mathbb{C}$. Since $\mathbb{R}$ has characteristic zero, the polynomial is separable, and so E is Galois over $\mathbb{R}$. Let G be its Galois group, and let H be a Sylow 2-subgroup of G.

Let $M = E^H$. Then M is of odd degree over $\mathbb{R}$, and $M = \mathbb{R}[\alpha]$ some α (Theorem 5.1). The minimum polynomial of α over $\mathbb{R}$ has odd degree, and so has a root in $\mathbb{R}$. It therefore has degree 1, and so $M = \mathbb{R}$ and $G = H$.

We now have that $\mathrm{Gal}(E/\mathbb{C})$ is a 2-group. If it is $\neq 1$, then it has a subgroup N of index 2. The field E^N has degree 2 over $\mathbb{C}$, and can therefore be obtained by extracting the square root of an element of $\mathbb{C}$ (see 3.23), but we have seen that all such elements already lie in $\mathbb{C}$. Hence $E^N = \mathbb{C}$, which is a contradiction. Thus $E = \mathbb{C}$. □

COROLLARY 5.6. *(a) The field $\mathbb{C}$ is the algebraic closure of $\mathbb{R}$.*

(b) The set of all algebraic numbers is an algebraic closure of $\mathbb{Q}$.

PROOF. Part (a) is obvious from the definition of "algebraic closure", and (b) follows from the discussion on p15. □

[4] Because it is not strictly a theorem in algebra: it is a statement about $\mathbb{R}$ whose construction is part of analysis. In fact, I prefer the proof based on Liouville's theorem in complex analysis to the more algebraic proof given in the text: if $f(z)$ is a polynomial without a root in $\mathbb{C}$, then $f(z)^{-1}$ will be bounded and holomorphic on the whole complex plane, and hence (by Liouville) constant. The Fundamental Theorem was quite a difficult theorem to prove. Gauss gave a proof in his doctoral dissertation in 1798 in which he used some geometric arguments which he didn't justify. He gave the first rigorous proof in 1816. The elegant argument given here is a simplification by Emil Artin of earlier proofs.

5.3. **Cyclotomic extensions.**

A *primitive* n^{th} root of 1 in F is an element of order n in $F^{\times}$. Such an element can exist only if F has characteristic 0 or characteristic p not dividing n.

PROPOSITION 5.7. *Let F be a field of characteristic* 0 *or characteristic p not dividing n. Let E be the splitting field of $X^n - 1$.*

(a) *There exists a primitive n^{th} root of* 1 *in E.*
(b) *If ζ is a primitive n^{th} root of* 1 *in E, then $E = F[\zeta]$.*
(c) *The field E is Galois over F, and the map*

$$\mathrm{Gal}(E/F) \to (\mathbb{Z}/n\mathbb{Z})^{\times}$$

sending σ to $[i]$ if $\sigma\zeta = \zeta^i$ is injective.

PROOF. (a) The roots of $X^n - 1$ are distinct, because its derivative nX^{n-1} has only zero as a root (we use here the condition on the characteristic), and so E contains n distinct n^{th} roots of 1. The n^{th} roots of one form a finite subgroup of $E^{\times}$, and so (see Exercise 3) they form a cyclic group. Any generator will have order n, and hence will be a primitive n^{th} root of 1.

(b) The roots of $X^n - 1$ are the powers of ζ, and $F[\zeta]$ contains them all.

(c) If ζ is one primitive n^{th} root of 1, then the remaining primitive n^{th} roots of 1 are the elements ζ^i with i relatively prime to n. Since $\sigma\zeta$ is again a primitive n^{th} root of 1 for any automorphism σ of E, it equals ζ^i for some i relatively prime to n, and the map $\sigma \mapsto i$ mod n is injective because ζ generates E over F. It obviously is a homomorphism (and is independent of the choice of ζ). □

The map $\sigma \mapsto i : \mathrm{Gal}(F[\zeta]/F) \to (\mathbb{Z}/n\mathbb{Z})^{\times}$ need not be surjective. For example, if $F = \mathbb{C}$, then its image is $\{1\}$, and if $F = \mathbb{R}$, it is $\{\pm 1\}$ $(n \neq 2)$—because $F[\zeta] = \mathbb{C}$, $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ is generated by complex conjugation ι, and $\iota\zeta = \bar{\zeta} = \zeta^{n-1}$. On the other hand, when $n = p$ is prime, we saw in (1.31) that $[\mathbb{Q}[\zeta] : \mathbb{Q}] = p - 1$, and so the map is surjective. We shall prove that the map is surjective for all n when $F = \mathbb{Q}$.

The polynomial $X^n - 1$ has some obvious factors in $\mathbb{Q}[X]$, namely, the polynomials $X^d - 1$ for any $d|n$. The quotient of $X^n - 1$ by all these factors for $d < n$ is called the n^{th} *cyclotomic polynomial* Φ_n. Thus

$$\Phi_n = \prod (X - \zeta) \qquad \text{(product over the primitive } n^{\text{th}} \text{ roots of 1).}$$

It has degree $\varphi(n)$, the order of $(\mathbb{Z}/n\mathbb{Z})^{\times}$. Since every n^{th} root of 1 is a primitive d^{th} root of 1 for exactly one d dividing n, we see that

$$X^n - 1 = \prod_{d|n} \Phi_d(X).$$

For example, $\Phi_1(X) = X - 1$, $\Phi_2(X) = X + 1$, $\Phi_3(X) = X^2 + X + 1$, and

$$\Phi_6(X) = \frac{X^6 - 1}{(X-1)(X+1)(X^2+X+1)} = X^2 - X + 1.$$

This gives an easy inductive method of computing the cyclotomic polynomials. Alternatively ask Maple by typing: `with(numtheory); cyclotomic(n,X);`. Because $X^n - 1$ has coefficients in $\mathbb{Z}$ and is monic, any monic factor of it has coefficients in $\mathbb{Z}$ (see (1.6)). In particular, the cyclotomic polynomials lie in $\mathbb{Z}[X]$.

LEMMA 5.8. *Let F be a field of characteristic 0 or p not dividing n, and let ζ be a primitive n^{th} root of 1 in some extension field. The following are equivalent:*

(a) *the n^{th} cyclotomic polynomial Φ_n is irreducible;*
(b) *the degree $[F[\zeta]:F]=\varphi(n)$;*
(c) *the homomorphism*

$$\mathrm{Gal}(F[\zeta]/F)\to(\mathbb{Z}/n\mathbb{Z})^{\times}$$

is an isomorphism.

PROOF. Because ζ is a root of Φ_n, the minimum polynomial of ζ divides Φ_n. It is equal to it if and only if $[F[\zeta]:F]=\varphi(n)$, which is true if and only if the injection $\mathrm{Gal}(F[\zeta]/F)\hookrightarrow(\mathbb{Z}/n\mathbb{Z})^{\times}$ is onto. □

THEOREM 5.9. *The n^{th} cyclotomic polynomial Φ_n is irreducible in $\mathbb{Q}[X]$.*

PROOF. Let $f(X)$ be a monic irreducible factor of Φ_n in $\mathbb{Q}[X]$. Its roots will be primitive n^{th} roots of 1, and we have to show they include *all* primitive n^{th} roots of 1. For this it suffices to show that

$$\zeta \text{ a root of } f(X) \implies \zeta^i \text{ a root of } f(X) \text{ for all } i \text{ such that } \gcd(i,n)=1.$$

Such an i is a product of primes not dividing n, and so it suffices to show that

$$\zeta \text{ a root of } f(X) \implies \zeta^p \text{ a root of } f(X) \text{ for all primes } p\nmid n.$$

Write

$$\Phi_n(X)=f(X)g(X).$$

Again (1.6) implies that $f(X)$ and $g(X)$ lie in $\mathbb{Z}[X]$. Suppose ζ is a root of f, but that for some prime p not dividing n, ζ^p is not a root of f. Then ζ^p is a root $g(X)$, which implies that ζ is a root of $g(X^p)$. Since $f(X)$ and $g(X^p)$ have a common root, their greatest common divisor (in $\mathbb{Q}[X]$) is $\neq 1$ (see 3.1). Write $h(X)\mapsto\bar{h}(X)$ for the map $\mathbb{Z}[X]\mapsto\mathbb{F}_p[X]$, and note that

$$\gcd(f(X),g(X^p))\neq 1 \implies \gcd(\bar{f}(X),\bar{g}(X^p))\neq 1.$$

But $\bar{g}(X^p)=\bar{g}(X)^p$ (use the $\mod p$ binomial theorem and that $a^p=a$ for all $a\in\mathbb{F}_p$), and so $\gcd(\bar{f}(X),\bar{g}(X)^p)\neq 1$, which implies that $\bar{f}(X)$ and $\bar{g}(X)$ have a common factor. Hence X^n-1 (regarded as an element of $\mathbb{F}_p[X]$) has multiple roots, but we saw in the proof of 5.7 that it doesn't. Contradiction. □

REMARK 5.10. This proof is very old—in essence it goes back to Dedekind in 1857—but its general scheme has recently become very popular: take a statement in characteristic zero, reduce modulo p (where the statement may no longer be true), and exploit the existence of the Frobenius automorphism $a\mapsto a^p$ to obtain a proof of the original statement. For example, commutative algebraists use this method to prove results about commutative rings, and there are theorems about complex manifolds[5] that have *only* been proved by reducing things to characteristic p.

There are some beautiful and mysterious relations between what happens in characteristic 0 and in characteristic p. For example, let $f(X_1,...,X_n)\in\mathbb{Z}[X_1,...,X_n]$. We can

(i) look at the solutions of $f=0$ in $\mathbb{C}$, and so get a topological space;
(ii) reduce mod p, and look at the solutions of $\bar{f}=0$ in $\mathbb{F}_{p^n}$.

[5] This is from my old notes—I no longer remember what I was thinking of.

The Weil conjectures (Weil 1949; proved by Grothendieck and Deligne 1973) assert that the Betti numbers of the space in (i) control the cardinalities of the sets in (ii).

THEOREM 5.11. *The regular n-gon is constructible if and only if $n = 2^k p_1 \cdots p_s$ where the p_i are distinct Fermat primes.*

PROOF. The regular n-gon is constructible if and only if $\cos \frac{2\pi}{n}$ (or $\zeta = e^{2\pi i/n}$) is constructible. We know that $\mathbb{Q}[\zeta]$ is Galois over $\mathbb{Q}$, and so (according to 1.27 and 3.22) ζ is constructible if and only if $[\mathbb{Q}[\zeta] : \mathbb{Q}]$ is a power of 2. But (see Groups 3.10)

$$\varphi(n) = \prod_{p|n} (p-1)p^{n(p)-1}, \quad n = \prod p^{n(p)},$$

and this is a power of 2 if and only if n has the required form. □

REMARK 5.12. The final section of Gauss's, *Disquisitiones Arithmeticae* (1801) is titled "Equations defining sections of a Circle". In it Gauss proves that the n^{th} roots of 1 form a cyclic group, that $X^n - 1$ is solvable (this was before the theory of abelian groups had been developed, and before Galois), and that the regular n-gon is constructible when n is as in the Theorem. He also claimed to have proved the converse statement[6]. This leads some people to credit him with the above proof of the irreducibility of Φ_n, but in the absence of further evidence, I'm sticking with Dedekind.

5.4. **Independence of characters.**

THEOREM 5.13 (Dedekind's theorem on the independence of characters). *Let F be a field, and let G be a group (monoid will do). Then any finite set $\{\chi_1, \ldots, \chi_m\}$ of homomorphisms $G \to F^\times$ is linearly independent over F, i.e.,*

$$\sum a_i \chi_i = 0 \text{ (as a function } G \to E) \implies a_1 = 0, \ldots, a_m = 0.$$

PROOF. Induction on m. If $m = 1$, it's obvious. Assume it for $m - 1$. We suppose

$$a_1\chi_1(x) + a_2\chi_2(x) + \cdots + a_m\chi_m(x) = 0 \quad \text{for all } x \in G,$$

and show that this implies the a_i to be zero. Since $\chi_1 \neq \chi_2$, $\chi_1(g) \neq \chi_2(g)$ for some $g \in G$. On replacing x with gx in the equation, we obtain the equation

$$a_1\chi_1(g)\chi_1(x) + a_2\chi_1(g)\chi_2(x) + \cdots + a_m\chi_1(g)\chi_m(x) = 0, \quad \text{all } x \in G.$$

On multiplying the first equation by $\chi_1(g)$ and subtracting it from the second, we obtain the equation

$$a_2'\chi_2 + \cdots + a_m'\chi_m = 0, \qquad a_i' = a_i(\chi_i(g) - \chi_1(g)).$$

The induction hypothesis now shows that $a_i' = 0$ for all $i \geq 2$. Since $\chi_2(g) - \chi_1(g) \neq 0$, we must have $a_2 = 0$, and the induction hypothesis shows that all the remaining a_i's are also zero. □

[6] "Whenever $n - 1$ involves prime factors other than 2, we are always led to equations of higher degree....WE CAN SHOW WITH ALL RIGOR THAT THESE HIGHER-DEGREE EQUATIONS CANNOT BE AVOIDED IN ANY WAY NOR CAN THEY BE REDUCED TO LOWER-DEGREE EQUATIONS. The limits of the present work exclude this demonstration here, but we issue this warning lest anyone attempt to achieve geometric constructions for sections other than the ones suggested by our theory...and so spend his time uselessly."

COROLLARY 5.14. *Let F_1 and F_2 be fields, and let $\sigma_1, ..., \sigma_m$ be distinct homomorphisms $F_1 \to F_2$. Then $\sigma_1, ..., \sigma_m$ are linearly independent over F_2.*

PROOF. Apply the theorem to $\chi_i = \sigma_i | F_1^\times$. □

5.5. **Hilbert's Theorem 90.**

Let G be a finite group. A *G-module* is an abelian group M together with an action of G, i.e., a map $G \times M \to M$ such that

(a) $\sigma(m + m') = \sigma m + \sigma m'$ for all $\sigma \in G$, $m, m' \in M$;
(b) $(\sigma\tau)(m) = \sigma(\tau m)$ for all $\sigma, \tau \in G$, $m \in M$;
(c) $1m = m$ for all $m \in M$.

Thus, to give an action of G on M is the same as to give a homomorphism $G \to \mathrm{Aut}(M)$ (automorphisms of M as an abelian group).

EXAMPLE 5.15. Let E be a Galois extension of F, with Galois group G; then $(E, +)$ and $E^\times$ are G-modules.

Let M be a G-module. A *crossed homomorphism* is a map $f : G \to M$ such that

$$f(\sigma\tau) = f(\sigma) + \sigma f(\tau).$$

Note that the condition implies that $f(1) = f(1 \cdot 1) = f(1) + f(1)$, and so $f(1) = 0$.

EXAMPLE 5.16. (a) Consider a crossed homomorphism $f : G \to M$, and let $\sigma \in G$. Then

$$f(\sigma^2) = f(\sigma) + \sigma f(\sigma),$$
$$f(\sigma^3) = f(\sigma \cdot \sigma^2) = f(\sigma) + \sigma f(\sigma) + \sigma^2 f(\sigma)$$

and so on, until

$$f(\sigma^n) = f(\sigma) + \sigma f(\sigma) + \cdots + \sigma^{n-1} f(\sigma).$$

Thus, if G is a cyclic group of order n generated by σ, then a crossed homomorphism $f : G \to M$ is determined by $f(\sigma) = x$, and x satisfies the equation

$$x + \sigma x + \cdots + \sigma^{n-1} x = 0, \qquad (*)$$

Conversely, if $x \in M$ satisfies (*), then the formulas $f(\sigma^i) = x + \sigma x + \cdots + \sigma^{i-1} x$ define a crossed homomorphism $f : G \to M$. In this case we have a one-to-one correspondence

$$\{\text{crossed homs } f : G \to M\} \overset{f \mapsto f(\sigma)}{\leftrightarrow} \{x \in M \text{ satisfying } (*)\}.$$

(b) For any $x \in M$, we obtain a crossed homomorphism by putting

$$f(\sigma) = \sigma x - x, \qquad \text{all } \sigma \in G.$$

Such a crossed homomorphism is called a *principal crossed homomorphism.*

(c) If G acts trivially on M, i.e., $\sigma m = m$ for all $\sigma \in G$ and $m \in M$, then a crossed homomorphism is simply a homomorphism, and there are no nontrivial principal crossed homomorphisms.

The sum of two crossed homomorphisms is again a crossed homomorphism, and the sum of two principal crossed homomorphisms is again principal. Thus we can define

$$H^1(G, M) = \frac{\{\text{crossed homomorphisms}\}}{\{\text{principal crossed homomorphisms}\}}.$$

The cohomology groups $H^n(G, M)$ have been defined for all $n \in \mathbb{N}$, but since this was not done until the twentieth century, it will not be discussed in this course.

EXAMPLE 5.17. Let $\pi : \widetilde{X} \to X$ be the universal covering space of a topological space X, and let Γ be the group of covering transformations. Under some fairly general hypotheses, a Γ-module M will define a sheaf $\mathcal{M}$ on X, and $H^1(X, \mathcal{M}) \approx H^1(\Gamma, M)$. For example, when $M = \mathbb{Z}$ with the trivial action of Γ, this becomes the isomorphism $H^1(X, \mathbb{Z}) \approx H^1(\Gamma, \mathbb{Z}) = \operatorname{Hom}(\Gamma, \mathbb{Z})$.

THEOREM 5.18. *Let E be a Galois extension of F with group G; then $H^1(G, E^\times) = 0$, i.e., every crossed homomorphism $G \to E^\times$ is principal.*

PROOF. Let f be a crossed homomorphism $G \to E^\times$. In multiplicative notation, this means,

$$f(\sigma\tau) = f(\sigma) \cdot \sigma(f(\tau)), \quad \sigma, \tau \in G,$$

and we have to find a $\gamma \in E^\times$ such that $f(\sigma) = \sigma\gamma/\gamma$ for all $\sigma \in G$. Because the $f(\tau)$ are nonzero, Dedekind's theorem implies that

$$\sum f(\tau)\tau : E \to E$$

is not the zero map, i.e., there exists an $\alpha \in E$ such that

$$\beta = \sum_{\tau \in G} f(\tau)\tau\alpha \neq 0.$$

But then, for $\sigma \in G$,

$$\sigma\beta = \sum_{\tau \in G} \sigma(f(\tau)) \cdot \sigma\tau(\alpha) = \sum_{\tau \in G} f(\sigma)^{-1} \, f(\sigma\tau) \cdot \sigma\tau(\alpha) = f(\sigma)^{-1} \, \sum_{\tau \in G} f(\sigma\tau)\sigma\tau(\alpha) = f(\sigma)^{-1}\beta,$$

which shows that $f(\sigma) = \frac{\beta}{\sigma(\beta)}$ and so we can take $\beta = \gamma^{-1}$. □

Let E be a Galois extension of F with Galois group G. We define the *norm* of an element $\alpha \in E$ to be

$$\operatorname{Nm}\alpha = \prod_{\sigma \in G} \sigma\alpha.$$

Then, for $\tau \in G$,

$$\tau(\operatorname{Nm}\alpha) = \prod_{\sigma \in G} \tau\sigma\alpha = \operatorname{Nm}\alpha,$$

and so $\operatorname{Nm}\alpha \in F$. The map $\alpha \mapsto \operatorname{Nm}\alpha : E^\times \to F^\times$ is a homomorphism. For example, the norm map $\mathbb{C}^\times \to \mathbb{R}^\times$ is $\alpha \mapsto |\alpha|^2$ and the norm map $\mathbb{Q}[\sqrt{d}]^\times \to \mathbb{Q}^\times$ is $a + b\sqrt{d} \mapsto a^2 - db^2$.

We are interested in determining the kernel of this homomorphism. Clearly if α is of the form $\frac{\beta}{\tau\beta}$, then $\operatorname{Nm}(\alpha) = 1$. Our next result show that, for cyclic extensions, all elements with norm 1 are of this form.

COROLLARY 5.19 (Hilbert's theorem 90). [7]*Let E be a finite cyclic extension of F with Galois group $< \sigma >$; if $\operatorname{Nm}_{E/F}\alpha = 1$, then $\alpha = \beta/\sigma\beta$ for some $\beta \in E$.*

[7] The theorem is Satz 90 in Hilbert's book, Theorie der Algebraische Zahlkörper, 1897, which laid the foundations for modern algebraic number theory. Many point to it as a book that made a fundamental contribution to mathematical progress, but Emil Artin has been quoted as saying that it set number theory back thirty years—it wasn't sufficiently abstract for his taste.

PROOF. Let $m = [E : F]$. The condition on α is that $\alpha \cdot \sigma\alpha \cdots \sigma^{m-1}\alpha = 1$, and so (see 5.16a) there is a crossed homomorphism $f : <\sigma> \to E^{\times}$ with $f(\sigma) = \alpha$. The theorem now shows that f is principal, which means that there is a β with $f(\sigma) = \beta/\sigma\beta$. □

5.6. **Cyclic extensions.**

We are now able to classify the cyclic extensions of degree n of a field F in the case that F contains n n^{th} roots of 1.

THEOREM 5.20. *Let F be a field containing a primitive n^{th} root of* 1.

(a) *The Galois group of $X^n - a$ is cyclic of order dividing n.*
(b) *Conversely, if E is cyclic of degree n over F, then there is an element $\beta \in E$ such that $E = F[\beta]$ and $b =_{df} \beta^n \in F$; hence E is the splitting field of $X^n - b$.*

PROOF. (a) If α is one root of $X^n - a$, then the other roots are the elements of the form $\zeta\alpha$ with ζ an n th root of 1. Hence the splitting field of $X^n - a$ is $F[\alpha]$. The map $\sigma \mapsto \frac{\sigma\alpha}{\alpha}$ is an injective homomorphism of $\text{Gal}(F[\alpha]/F)$ into the cyclic group $<\zeta>$.

(b) Let ζ be a primitive n^{th} root of 1 in F, and let σ generate $\text{Gal}(E/F)$. Then $\text{Nm}\,\zeta = \zeta^n = 1$, and so, according to Hilbert's Theorem 90, there is an element $\beta \in E$ such that $\sigma\beta = \zeta\beta$. Then $\sigma^i\beta = \zeta^i\beta$, and so only the identity element of $\text{Gal}(E/F[\beta])$ fixes β—we conclude by the Fundamental Theorem of Galois Theory that $E = F[\beta]$. On the other hand $\sigma\beta^n = \zeta^n\beta^n = \beta^n$, and so $\beta^n \in F$. □

REMARK 5.21. (a) Under the hypothesis of the theorem $X^n - a$ is irreducible, and its Galois group is of order n, if

(i) a is not a p^{th} power for any p dividing n;
(ii) if $4|n$ then $a \notin -4k^4$.

See Lang, Algebra, VIII, §9, Theorem 16.

(b) If F has characteristic p (hence has no p^{th} roots of 1 other than 1), then $X^p - X - a$ is irreducible in $F[X]$ unless $a = b^p - b$ for some $b \in F$, and when it is irreducible, its Galois group is cyclic of order p (generated by $\alpha \mapsto \alpha + 1$ where α is a root). Moreover, every extension of F which is cyclic of degree p is the splitting field of such a polynomial.

REMARK 5.22 (Kummer theory). Above we gave a description of all Galois extensions of F with Galois group cyclic of order n in the case that F contains a primitive n^{th} root of 1. Under the same assumption on F, it is possible to give a description of all the Galois extensions of F with abelian Galois group of exponent n, i.e., a quotient of $(\mathbb{Z}/n\mathbb{Z})^r$ for some r.

Let E be such an extension of F, and let

$$S(E) = \{a \in F^{\times} \mid a \text{ becomes an } n^{th} \text{ power in } E\};$$

Then $S(E)$ is a subgroup of $F^{\times}$ containing $F^{\times n}$, and the map $E \mapsto S(E)$ defines a one-to-one correspondence between abelian extensions of E of exponent n and groups $S(E)$, $F^{\times} \supset S(E) \supset F^{\times n}$, such that $(S(E) : F^{\times n}) < \infty$. The field E is recovered from $S(E)$ as the splitting field of $\prod(X^n - a)$ (product over a set of representatives for $S(E)/F^{\times n}$). Moreover, there is a perfect pairing

$$(a, \sigma) \mapsto \frac{\sigma a}{a} : \frac{S(E)}{F^{\times n}} \times \text{Gal}(E/F) \to \mu_n \text{ (group of } n^{th} \text{ roots of 1).}$$

In particular, $[E : F] = (S(E) : F^{\times n})$. (Cf. Exercise 5 for the case $n = 2$.)

5.7. **Proof of Galois's solvability theorem.**

Recall that a polynomial $f(X) \in F[X]$ is said to be solvable if there is a tower of fields

$$F = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_m$$

such that

(a) $F_i = F_{i-1}[\alpha_i]$, where $\alpha_i^{m_i} \in F_{i-1}$ for some m_i;
(b) F_m splits $f(X)$.

Theorem 5.23. *Let F be a field of characteristic 0. A polynomial $f \in F[X]$ is solvable if and only if its Galois group G_f is solvable.*

Before proving the sufficiency, we need a lemma.

Lemma 5.24. *Let $f \in F[X]$ be separable, and let F' be an extension field of F. Then the Galois group of f as an element of $F'[X]$ is a subgroup of that of f as an element of $F[X]$.*

Proof. Let E' be a splitting field for f over F', and let $\alpha_1, \dots, \alpha_m$ be the roots of $f(X)$ in E'. Then $E = F[\alpha_1, ..., \alpha_m]$ is a splitting field of f over F. Any element of $\mathrm{Gal}(E'/F')$ permutes the α_i and so maps E into itself. The map $\sigma \mapsto \sigma|E$ is an injection $\mathrm{Gal}(E'/F') \to \mathrm{Gal}(E/F)$. □

Proof. (G_f solvable $\implies$ f solvable). Let $f \in F[X]$ have solvable Galois group. Let $F' = F[\zeta]$ where ζ is a primitive n^{th} root of 1 for some large n—for example, $n = (\deg f)!$ will do. The lemma shows that the Galois group G of f as an element of $F'[X]$ is a subgroup of G_f, and hence is solvable. This means that there is a sequence of subgroups

$$G = G_m \supset G_{m-1} \supset \cdots \supset G_1 \supset G_0 = \{1\}$$

such that each G_i is normal in G_{i+1} and G_{i+1}/G_i is cyclic (even of prime order, but we don't need this). Let E be a splitting field of $f(X)$ over F', and let $F_i = E^{G_i}$. We have a sequence of fields

$$F \subset F[\zeta] = F' \subset F_1 \subset F_2 \subset \cdots \subset F_m = E$$

with F_i Galois over F_{i-1} with cyclic Galois group. According to (5.20b), $F_i = F_{i-1}[\alpha_i]$ with $\alpha_i^{[F_i:F_{i-1}]} \in F_{i-1}$. This shows that f is solvable. □

Before proving the necessity, we need to make some observations. Let Ω be a Galois extension of F, and let E be an extension of F contained in Ω. The *Galois closure* $\widetilde{E}$ of E in Ω is the smallest subfield of Ω containing E that is Galois over F. Let $G = \mathrm{Gal}(\Omega/F)$ and $H = \mathrm{Gal}(\Omega/E)$. Then $\widetilde{E}$ will be the subfield of Ω corresponding to the largest normal subgroup of G contained in H (Galois correspondence 3.17), but this is $\bigcap_{\sigma \in G} \sigma H \sigma^{-1}$ (see Groups 4.10), and $\sigma H \sigma^{-1}$ corresponds to σE. Hence (see 3.18) $\widetilde{E}$ is the composite of the fields σE, $\sigma \in G$. In particular, we see that if $E = F[\alpha_1, \dots, \alpha_m]$, then $\widetilde{E}$ is generated over F by the elements $\sigma \alpha_i$, $\sigma \in G$.

Proof. (f solvable $\implies$ G_f solvable). It suffices to show that G_f is a quotient of a solvable group. Hence it suffices to find a Galois extension $\widetilde{E}$ of F with $\mathrm{Gal}(\widetilde{E}/F)$ solvable and such that $f(X)$ splits in $\widetilde{E}[X]$.

We are given that f splits in an extension F_m of F with the following property: $F_m = F[\alpha_1, \dots, \alpha_m]$ and, for all i, there exists an m_i such that $\alpha_i^{m_i} \in F[\alpha_1, \dots, \alpha_{i-1}]$. By (5.1) we know $F_m = F[\gamma]$ for some γ. Let $g(X)$ be the minimum polynomial of γ over F, and let

Ω be a splitting field of $g(X)(X^n-1)$ for some suitably large n. We can identify F_m with a subfield of Ω. Let $G=\{\sigma_1=1,\sigma_2,\dots\}$ be the Galois group of Ω/F and let ζ be a primitive n^{th} root of 1 in Ω. Choose $\widetilde{E}$ to be the Galois closure of $F_m[\zeta]$ in Ω. According to the above remarks, $\widetilde{E}$ is generated over F by the elements

$$\zeta,\alpha_1,\alpha_2,\dots,\alpha_m,\sigma_2\alpha_1,\dots,\sigma_2\alpha_m,\sigma_3\alpha_1,\dots.$$

When we adjoin these elements one by one, we get a sequence of fields

$$F\subset F[\zeta]\subset F[\zeta,\alpha_1]\subset\cdots\subset F'\subset F''\subset\cdots\subset\widetilde{E}$$

such that each field F'' is obtained from its predecessor F' by adjoining an r^{th} root of an element of F'. According to (5.20a) and (5.7), each of these extensions is Galois with cyclic Galois group, and so G has a normal series with cyclic quotients. It is therefore solvable. □

5.8. **The general polynomial of degree n.**

When we say that the roots of

$$aX^2+bX+c$$

are

$$\frac{-b\pm\sqrt{b^2-4ac}}{2}$$

we are thinking of a,b,c as variables: for any particular values of a,b,c, the formula gives the roots of the particular equation. We shall prove in this section that there is no similar formula for the roots of the "general polynomial" of degree ≥ 5.

We define the *general polynomial of degree n* to be

$$f(X)=X^n-t_1X^{n-1}+\cdots+(-1)^nt_n\in F[t_1,...,t_n][X]$$

where the t_i are variables. We shall show that, when we regard f as a polynomial in X with coefficients in the field $F(t_1,\dots,t_n)$, its Galois group is S_n. Then Theorem 5.23 proves the above remark (at least on characteristic zero).

Symmetric polynomials. Let R be a commutative ring (with 1). A polynomial $P(X_1,...,X_n)\in R[X_1,\dots,X_n]$ is said to be *symmetric* if it is unchanged when its variables are permuted, i.e., if

$$P(X_{\sigma(1)},\dots,X_{\sigma(n)})=P(X_1,\dots,X_n),\quad \text{all } \sigma\in S_n.$$

For example

$$\begin{array}{lcll}
p_1 & = & \sum_i X_i & =X_1+X_2+\cdots+X_n,\\
p_2 & = & \sum_{i<j} X_iX_j & =X_1X_2+X_1X_3+\cdots+X_1X_n+X_2X_3+\cdots+X_{n-1}X_n,\\
p_3 & = & \sum_{i<j<k} X_iX_jX_k, & =X_1X_2X_3+\cdots\\
\dots & & & \\
p_r & = & \sum_{i_1<\cdots<i_r} X_{i_1}...X_{i_r} & \\
\dots & & & \\
p_n & = & X_1X_2\cdots X_n &
\end{array}$$

are all symmetric, because p_r is the sum of *all* monomials of degree r made up out of distinct X_i's. These particular polynomials are called the *elementary symmetric polynomials.*

Theorem 5.25 (Symmetric polynomials theorem). *Every symmetric polynomial $P(X_1,...,X_n)$ in $R[X_1,...,X_n]$ is equal to a polynomial in the elementary symmetric polynomials with coefficients in R, i.e., $P\in R[p_1,...,p_n]$.*

PROOF. We define an ordering on the monomials in the X_i by requiring that

$$X_1^{i_1}X_2^{i_2}\cdots X_n^{i_n} > X_1^{j_1}X_2^{j_2}\cdots X_n^{j_n}$$

if either

$$i_1+i_2+\cdots+i_n > j_1+j_2+\cdots+j_n$$

or equality holds and, for some s,

$$i_1=j_1,\ldots,i_s=j_s, \text{ but } i_{s+1}>j_{s+1}.$$

For example,

$$X_1X_2^3X_3 > X_1X_2^2X_3 > X_1X_2X_3^2.$$

Let $X_1^{k_1}\cdots X_n^{k_n}$ be the highest monomial occurring in P with a coefficient $c \neq 0$. Because P is symmetric, it contains all monomials obtained from $X_1^{k_1}\cdots X_n^{k_n}$ by permuting the X's. Hence $k_1 \geq k_2 \geq \cdots \geq k_n$.

The highest monomial in p_i is $X_1\cdots X_i$, and it follows that the highest monomial in $p_1^{d_1}\cdots p_n^{d_n}$ is

$$X_1^{d_1+d_2+\cdots+d_n}X_2^{d_2+\cdots+d_n}\cdots X_n^{d_n}.$$

Therefore

$$P(X_1,\ldots,X_n)-cp_1^{k_1-k_2}p_2^{k_2-k_3}\cdots p_n^{k_n} < P(X_1,\ldots,X_n).$$

We can repeat this argument with the polynomial on the left, and after a finite number of steps, we will arrive at a representation of P as a polynomial in $p_1,\ldots,p_n$. □

Let $f(X)=X^n+a_1X^{n-1}+\cdots+a_n \in R[X]$, and let $\alpha_1,\ldots,\alpha_n$ be the roots of $f(X)$ in some ring S containing R, i.e., $f(X)=\prod(X-\alpha_i)$ in $S[X]$. Then

$$a_1=-p_1(\alpha_1,\ldots,\alpha_n), \quad a_2=p_2(\alpha_1,\ldots,\alpha_n), \quad \ldots, \quad a_n=\pm p_n(\alpha_1,\ldots,\alpha_n).$$

Thus the *elementary* symmetric polynomials in the roots of $f(X)$ lie in R, and so the theorem implies that *every* symmetric polynomial in the roots of $f(X)$ lies in R. For example, the discriminant

$$D(f)=\prod_{i<j}(\alpha_i-\alpha_j)^2$$

of f lies in R.

The general polynomial.

THEOREM 5.26 (Symmetric functions theorem). *When S_n acts on $E=F(X_1,...,X_n)$ by permuting the X_i's, the field of invariants is $F(p_1,...,p_n)$.*

PROOF. Suppose $f=\frac{g}{h}$, $g,h \in F[X_1,\ldots,X_n]$, is symmetric, i.e., fixed by all $\sigma \in S_n$. Then $H=\prod_{\sigma\in S_n}\sigma h$ is symmetric, and so therefore is Hf. Both Hf and H are polynomials, and therefore lie in $F[p_1,\ldots,p_n]$. Hence their quotient $f=\frac{Hf}{H}$ lies in $F(p_1,\ldots,p_n)$. □

COROLLARY 5.27. *The field $F(X_1,...,X_n)$ is Galois over $F(p_1,...,p_n)$ with Galois group S_n (acting by permuting the X_i).*

PROOF. We have shown that $F(p_1,\ldots,p_n)=F(X_1,\ldots,X_n)^{S_n}$, and so this follows from (3.12). □

THEOREM 5.28. *The Galois group of the general polynomial of degree n is S_n.*

Proof. Let $f(X)$ be the general polynomial of degree n,

$$f(X) = X^n - t_1X^{n-1} + \cdots + (-1)^n t_n \in F[t_1, ..., t_n][X].$$

Consider the homomorphism

$$F[t_1, \ldots, t_n] \to F[p_1, \ldots, p_n], \quad t_i \mapsto p_i.$$

We shall prove shortly that this is an isomorphism, and therefore induces an isomorphism on the fields of fractions

$$F(t_1, \ldots, t_n) \to F(p_1, \ldots, p_n), \quad t_i \mapsto p_i.$$

Under this isomorphism, $f(X)$ corresponds to

$$g(X) = X^n - p_1X^{n-1} + \cdots + (-1)^n p_n.$$

But $g(X) = \prod(X - X_i)$ in $F(X_1, \ldots, X_n)[X]$, and so $F(X_1, \ldots, X_n)$ is the splitting field of $g(X) \in F(p_1, \ldots, p_n)[X]$. Therefore the last corollary shows that the Galois group of g is S_n, which must also be the Galois group of f.

It remains to show that the homomorphism $t_i \mapsto p_i$ is an isomorphism. Let $E \supset F(t_1, \ldots, t_n)$ be a splitting field of f, and let $\alpha_1, ..., \alpha_n$ be the roots of f in E. Consider the diagram

$$\begin{tikzcd}
E \supset F[\alpha_1, \ldots, \alpha_n] & F[X_1, \ldots, X_n] \arrow[l, "\alpha_i \leftarrow X_i"'] \\
\cup & \cup \\
F[t_1, \ldots, t_n] \arrow[r, "t_i \mapsto p_i"] & F[p_1, \ldots, p_n].
\end{tikzcd}$$

The top and bottom maps are well-defined because $F[X_1, ..., X_n]$ and $F[t_1, ..., t_n]$ are polynomial rings. The diagram commutes because $t_i = p_i(\alpha_1, ..., \alpha_n)$. Hence the lower horizontal map is injective, and, since it is obviously surjective, it is an isomorphism. □

Remark 5.29. In the final section of this course, we'll discuss algebraic independence. Then it will be obvious that the map $t_i \mapsto p_i : F[t_1, \ldots, t_n] \to F[p_1, \ldots, p_n]$ is an isomorphism, which simplifies the proof.

Remark 5.30. Since S_n occurs as a Galois group over $\mathbb{Q}$, and every finite group occurs as a subgroup of some S_n, it follows that every finite group occurs as a Galois group over some finite extension of $\mathbb{Q}$, but does every finite Galois group occur as a Galois group over $\mathbb{Q}$ itself?

The Hilbert-Noether program for proving this was the following.

Hilbert proved that if G occurs as the Galois group of an extension $E \supset \mathbb{Q}(t_1, ..., t_n)$ (the t_i are variables), then it occurs infinitely often as a Galois group over $\mathbb{Q}$. For the proof, realize E as the splitting field of a polynomial $f(X) \in k[t_1, \ldots, t_n][X]$ and prove that for infinitely many values of the t_i, the polynomial you obtain in $\mathbb{Q}[X]$ has Galois group G. (This is quite a difficult theorem—see Serre, *Lectures on the Mordell-Weil Theorem,* Chapter 9.)

Noether conjectured the following: Let $G \subset S_n$ act on $F(X_1, ..., X_n)$ by permuting the X_i; then $F(X_1, \ldots, X_n)^G \approx F(t_1, ..., t_n)$ (for variables t_i).

Unfortunately, Swan proved in 1969 that the conjecture is false for C_{47}. Hence this approach can not lead to a proof that all finite groups occur as Galois groups over $\mathbb{Q}$, but it doesn't exclude other approaches. [For more information on the problem, see Serre, ibid., Chapter 10, and Serre, *Topics in Galois Theory*, 1992.]

Remark 5.31. Take $F = \mathbb{C}$, and consider the subset of $\mathbb{C}^{n+1}$ defined by the equation

$$X^n - T_1X^{n-1} + \cdots + (-1)^nT_n = 0.$$

It is a beautiful complex manifold S of dimension n. Consider the projection

$$\pi : S \to \mathbb{C}^n, \quad (x, t_1, \ldots, t_n) \mapsto (t_1, \ldots, t_n).$$

Its fibre over a point $(a_1, \ldots, a_n)$ is the set of roots of the polynomial

$$X^n - a_1X^{n-1} + \cdots + (-1)^na_n.$$

The discriminant of $X^n - T_1X^{n-1} + \cdots + (-1)^nT_n$, regarded as a polynomial in X, is a polynomial $D(f) \in \mathbb{C}[T_1, \ldots, T_n]$. Let Δ be the zero set of $D(f)$ in $\mathbb{C}^n$. Then over each point of $\mathbb{C}^n \setminus \Delta$, there are exactly n points of S, and $S \setminus \pi^{-1}(\Delta)$ is a covering space over $\mathbb{C}^n \setminus \Delta$ with group of covering transformations S_n.

A brief history. As far back as 1500 BC, the Babylonians (at least) knew a general formula for the roots of a quadratic polynomial. Cardan (about 1515 AD) found a general formula for the roots of a cubic polynomial. Ferrari (about 1545 AD) found a general formula for the roots of quartic polynomial (he introduced the resolvant cubic, and used Cardan's result). Over the next 275 years there were many fruitless attempts to obtain similar formulas for higher degree polynomials, until, in about 1820, Ruffini and Abel proved that there are none.

5.9. **Norms and traces.**

The *trace* of a square matrix is the sum of its diagonal elements, $\mathrm{Tr}(a_{ij}) = \sum_i a_{ii}$. Since $\mathrm{Tr}(UAU^{-1}) = \mathrm{Tr}(A)$, we can define the *trace* of an endomorphism α of a finite-dimensional vector space V to be the trace of the matrix of α with respect to any basis of V.

Similarly, we can define the *determinant* and *characteristic polynomial* of α to be the determinant and characteristic polynomial of the matrix of α with respect to any basis of V.

In a little more detail, a direct computation shows that $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$, which shows that $\mathrm{Tr}(UAU^{-1}) = \mathrm{Tr}(A)$ and hence $\mathrm{Tr}(\alpha)$ is well-defined. The characteristic polynomial of α can be defined to be

$$c_\alpha(X) = X^n + c_1X^{n-1} + \cdots + c_n, \quad c_i = (-1)^i \operatorname{Tr}(\alpha|\Lambda^iV), \quad n = \dim V;$$

in particular, $c_1 = -\operatorname{Tr}(A)$ and $c_n = (-1)^n \det A$. If A is the matrix of α with respect to some basis for V, then $c_\alpha(X) = \det(XI_n - A)$.

For α and β endomorphisms of a finite-dimensional F-vector space V, we have

$$\begin{aligned} \mathrm{Tr}(\alpha) \in F; \qquad \mathrm{Tr}(\alpha+\beta) &= \mathrm{Tr}(\alpha) + \mathrm{Tr}(\beta); \\ \det(\alpha) \in F; \qquad \det(\alpha\beta) &= \det(\alpha)\det(\beta). \end{aligned}$$

Now let E be a finite extension of F of degree n, and regard E as an F-vector space. Then $\alpha \in E$ defines an F-linear map $\alpha_L : E \to E$, $x \mapsto \alpha x$.

Define:

$$\begin{aligned} \mathrm{Tr}_{E/F}(\alpha) &= \mathrm{Tr}(\alpha_L); && \mathrm{Tr} \text{ is a homomorphism } (E,+) \to (F,+); \\ \mathrm{Nm}_{E/F}(\alpha) &= \det(\alpha_L); && \mathrm{Nm} \text{ is homomorphism } (E^\times,\times) \to (F^\times,\times); \\ c_\alpha(X) &= c_{\alpha_L}(X). \end{aligned}$$

Note that $\alpha \mapsto \alpha_L$ is an *injective* ring F-homomorphism from E into the ring of endomorphisms of E as a vector space over F, and so the minimum polynomial of α (in the sense of Section 1.8) is the same as the minimum polynomial of α_L (in the sense of linear algebra).

EXAMPLE 5.32. (a) Consider the field extension $\mathbb{C} \supset \mathbb{R}$; the matrix of α_L, $\alpha = a + bi$, relative to the basis $1, i$ is $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$, and so

$$\mathrm{Tr}_{\mathbb{C}/\mathbb{R}}(\alpha) = 2\Re(\alpha), \quad \mathrm{Nm}_{\mathbb{C}/\mathbb{R}}(\alpha) = |\alpha|^2.$$

(b) For $\alpha \in F$, $\mathrm{Tr}(\alpha) = r\alpha$, $\mathrm{Nm}(\alpha) = \alpha^r$, $r = [E : F]$.

(c) Let $E = \mathbb{Q}[\alpha, i]$ be the splitting field of $X^8 - 2$. What are the norm and the trace of α? The definition requires us to compute a 16×16 matrix. We shall see a quicker way of computing them presently.

PROPOSITION 5.33. *Consider a finite field extension E/F, and let $f(X)$ be the minimum polynomial of $\alpha \in E$ (in the sense of Section 1.8). Then*

$$c_\alpha(X) = f(X)^{[E:F[\alpha]]}.$$

PROOF. Suppose first that $E = F[\alpha]$. In this case, we have to show that $c_\alpha(X) = f(X)$. But $f(X)|c_\alpha(X)$ because $c_\alpha(\alpha_L) = 0$ (Cayley-Hamilton theorem), and the injectivity of $E \to \mathrm{End}_{F\text{-linear}}(E)$ then implies that $c_\alpha(\alpha) = 0$. Since the polynomials are monic of the same degree, they must be equal.

For the general case, write V for E regarded as an F-vector space. The endomorphism α_L of V defines an action of $F[X]$ on V (see Math 593), and this action factors through $F[X]/(f(X)) = F[\alpha]$. Because $F[\alpha]$ is a field, V is a free $F[\alpha]$-module, and in fact, $V \approx F[\alpha]^m$ with $m = [E : F[\alpha]]$ (count dimensions over F). Hence the characteristic polynomial of α acting on V is the m^{th} power of its characteristic polynomial acting on $F[\alpha]$, which, according to case already proved, is $f(X)$.

Alternatively, we can be more explicit. Let $\beta_1, ..., \beta_n$ be a basis for $F[\alpha]$ over F, and let $\gamma_1, ..., \gamma_m$ be a basis for E over $F[\alpha]$. As we saw in the proof of (1.10), $\{\beta_i\gamma_k\}$ is a basis for E over F. Write $\alpha\beta_i = \sum a_{ji}\beta_j$; then $A = (a_{ij})$ has characteristic polynomial $f(X)$ according to the first case proved. Note that $\alpha\beta_i\gamma_k = \sum a_{ji}\beta_j\gamma_k$. Therefore the matrix of α_L in $\mathrm{End}(E)$ breaks up into $n \times n$ blocks with A's down the diagonal and zero matrices elsewhere. Therefore its characteristic polynomial is $f(X)^m$. □

COROLLARY 5.34. *Suppose that the roots of the minimum polynomial of α are $\alpha_1, \ldots, \alpha_n$ (in some splitting field containing E), and that $[E : F[\alpha]] = m$. Then*

$$\mathrm{Tr}(\alpha) = m \sum_{i=1}^{n} \alpha_i, \qquad \mathrm{Nm}_{E/F}\,\alpha = \left(\prod_{i=1}^{n} \alpha_i\right)^m.$$

PROOF. Write the minimum polynomial of α as

$$f(X) = X^n + a_1X^{n-1} + \cdots + a_n = \prod(X - \alpha_i).$$

Then

$$c_\alpha(X) = (f(X))^m = X^{mn} + ma_1X^{mn-1} + \cdots + a_n^m,$$

and so

$$\mathrm{Tr}_{E/F}(\alpha) = -ma_1 = m\sum \alpha_i,$$

and

$$\mathrm{Nm}_{E/F}(\alpha) = (-1)^{mn} a_n^m = (\prod \alpha_i)^m.$$

□

Example 5.35. (a) Consider the extension $\mathbb{C} \supset \mathbb{R}$. If $\alpha \in \mathbb{C} \setminus \mathbb{R}$, then

$$c_\alpha(X) = f(X) = X^2 - 2\Re(\alpha)X + |\alpha|^2.$$

If $\alpha \in \mathbb{R}$, then $c_\alpha(X) = (X-a)^2$.

(b) Let $E = \mathbb{Q}[\alpha, i]$ be the splitting field of $X^8 - 2$ (see Exercise 16). The minimum polynomial of $\alpha = \sqrt[8]{2}$ is $X^8 - 2$, and so

$$\begin{aligned} \mathrm{Tr}_{\mathbb{Q}[\alpha]/\mathbb{Q}}\,\alpha &= 0; \qquad \mathrm{Tr}_{E/\mathbb{Q}}\,\alpha = 0. \\ \mathrm{Nm}_{\mathbb{Q}[\alpha]/\mathbb{Q}}\,\alpha &= -2; \qquad \mathrm{Nm}_{E/\mathbb{Q}}\,\alpha = 4. \end{aligned}$$

Remark 5.36. Assume E is separable over F, and let Ω be an algebraic closure of F; let $\sigma_1, ..., \sigma_r$ be the distinct embeddings of E into Ω. Then

$$\begin{aligned} \mathrm{Tr}_{E/F}\,\alpha &= \sum \sigma_i\alpha \\ \mathrm{Nm}_{E/F}\,\alpha &= \prod \sigma_i\alpha. \end{aligned}$$

When $E = F[\alpha]$, this follows from the observation (cf. 2.1b) that the $\sigma_i\alpha$ are the roots of the minimum polynomial $f(X)$ of α over F. In the general case, $\sigma_1\alpha, ..., \sigma_r\alpha$ are still roots of $f(X)$ in Ω, but now each root of $f(X)$ occurs $[E : F[\alpha]]$ times (cf. the proof of 2.7).

For example, if E is Galois over F with Galois group G, then

$$\begin{aligned} \mathrm{Tr}_{E/F}\,\alpha &= \sum_{\sigma\in G} \sigma\alpha \\ \mathrm{Nm}_{E/F}\,\alpha &= \prod_{\sigma\in G} \sigma\alpha. \end{aligned}$$

Proposition 5.37. *For finite extensions $E \supset M \supset F$, we have*

$$\begin{aligned} \mathrm{Tr}_{E/M} \circ \mathrm{Tr}_{M/F} &= \mathrm{Tr}_{E/F}, \\ \mathrm{Nm}_{E/M} \circ \mathrm{Nm}_{M/F} &= \mathrm{Nm}_{E/F}\,. \end{aligned}$$

Proof. If E is separable over F, then this can be proved fairly easily using the descriptions in the above remark. We omit the proof in the general case. □

Proposition 5.38. *Let $f(X) \in F[X]$ factor as $f(X) = \prod_{i=1}^m (X - \alpha_i)$ in some splitting field, and let $\alpha = \alpha_1$. Then, with $f' = \frac{df}{dX}$, we have*

$$\operatorname{disc} f(X) = (-1)^{m(m-1)/2}\,\mathrm{Nm}_{F[\alpha]/F}\, f'(\alpha).$$

Proof. Compute that

$$\begin{aligned} \operatorname{disc} f(X) &\overset{\mathrm{df}}{=} \prod_{i<j} (\alpha_i - \alpha_j)^2 \\ &= (-1)^{m(m-1)/2} \cdot \prod_i (\prod_{j\neq i} (\alpha_i - \alpha_j)) \\ &= (-1)^{m(m-1)/2} \cdot \prod f'(\alpha_j) \\ &= (-1)^{m(m-1)/2}\,\mathrm{Nm}_{F[\alpha]/F}(f'(\alpha)). \end{aligned}$$

□

EXAMPLE 5.39. We compute the discriminant of

$$f(X) = X^n + aX + b, \quad a, b \in F,$$

assumed to be irreducible and separable. Let α be a root of $f(X)$, and let $\gamma = f'(\alpha) = n\alpha^{n-1} + a$. We compute its norm. On multiplying the equation

$$\alpha^n + a\alpha + b = 0$$

by $n\alpha^{-1}$ and rearranging, we obtain the equation

$$n\alpha^{n-1} = -na - nb\alpha^{-1}.$$

Hence

$$\gamma = n\alpha^{n-1} + a = -(n-1)a - nb\alpha^{-1}.$$

Solving for α gives

$$\alpha = \frac{-nb}{\gamma + (n-1)a},$$

from which it is clear that $F[\alpha] = F[\gamma]$, and so the minimum polynomial of γ over F has degree n also. If we write

$$f(\frac{-nb}{X + (n-1)a}) = \frac{P(X)}{Q(X)},$$

then $P(\gamma) = f(\alpha) = 0$. Since

$$P(X) = (X + (n-1)a)^n - na(X + (n-1)a)^{n-1} + (-1)^n n^n b^{n-1}$$

is monic of degree n, it must be the minimum polynomial of γ. Therefore $\operatorname{Nm}\gamma$ is $(-1)^n$ times the constant term of this polynomial, and so we find that

$$\operatorname{Nm}\gamma = n^n b^{n-1} + (-1)^{n-1}(n-1)^{n-1}a^n.$$

Finally we obtain the formula,

$$\operatorname{disc}(X^n + aX + b) = (-1)^{n(n-1)/2}(n^n b^{n-1} + (-1)^{n-1}(n-1)^{n-1}a^n),$$

which is something Maple doesn't know (because it doesn't understand symbols as exponents). For example,

$$\operatorname{disc}(X^5 + aX + b) = 5^5 b^4 + 4^4 a^5.$$

5.10. **Infinite Galois extensions (sketch).**

Recall that we defined a finite extension Ω of F to be Galois over F if it is normal and separable, i.e., if every irreducible polynomial $f \in F[X]$ having a root in Ω has $\deg f$ distinct roots in Ω. Similarly, we define an algebraic extension Ω of F to be *Galois* over F if it is normal and separable. Equivalently, a field $\Omega \supset F$ is Galois over F if it is a union of subfields E finite and Galois over F.

Let $\operatorname{Gal}(\Omega/F) = \operatorname{Aut}(\Omega/F)$, and consider the map

$$\sigma \mapsto (\sigma|E) : \operatorname{Gal}(\Omega/F) \to \prod \operatorname{Gal}(E/F)$$

(product over the finite Galois extensions E of F contained in Ω). This map is injective, because Ω is a union of finite Galois extensions. We give each finite group $\operatorname{Gal}(E/F)$ the discrete topology and $\prod \operatorname{Gal}(E/F)$ the product topology, and we give $\operatorname{Gal}(\Omega/F)$ the subspace topology. Thus the subgroups $\operatorname{Gal}(\Omega/E)$, $[E : F] < \infty$, form a fundamental system of neighbourhoods of 1 in $\operatorname{Gal}(\Omega/F)$.

By the Tychonoff theorem, $\prod \mathrm{Gal}(E/F)$ is compact, and it is easy to see that the image of $\mathrm{Gal}(\Omega/F)$ is closed—hence it is compact and Hausdorff.

Theorem 5.40. *Let Ω be Galois over F with Galois group G. The maps*

$$H \mapsto \Omega^H, \quad M \mapsto \mathrm{Gal}(\Omega/M)$$

define a one-to-one correspondence between the closed *subgroups of G and the intermediate fields M. A field M is of finite degree over F if and only if* $\mathrm{Gal}(\Omega/M)$ *is open in* $\mathrm{Gal}(\Omega/F)$.

Proof. Omit—it is not difficult given the finite case. See for example, E. Artin, Algebraic Numbers and Algebraic Functions, p103. □

Remark 5.41. The remaining assertions in the Fundamental Theorem of Galois Theory carry over to the infinite case provided that one requires the subgroups to be closed.

Example 5.42. Let Ω be an algebraic closure of a finite field $\mathbb{F}_p$. Then $G = \mathrm{Gal}(\Omega/\mathbb{F}_p)$ contains a canonical Frobenius element, $\sigma = (a \mapsto a^p)$, and it is generated by it as a topological group, i.e., G is the closure of $<\sigma>$. Endow $\mathbb{Z}$ with the topology for which the groups $n\mathbb{Z}$, $n \geq 1$, form a fundamental system of neighbourhoods of 0. Thus two integers are close if their difference is divisible by a large integer.

As for any topological group, we can complete $\mathbb{Z}$ for this topology. A Cauchy seqence in $\mathbb{Z}$ is a sequence $(a_i)_{i\geq 1}$, $a_i \in \mathbb{Z}$, satisfying the following condition: for all $n \geq 1$, there exists an N such that $a_i \equiv a_j \mod n$ for $i, j > N$. Call a Cauchy sequence in $\mathbb{Z}$ trivial if $a_i \to 0$ as $i \to \infty$, i.e., if for all $n \geq 1$, there exists an N such that $a_i \equiv 0 \mod n$. The Cauchy sequences form a commutative group, and the trivial Cauchy sequences form a subgroup. We can define $\widehat{\mathbb{Z}}$ to be the quotient of the first group by the second. It has a ring structure, and the map sending $m \in \mathbb{Z}$ to the constant sequence $m, m, m, \ldots$ identifies $\mathbb{Z}$ with a subgroup of $\widehat{\mathbb{Z}}$.

Let $\alpha \in \widehat{\mathbb{Z}}$ be represented by the Cauchy sequence (a_i). The restriction of σ to $\mathbb{F}_{p^n}$ has order n. Therefore $(\sigma|\mathbb{F}_{p^n})^{a_i}$ is independent of i provided it is sufficiently large, and we can define $\sigma^\alpha \in \mathrm{Gal}(\Omega/\mathbb{F}_p)$ to be such that, for each n, $\sigma^\alpha|\mathbb{F}_{p^n} = (\sigma|\mathbb{F}_{p^n})^{a_i}$ for all i sufficiently large (depending on n). The map $\alpha \mapsto \sigma^\alpha : \widehat{\mathbb{Z}} \to \mathrm{Gal}(\Omega/\mathbb{F}_p)$ is an isomorphism.

The group $\widehat{\mathbb{Z}}$ is uncountable. To most analysts, it is a little weird—its connected components are one-point sets. To number theorists it will seem quite natural— the Chinese remainder theorem implies that it is isomorphic to $\prod_{p \text{ prime}} \mathbb{Z}_p$ where $\mathbb{Z}_p$ is the ring of p-adic integers.

Example 5.43. Let Ω be the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$; then $\mathrm{Gal}(\Omega/\mathbb{Q})$ is one of the most basic, and intractible, objects in mathematics. Note that, as far as we know, it could have *every* finite group as a quotient, and it certainly has S_n as a quotient group for every n (and every sporadic simple group, and every...). We do however understand $\mathrm{Gal}(F^{\mathrm{ab}}/F)$ when $F \subset \mathbb{C}$ is a finite extension of $\mathbb{Q}$ and F^{ab} is the union of all finite abelian extensions of F contained in $\mathbb{C}$. For example, $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) \approx \widehat{\mathbb{Z}}^\times$. (This is abelian class field theory—see Math 776.)

6. Transcendental Extensions

In this section we consider fields $\Omega \supset F$ with Ω much bigger than F. For example, we could have $\mathbb{C} \supset \mathbb{Q}$.

Elements $\alpha_1, ..., \alpha_n$ of Ω are said to be *algebraically dependent* over F if there is a nonzero polynomial $f(X_1, ..., X_n) \in F[X_1, ..., X_n]$ such that $f(\alpha_1, ..., \alpha_n) = 0$. Otherwise, the elements are said to be *algebraically independent* over F. Thus they are algebraically independent if

$$a_{i_1,...,i_n} \in F, \quad \sum a_{i_1,...,i_n} \alpha_1^{i_1} ... \alpha_n^{i_n} = 0 \implies a_{i_1,...,i_n} = 0 \text{ all } i_1, ..., i_n.$$

Note the similarity with linear independence. In fact, if f is required to be homogeneous of degree 1, then the definition becomes that of linear independence. The theory in this section is logically very similar to a part of linear algebra. It is useful to keep the following correspondences in mind:

Linear algebra	Transcendence
linearly independent	algebraically independent
$A \subset \text{span}(B)$	A algebraically dependent on B
basis	transcendence basis
dimension	transcendence degree

Example 6.1. (a) A single element α is algebraically independent over F if and only if it is transcendental over F.

(b) The complex numbers π and e are almost certainly algebraically independent over $\mathbb{Q}$, but this has not been proved.

An infinite set A is *algebraically independent* if every finite subset of A is algebraically independent.

Remark 6.2. To say that $\alpha_1, ..., \alpha_n$ are algebraically independent over F, is the same as to say that the map

$$f(X_1, ..., X_n) \mapsto f(\alpha_1, ..., \alpha_n) : F[X_1, ..., X_n] \to F[\alpha_1, ..., \alpha_n]$$

is an injection, and hence an isomorphism. This isomorphism then extends to the fields of fractions,

$$X_i \mapsto \alpha_i : F(X_1, ..., X_n) \to F(\alpha_1, ..., \alpha_n)$$

In this case, $F(\alpha_1, ..., \alpha_n)$ is called a *pure transcendental extension* of F. Then (see 5.28) the polynomial

$$f(X) = X^n - \alpha_1 X^{n-1} + \ldots (-1)^n \alpha_n$$

has Galois group S_n over $F(\alpha_1, ..., \alpha_n)$.

Let $\beta \in \Omega$ and let $A \subset \Omega$. The following conditions are equivalent:

(a) β is algebraic over $F(A)$;
(b) there exist $\alpha_1, \ldots, \alpha_n \in F(A)$ such that $\beta^n + \alpha_1 \beta^{n-1} + \cdots + \alpha_n = 0$;
(c) there exist $\alpha_0, \ldots, \alpha_n \in F[A]$ such that $\alpha_0 \beta^n + \cdots + \alpha_n = 0$;
(d) there exists an $f(X_1, \ldots, X_m, Y) \in F[X_1 \ldots, X_m, Y]$ and $a_1, \ldots, a_m \in F$ such that $f(a_1, \ldots, a_m, Y) \neq 0$ but $f(a_1, \ldots, a_m, \beta) = 0$.

When these conditions hold, we say that β is *algebraically dependent* on A (over F). A set B is *algebraically dependent* on A if each element of B is algebraically dependent on A.

Theorem 6.3 (Fundamental result). *Let $A = \{\alpha_1, ..., \alpha_m\}$ and $B = \{\beta_1, ..., \beta_n\}$ be two subsets of Ω. Assume*

(a) *A is algebraically independent (over F);*
(b) *A is algebraically dependent on B (over F).*

Then $m \leq n$.

Proof. We first prove a lemma. □

Lemma 6.4 (The exchange property). *Let $\{\alpha_1, ..., \alpha_n\}$ be a subset of Ω; if β is algebraically dependent on $\{\alpha_1, ..., \alpha_m\}$ but not on $\{\alpha_1, ..., \alpha_{m-1}\}$, then α_m is algebraically dependent on $\{\alpha_1, ..., \alpha_{m-1}, \beta\}$.*

Proof. Because β is algebraically dependent on $\{\alpha_1, \ldots, \alpha_m\}$, there exists a polynomial $f(X_1, ..., X_m, Y)$ with coefficients in F such that

$$f(\alpha_1, ..., \alpha_m, Y) \neq 0, \quad f(\alpha_1, ..., \alpha_m, \beta) = 0.$$

Write

$$f(X_1, ..., X_m, Y) = \sum_i a_i(X_1, ..., X_{m-1}, Y) X_m^i$$

and observe that, because $f(\alpha_1, \ldots, \alpha_m, Y) \neq 0$, at least one of the polynomials $a_i(\alpha_1, ..., \alpha_{m-1}, Y)$, say a_{i_0}, is not the zero polynomial. Because β is not algebraically dependent on $\{\alpha_1, ..., \alpha_{m-1}\}$, $a_{i_0}(\alpha_1, ..., \alpha_{m-1}, \beta) \neq 0$. Therefore, $f(\alpha_1, ..., \alpha_{m-1}, X_m, \beta)$ is not the zero polynomial. Since $f(\alpha_1, ..., \alpha_m, \beta) = 0$, this shows that α_m is algebraically dependent on $\{\alpha_1, ..., \alpha_{m-1}, \beta\}$. □

Lemma 6.5 (Transitivity of algebraic dependence). *If C is algebraically dependent on B, and B is algebraically dependent on A, then C is algebraically dependent on A.*

Proof. The argument in the proof (2.10) shows that if γ is algebraic over a field E which is algebraic over a field F, then γ is algebraic over F (if $a_1, \ldots, a_n$ are the coefficients of the minimum polynomial of γ over E, then the field $F[a_1, \ldots, a_n, \gamma]$ has finite degree over F). Apply this with $F(A \cup B)$ for E and $F(A)$ for F. □

Proof. (of the theorem). We now prove the theorem. Let k be the number of elements that A and B have in common. If $k = m$, then $A \subset B$, and certainly $m \leq n$. Suppose that $k < m$, and write $B = \{\alpha_1, ..., \alpha_k, \beta_{k+1}, ..., \beta_n\}$. Since α_{k+1} is algebraically dependent on $\{\alpha_1, ..., \alpha_k, \beta_{k+1}, ..., \beta_n\}$ but not on $\{\alpha_1, ..., \alpha_k\}$, there will be a β_j, $k+1 \leq j \leq n$, such that α_{k+1} is algebraically dependent on $\{\alpha_1, ..., \alpha_k, \beta_{k+1}, ..., \beta_j\}$ but not $\{\alpha_1, ..., \alpha_k, \beta_{k+1}, ..., \beta_{j-1}\}$. The exchange lemma then shows that β_j is algebraically dependent on

$$B_1 =_{df} B \cup \{\alpha_{k+1}\} - \{\beta_j\}.$$

Therefore B is algebraically dependent on B_1, and so A is algebraically dependent on B_1 (by the last lemma). If $k+1 < m$, repeat the argument with A and B_1. Eventually we'll achieve $k = m$, and $m \leq n$. □

Definition 6.6. A *transcendence basis* for Ω over F is an algebraically independent set A such that Ω is algebraic over $F(A)$.

Lemma 6.7. *If Ω is algebraic over $F(A)$, and A is minimal among subsets of Ω with this property, then it is a transcendence basis for Ω over F.*

PROOF. If $\alpha_1, \dots, \alpha_m \in A$ are not algebraically independent, then one is algebraically dependent on the remainder, and it follows from (6.5) that Ω will still be algebraic over $F(A)$ after it has been dropped from A. □

THEOREM 6.8. *If there is a finite subset $A \subset \Omega$ such that Ω is algebraic over $F(A)$, then Ω has a finite transcendence basis over F. Moreover, every transcendence basis is finite, and they all have the same number of elements.*

PROOF. In fact, any minimal subset A' of A such that Ω is algebraic over $F(A')$ will be a transcendence basis. The second statement follows from Theorem 6.3. □

The cardinality of a transcendence basis for Ω over F is called the *transcendence degree* of Ω over F. For example, the pure transcendental extension $F(X_1, \dots, X_n)$ has transcendence degree n over F.

EXAMPLE 6.9. Let $p_1, \dots, p_n$ be the elementary symmetric polynomials in $X_1, \dots, X_n$. The field $F(X_1, \dots, X_n)$ is algebraic over $F(p_1, \dots, p_n)$, and so $\{p_1, p_2, \dots, p_n\}$ contains a transcendence basis for $F(X_1, \dots, X_n)$. Because $F(X_1, \dots, X_n)$ has transcendence degree n, the p_i's must themselves be a transcendence basis.

EXAMPLE 6.10. Let Ω be the field of meromorphic functions on a compact complex manifold M.

(a) The only meromorphic functions on the Riemann sphere are the rational functions in z. Hence, in this case, Ω is a pure transcendental extension of $\mathbb{C}$ of transcendence degree 1.

(b) If M is a Riemann surface, then the transcendence degree of Ω over $\mathbb{C}$ is 1, and Ω is a pure transcendental extension of $\mathbb{C}$ $\iff$ M is isomorphic to the Riemann sphere

(c) If M has complex dimension n, then the transcendence degree is $\leq n$, with equality holding if M is embeddable in some projective space.

LEMMA 6.11. *Suppose that A is algebraically independent, but that $A \cup \{\beta\}$ is algebraically dependent. Then β is algebraic over $F(A)$.*

PROOF. The hypothesis is that there exists a nonzero polynomial $f(X_1, ..., X_n, Y) \in F[X_1, ..., X_n, Y]$ such that $f(a_1, ..., a_n, \beta) = 0$, some distinct $a_1, ..., a_n \in A$. Because A is algebraically independent, Y does occur in f. Therefore

$$f = g_0 Y^m + g_1 Y^{m-1} + \cdots + g_m, \quad g_i \in F[X_1, ..., X_n], \quad g_0 \neq 0, \quad m \geq 1.$$

As $g_0 \neq 0$ and the a_i are algebraically independent, $g_0(a_1, ..., a_n) \neq 0$. Because β is a root of

$$f = g_0(a_1, ..., a_n) X^m + g_1(a_1, ..., a_n) X^{m-1} + \cdots + g_m(a_1, ..., a_n),$$

it is algebraic over $F(a_1, ..., a_n) \subset F(A)$. □

PROPOSITION 6.12. *Every maximal algebraically independent subset of Ω is a transcendence basis for Ω over F.*

PROOF. We have to prove that Ω is algebraic over $F(A)$ if A is maximal among algebraically independent subsets. But the maximality implies that, for every $\beta \in \Omega$, $A \cup \{\beta\}$ is algebraically dependent, and so the lemma shows that β is algebraic over $F(A)$. □

THEOREM 6.13 (*). *Every field Ω containing F has a transcendence basis over F.*

PROOF. Let S be the set of algebraically independent subsets of Ω. We can partially order it by inclusion. Let T be a totally ordered subset, and let $B = \cup\{A \mid A \in T\}$. I claim that $B \in S$, i.e., that B is algebraically independent. If not, there exists a finite subset B' of B that is not algebraically independent. But such a subset will be contained in one of the sets in T, which is a contradiction. Now we can apply Zorn's lemma to obtain a maximal algebraically independent subset A. □

It is possible to show that any two (possibly infinite) transcendence bases for Ω over F have the same cardinality.

PROPOSITION 6.14. *Any two algebraically closed fields with the same transcendence degree over F are F-isomorphic.*

PROOF. Choose transcendence bases A and A' for the two fields, and choose a bijection $\varphi : A \to A'$. Then φ extends uniquely to an F-isomorphism $\varphi : F[A] \to F[A']$, and hence to an isomorphism of the fields of fractions $F(A) \to F(A')$. Use this isomorphism to identify $F(A)$ with $F(A')$. Then the two fields in question are algebraic closures of the same field, and hence are isomorphic (Theorem 2.16). □

REMARK 6.15. Any two algebraically closed fields with the same uncountable cardinality and the same characteristic are isomorphic. The idea of the proof is as follows. Let F and F' be the prime subfields of Ω and Ω'; we can identify F with F'. Then show that when Ω is uncountable, the cardinality of Ω is the same as the cardinality of a transcendence basis over F. Finally, apply the proposition.

REMARK 6.16. What are the automorphisms of $\mathbb{C}$? If we assume the axiom of choice, then it is easy to construct many: choose any transcendence basis A for $\mathbb{C}$ over $\mathbb{Q}$, and choose any permutation α of A; then α defines an isomorphism $\mathbb{Q}(A) \to \mathbb{Q}(A)$ that can be extended to an automorphism of $\mathbb{C}$. On the other hand, without the axiom of choice, there are probably only two, the identity map and complex conjugation. (I have been told that any other is nonmeasurable, and it is known that the axiom of choice is required to construct nonmeasurable functions.)

THEOREM 6.17 (Lüroth's theorem). *Any subfield E of $F(X)$ containing F but not equal to F is a pure transcendental extension of F.*

PROOF. See, Jacobson, Lectures in Abstract Algebra III, p157. □

REMARK 6.18. This fails when there is more than one variable—see the footnote on p38 and Noether's conjecture 5.30. The best that is true is that if $[F(X,Y) : E] < \infty$ and F is algebraically closed of characteristic zero, then E is a pure transcendental extension of F (Theorem of Zariski, 1958).