1 Basic Results and Definitions

1.1 Basic Field Theory

Definition. *A field if a set F with two binary operations $+, \cdot$ such that*

1. *$(F, +)$ is an abelian group*
2. *$(F^\times, \cdots)$ is an abelian group where $F^\times = F \setminus \{0\}$*
3. *$+, \cdot$ distribute over each over*

$$a \cdot (b + c) = a \cdot b + a \cdot c \qquad (a + b) \cdot c = a \cdot c + b \cdot c$$

This definition of a field is purely group theoretic, but more commonly we may use some machinery from ring theory to restate the definition as follows:

Definition. *A field is an integral domain (i.e. a ring with no zero divisors) in which every nonzero element is a unit (i.e. has a multiplicative inverse).*

Example. The familiar $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields, the smallest (and also one of the most important) example of a field is

$$\mathbb{F}_2 = \{0, 1\} = \mathbb{Z}/2\mathbb{Z}$$

Lemma 1.1. A nonzero commutative ring R is a field if and only if it only its only ideals are the trivial ideals (0) and $(1) = R$.

Proof. Straightforward. □

Definition. *A subfield of a field F is a subring which is closed under inverses.*

Field homomorphisms are simply ring homomorphisms, however they have the special property that they are automatically injective since the kernel is a proper ideal of the domain.

Definition. *Given a field F, an F-algebra (or algebra over F) is a ring R containing F as a subring. A homomorphisms of F-algebras is a ring homomorphisms which is F-invariant*

$$\phi : R \to R' \qquad \phi(c) = c \quad \forall c \in F$$

Definition. *The characteristic of a field F is the smallest number p such that*

$$p \cdot 1_F = \underbrace{1_F + 1_F + \cdots + 1_F}_{p \text{ times}} = 0$$

In other words it is the smallest p which generates the kernel of the map

$$\mathbb{Z} \to F \qquad n \mapsto n \cdot 1_F$$

There are two possible cases for the characteristic. If the kernel is (0) and the map injective, then we say F has characteristic 0. This means that we can extend the map to get

$$\mathbb{Q} \to F \qquad \frac{m}{n} \mapsto (m \cdot 1_F)(n \cdot 1_F)^{-1}$$

In particular, this is an injection and F contains a copy of $\mathbb{Q}$.

If the kernel is nontrivial, then it must be of the form (p) for some prime p. Thus the map gives an isomorphism

$$\mathbb{Z}/p\mathbb{Z} \cong \{m \cdot 1_F \mid m \in \mathbb{Z}\} \subseteq F$$

and we say that F contains a copy of $\mathbb{F}_p$.

A field isomorphic to $\mathbb{F}_2, \mathbb{F}_3, \cdots \mathbb{F}_p, \mathbb{Q}$ are known as prime fields and every field will contain exactly one prime subfield given by its characteristic. This allows us to generalize the definition

Definition. *A commutative ring R is said to have characteristic p (or 0) if it contains a prime subfield of characteristic p (or 0).*

If a ring R has a nonzero characteristic p, then for all $a \in R$

$$pa = (a + a + \cdots + a) = a(1 + 1 + \cdots + 1) = a0 = 0$$

Conversely, if $pa = 0$ for all $a \in R$ then R has characteristic p. A neat property of nonzero characteristics is that it makes the "freshman's dream" true

$$(a + b)^p = a^p + b^p$$

In particular, this allows us to define a ring (and even $\mathbb{F}_p$-algebra) homomorphism

$$F : R \to R \qquad a \mapsto a^p$$

known as the Frobenius endomorphism. Furthermore, the map $a \mapsto a^{p^n}$ is also a homomorphism as it can obtained by composing the Frobenius with itself n times.

The first major use of Galois theory was in studying roots of polynomials. Thus it makes sense to examine some facts about polynomials and polynomials rings. The main result of note is that there is a one-to-one correspondence

$$\{\text{Nonzero ideals } I \subseteq F[x]\} \iff \{\text{monic polynomials } f \in R[x]\}$$

Furthermore, prime ideals correspond to irreducible monic polynomials.

Lemma 1.2. Let $f \in \mathbb{Z}[x]$. If f factors nontrivially in $\mathbb{Q}[x]$, then it also does in $\mathbb{Z}[x]$

Proposition 1.3. If $f \in \mathbb{Z}[x]$ is monic, then every monic factors of f in $\mathbb{Q}[x]$ lies in $\mathbb{Z}[x]$.

The following proposition gives an easy way to determine if polynomials are irreducible, known as Eisenstein's Criterion.

Proposition 1.4. Consider a polynomial

$$f = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_0 \qquad a_i \in \mathbb{Z}$$

If there exists a prime p such that:

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

then f is irreducible in $\mathbb{Q}[x]$.

This criterion also works for other unique factorization domains by replacing $\mathbb{Q}$ with its field of fractions.

1.2 Field Extensions

Definition. *Let F be a field, a field extension E of F is a field containing F (i.e. an F-algebra which is a field).*

Definition. *The degree of a field extension $[E : F]$ is the dimension of E as an F-vector space. An extension is finite if its degree is finite.*

A useful property of extension degrees it that they multiply.

Proposition 1.5. Let $F \subseteq E \subseteq L$ be fields, then L/F is finite if and only if L/E and E/F are finite, in which case

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

If E/F and E'/F are field extensions, then a homomorphism of field extensions (called a F-homomorphism) is a homomorphism which fixes the elements of F, just like an F-algebra homomorphism.

Example. $[\mathbb{C} : \mathbb{R}] = 2$ because it has basis $\{i, 1\}$.

We will show how to generate field extensions for arbitrary polynomials, but first we must start from the beginning at rings. Recall that the intersection of subrings of a ring is still a ring.

Definition. *Let $F \subseteq E$ be a subfield and $S \subseteq E$ some subset. The intersection of all subrings of E which contain both F and S and is the smallest such subring. We call this subring the subring of E generated by F and S (or generated over F by S), denoted $F[S]$.*

Oftentimes S is finite $S = \{\alpha_1, \cdots, \alpha_n\}$ so we write $F[S] = F[\alpha_1, \ldots, \alpha_n]$.

Lemma 1.6. The ring $F[S]$ consists of all finite linear sums

$$\sum a_{i_1 \cdots i_n} \alpha_1^{i_1} \cdots \alpha_n^{i_n} \qquad a_{i_1 \cdots i_n} \in F \quad \alpha_i \in S$$

Example. The ring $\mathbb{Q}[i]$ consists of all complex numbers $a + bi$ where $a, b \in \mathbb{Q}$. The ring $\mathbb{R}[i]$ is commonly known as $\mathbb{C}$. The ring $\mathbb{Q}[\pi]$ is the ring of sums

$$a_0 + a_1\pi + a_2\pi^2 + \cdots + a_n\pi^n \qquad a_i \in \mathbb{Q}$$

Since the indices/exponents i_j can run through all natural numbers, these sums need not be unique. For instance, in $\mathbb{R}[i]$ we can write $1 = -i^2 = i^4 = \cdots$

Lemma 1.7. Let R be an integral domain which contains a field F (as a subring). If R is finite-dimensional as a F-vector space, then it is a field.

Proof. We just need to show that all nonzero $a \in R$ are units. The map

$$\phi : R \to R \qquad \phi(x) = ax$$

is injective since R is integral and linear by definition. If R can be regarded as a finite-dimensional F-vector space, then ϕ must also be surjective and thus we can find some $b \in R$ such that $\phi(b) = ab = 1$. □

This lemma will come in handy later in proving that our constructed extension is indeed a field. Now we can move on to the next step, which is generating fields. Similar to before, the intersection of a subfields of a field remains a field.

Definition. *Let $F \subseteq E$ be a subfield and $S \subseteq E$ some set. Then the intersection of all subfields which containing F and S is the smallest such subfield and known as the subfield generated by F and S (or generated over F by S), denoted $F(S)$.*

As usual, when S is finite we will write $F(S) = F(\alpha_1, \ldots, \alpha_n)$. The generated subfield can be easily characterized by noting that it must be the field of fractions of the ring $F[S]$. Lemma 1.7 shows that if $F[S]$ is finite dimensional over F, then $F(S) = F[S]$ since it is already a field.

Example. The ring $\mathbb{Q}[i]$ is already a field while the field $\mathbb{Q}(\pi)$ consists of all elements which can be expressed in the form

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

Definition. *An extension E/F is simple if $E = F(\alpha)$ for some $\alpha \in E$.*

Definition. *If $F, F' \subseteq E$ are subfields, then the intersection of all subfields containing F and F' is the smallest such subfield and known as the composite of F and F'. It is denoted $F \cdot F'$ and can also be described as*

$$F \cdot F' = F(F') = F'(F)$$

Now we may proceed with constructing field extensions.

Proposition 1.8. Let $f(X) \in F[X]$ be an irreducible monic polynomial of degree m, then

$$F[x] = F[X]/(f(X))$$

is a field (extension) of degree m over F. Computations in $F[x]$ ultimately come down to computations in F.

By modding out the ideal $(f(X))$, we are essentially appending a root to a field to get an extension. This will become more clear in the following examples.

Example. Let $f(X) = X^2 + 1 \in \mathbb{R}[X]$, then

$$\mathbb{R}[x] = \{a + bx \mid a, b \in \mathbb{R}\}$$

The field operations are

$$(a + bx) + (a' + b'x) = (a + a') + (b + b')x$$

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

$$(a + bx)^{-1} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}x$$

If it is not already obvious by now, we usually identify $i = x$ and this extension is simply $\mathbb{C}$.

Example. Let $f(X) = X^3 - 3X - 1 \in \mathbb{Q}[X]$, an extension is

$$\mathbb{Q}[x] = \left\{a + bx + cx^2 \mid a, b, c \in \mathbb{Q}\right\}$$

Consider the element $\beta = x^4 + 2x^3 + 3$. First we note that this is not fully reduced, in fact

$$\beta = 3x^2 + 7x + 5(\mod x^3 - 3x - 1)$$

Since $f(x)$ is irreducible, we must have $gcd(f, \beta) = 1$ and Euclid's algorithm can be used to find

$$(x^3 - 3x - 1)\left(-\frac{7}{37}x + \frac{29}{111}\right) + (3x^2 + 7x + 5)\left(\frac{7}{111}x^2 - \frac{26}{111}x + \frac{28}{111}\right) = 1$$

Since the first term gets modded out, this gives the inverse

$$\beta^{-1} = \frac{7}{111}x^2 - \frac{26}{111}x + \frac{28}{111}$$

Definition. *Let $f \in F[X]$ be a monic irreducible polynomial. A pair (E, α) consisting of an extension E/F and $\alpha \in E$ is a stem field for f if $E = F[\alpha]$ and $f(\alpha) = 0$.*

In other words a stem field for f is an extension generated by a root of f. Our construction from before gives a stem field for any irreducible monic polynomial ($E = F[x]$ and $\alpha = x$).

Let (E, α) be a stem field and note that there is a surjective F-algebra homomorphism

$$\phi : F[X] \to E \qquad g(X) \mapsto g(\alpha)$$

Ker ϕ is an ideal generated by some nonzero monic polynomial which divides f. But f is irreducible, so Ker $\phi = (f)$, in other words

$$F[x] = F[X]/(f(X)) \cong E$$

Thus the stem field (E, α) is isomorphic to the field we constructed earlier and so every element can be written uniquely in the form

$$a_0 + a_1\alpha + \cdots + a_n m - 1\alpha^{m-1} \qquad a_i \in F, \quad m = \deg(f)$$

This also implies that stem fields are unique up to isomorphism given α. Thus we will sometimes abbreviate the stem field $(F[\alpha], \alpha)$ and just the stem field $F[\alpha]$.

1.3 Algebraic and Transcendental Elements

Definition. *Let E/F be a field extension. An element $\alpha \in E$ is algebraic if it is the root of some polynomial $f \in F[X]$, otherwise it is transcendental.*

We can view algebraic elements in terms of kernels. An elements $\alpha \in E/F$ defines a homomorphism

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

which is just the "evaluate at α" map. There are two possibilities for the kernel. If the kernel is trivial, then α is transcendental and we have an isomorphism

$$F[X] \cong F[\alpha] \quad \text{extends to} \quad F(X) \cong F(\alpha)$$

If the kernel is nonzero, then α is algebraic and the polynomials $g \in F[X]$ for which $g(\alpha) = 0$ for an ideal. In particular, this ideal is generated by some monic polynomial of least degree, this polynomial is given special importance and can be characterized in different ways.

Definition. *A polynomial $f \in F[X]$ is the minimal polynomial of α over F is any of the conditions hold:*

1. *f is monic, irreducible, and $f(\alpha) = 0$*
2. *f is the monic polynomial of least degree such that $f(\alpha) = 0$*
3. *f is monic, $f(\alpha) = 0$ and f divides every other $g \in F[X]$ for which $g(\alpha) = 0$*

We know that the minimal polynomial f must be irreducible because otherwise it's two factors evaluated at α would give two nonzero elements of E which multiply to zero. Note that when α is algebraic, there is an isomorphism

$$F[X]/(f) \to F[\alpha] \qquad g(X) \mapsto g(\alpha)$$

Since the first is a field, $F[\alpha]$ is also a field, in particular it's a stem field for f.

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

From the definition we see that a field extension E/F is transcendental if any element of E is transcendental over F. Thus algebraic extensions can (and should) be considered "nice" extensions.

Proposition 1.9. Let E/F be a field extension. If E is finite, then it is algebraic and finitely generated (as a field) over F. Conversely, if E is generated over F by a finite set of algebraic elements, then it is finite over F.

Corollary 1.10. a) If E/F is algebraic, then every subring of E containing F is a field. In other words, every subextension of an algebraic extension is algebraic.

b) Suppose $F \subset E \subset L$, if L/E is algebraic and E/F is algebraic, then L/F is algebraic.

Proof. a) For any $\alpha \in R$, $F[\alpha] \subset R$. But α is algebraic over F so $F[\alpha]$ is a field, thus $\alpha^{-1} \in R$ as well.

b) By assumption, every $\alpha \in L$ is the root of a monic polynomial

$$X^m + a_{m-1}X^{m-1} + \cdots + a_0 \in E[X]$$

We have a tower of extensions

$$F[a_0, \ldots, a_{m-1}, \alpha] \supseteq F[\alpha_0, \ldots, a_{m-1}] \supset \cdots \supset F$$

each of which is generated from the next using a single algebraic element (since E/F is algebraic) and thus are finite. Since the index is multiplicative, this implies that $F[a_0, \ldots, a_{m-1}, \alpha]$ is finite over F and thus α is algebraic over F. □

In general, while it is cool and good to have a field extension which contains a single root of some polynomial f, it is even more cool and good to have an extension which contains every root.

Definition. *Let F be a field. A polynomial is said to split in $F[X]$ if it can be expressed as a product of polynomials of degree ≤ 1 in $F[X]$.*

Proposition 1.11. For a field Ω, the following are equivalent:

a) Every nonconstant polynomial in $\Omega[X]$ splits in Ω

b) Every nonconstant polynomial in $\Omega[X]$ has at least one root in Ω

c) The only irreducible polynomials in $\Omega[X]$ are those of degree 1

d) Every field of finite degree over Ω equals Ω

Proof. $a \to b \to c$ are obvious.

$c \to a$ follows from the fact that $\Omega[X]$ is a unique factorization domain.

$c \to d$: Let E/Ω be a finite extensions and $\alpha \in E$. Since the minimal polynomial of α is irreducible, it is of degree 1 and so $\alpha \in \Omega$

$d \to c$: Let $f \in \Omega[X]$ be irreducible, then $\Omega[X]/(f)$ is an extension of degree $\deg f$. But every finite extension must equal Ω, so $\deg f = 1$. □

Definition. *A field which satisfies any of the above conditions is said to be algebraically closed. An algebraic closure of another field F is a field which is algebraic closed and algebraic over F.*

The classic example comes from the fundamental theorem of algebra, which states that $\mathbb{C}$ is algebraically closed and in particular it is an algebraic closure of $\mathbb{R}$. We'll give a better criterion for determining when an extension is algebraically closed.

Proposition 1.12. If Ω is algebraic over F and every polynomial $f \in F[X]$ splits in $\Omega[X]$, then Ω is algebraically closed and thus an algebraic closure of F.

Proof. Let $f \in \Omega[X]$ be a nonconstant polynomial. We know that f has a root α in some finite extension Ω'/Ω (e.g. a stem field). Let

$$f = a_n X^n + \cdots + a_0 \qquad a_i \in \Omega$$

and consider the sequence of extensions

$$F \subset F[a_0, \cdots, a_n] \subset F[a_0, \cdots, a_n, \alpha]$$

Each extension is generated by a finite number of algebraic elements □

Finally, we give a quick and easy way to construct an algebraic closure.

Proposition 1.13. Let $F \subset \Omega$, then the set

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

is a field, called the algebraic closure of F in Ω.

Proof. Suppose α, β are algebraic over F, then $F[\alpha, \beta]$ is a finite field extensions over F since it is generated by algebraic elements. Thus every element of $F[\alpha, \beta]$ is algebraic over F, in particular $\alpha \pm \beta, \alpha/\beta, \alpha\beta$. □

Corollary 1.14. Let Ω be an algebraically closed field. For every subfield $F \subseteq \Omega$, the algebraic closure of F in Ω is an algebraic closure of F.

Proof. Let E be the algebraic closure of F in Ω, which is algebraic over F by construction. Since Ω is algebraically closed, every polynomial in $F[X]$ will split in $\Omega[X]$. The roots will lie in E and so it splits in $E[X]$ as well, thus E is an algebraic closure of F. □

The corollary shows that every subfield of $\mathbb{C}$ has an algebraic closure. More generally, we can prove that every field has an algebraic closure, but the proof will require invoking the axiom of choice.

1.4 Additional Exercises

Exercise 1.1. Let $E = \mathbb{Q}[\alpha]$ where $\alpha^3 - \alpha^2 + \alpha + 2 = 0$. Express $(\alpha^2 + \alpha + 1)(\alpha^2 - \alpha)$ and $(\alpha - 1)^{-1}$ in the from $a\alpha^2 + b\alpha + c$ where $a, b, c \in \mathbb{Q}$.

Solution: First note that in $q[\alpha]$, higher order polynomials can be reduced using

$$\alpha^3 = \alpha^2 - \alpha - 2$$

Thus we can just use normal polynomial multiplication and then reduce to get

$$\begin{aligned}(\alpha^2 + \alpha + 1)(\alpha^2 - \alpha) &= \alpha^4 - \alpha \\ &= \alpha(\alpha^2 - \alpha - 3) \\ &= \alpha^3 - \alpha^2 - 3\alpha \\ &= -4\alpha - 2\end{aligned}$$

To obtain an inverse, we use the Euclidean algorithm. Luckily we only need one step

$$\alpha^3 - \alpha^2 + \alpha + 2 = (\alpha^2 + 1)(\alpha - 1) + 3$$

$$\frac{1}{3}(\alpha^3 - \alpha^2 + \alpha + 2) - \frac{1}{3}(\alpha^2 + 1)(\alpha - 1) = 1$$

$$\therefore (\alpha - 1)^{-1} = -\frac{\alpha^2 + 1}{3}$$

Exercise 1.2. Determine $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}]$

Solution: We intuitively expect the degree to be 4 because a basis is $\left\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\right\}$, but let's verify that explicitly by writing the degree as

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$$

The minimal polynomial of $\sqrt{2}$ in $\mathbb{Q}$ is clearly $X^2 - 2$ so the degree of that stem field is 2. The minimal polynomial of $\sqrt{3}$ in $\mathbb{Q}(\sqrt{2})$ is still $X^2 - 3$ because Eisenstein's criterion still holds ($p = 3$ is still prime). Thus we compute the degree

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 2 \cdot 2 = 4$$

Exercise 1.3. Let F be a field and $f(X) \in F[X]$.

a) For every $a \in F$, show that there is a polynomial $q(X) \in F[X]$ such that

$$f(X) = q(X)(X - a) + f(a)$$

b) Deduce that $f(a) = 0$ if and only if $(X - a) \mid f(X)$

c) Deduce that $f(X)$ can have at most $\deg f$ roots.

d) Let G be a finite abelian group. If G has at most m elements of order dividing m for each divisor m of $|G|$, show that G is cyclic.

e) Deduce that every finite subgroup of $F^\times$ for a field F is cyclic.

Solution: a) Dividing $f(X)$ by $X - a$ gives the desired $q(X)$

b) If $f(a) = 0$, then per the previous statement we can write $f(X) = q(X)(X - a) + 0$ and thus $(X - a) \mid f(X)$. Conversely, if $(X - a) \mid f(X)$, then there exists some $q(X)$ such that $f(X) = q(X)(X - a)$ and thus $f(a)$ must be zero.

c) We must have $\deg q = \deg f - 1$. For every root of f, we can reduce the degree of q by 1. This can only be done $\deg f$ times before q becomes a constant and f becomes completely factorized. Since factorization in $F[X]$ is unique, there can only be at most $\deg f$ roots.

d) A finite abelian group can be decomposed into cyclic factors

$$G = C_n \oplus C_m \oplus \cdots$$

Where $m, n, \ldots$ are prime powers. In general they need not be unique, but this would violate the assumption that G has at most m elements of order diving m. If $gcd(m, n) \neq 1$, then there exists a prime p which divides both m, n. This results in (at least) p^2 elements of order p, a contradiction.

If $gcd(m, n) = 1$, then $mn \mid |G|$ and there are two cases. If $mn = |G|$, then $G = C_m \oplus C_n \cong C_{mn}$ and thus is cyclic. Otherwise there is another cyclic factor and we repeat the argument until we either get a nontrivial gcd, or there is only one cyclic factor remaining. Either way, G will be cyclic.

e) The elements of order m in $F^\times$ are just the roots of the polynomial $X^m - 1$. We proved earlier that there can be at most m roots of that polynomial, so we can apply the previous proposition to show that $F^\times$ is cyclic.

Exercise 1.4. Let $f(X)$ be an irreducible polynomial over F of degree n and E a field extension of F of degree m. If $gcd(m, n) = 1$, then f is irreducible over E.

Solution: Suppose f is reducible and that $g \in E[X]$ is an irreducible factor. Let (L, α) be a stem field of g over E and note

$$[L : F] = [L : E][E : F] = (\deg g) \cdot m \longrightarrow m \mid [L : F]$$

We can construct a stem field another way, but noting that α is also a root of f and so $(F[\alpha], \alpha)$ is a stem field for f over F. Since $F[\alpha] \subset L$,

$$[L : F] = [L : F[\alpha]][F[\alpha] : F] = [L : F[\alpha]] \cdot n \longrightarrow n \mid [L : F]$$

But $gcd(m, n) = 1$ so we must have $[L : F] = mn$ since $\deg g < \deg f$ and so $\deg g = n$ which means that $f = g$ is irreducible in E.

Exercise 1.5. Show that there does not exist a polynomial $f \in \mathbb{Z}[x]$ of degree > 1 that is irreducible mod p for all primes p.

Solution: Suppose such an f exists, the polynomials $f(X) \pm 1$ have finitely many roots in $\mathbb{Z}$. Thus there must exist some $n \in \mathbb{Z}$ such that $f(n) \neq \pm 1$. Let p be a prime diving $f(n)$ and we will have a field $\mathbb{F}_p$ for which f is not irreducible.

Exercise 1.6. Let $\alpha = \sqrt[3]{2}$ and let R be the set of complex numbers of the form $a + b\alpha + c\alpha^2$ with $a, b, c \in \mathbb{Q}$. Show that R is a field.

Solution: One way to see that R is a field is to note that it is a stem field for $X^3 - 2$ over $\mathbb{Q}$. Explicitly, R is clearly a ring so we just need to find inverses. Since $X^3 - 2$ is irreducible, Euclid's algorithm will give us polynomials p, q such that

$$p(X)(X^3 - 2) + q(X)(a + bX + cX^2) = 1$$

$q(X)$ will be the desired inverse and thus R is a field.

2 Splitting Fields

2.1 Definition

Let $E/F, E'/F$ be extensions, recall that an F-homomorphism of extensions is a field homomorphism $\phi : E \to E'$ such that $\phi(a) = a$ for all $a \in F$. An F-isomorphism is just a bijective F-homomorphism. Since an F-homomorphism can be interpreted as an injective F-linear map of F-vector spaces, an F-isomorphism requires that $\deg E = \deg E'$ over F.

Proposition 2.1. Let $F(\alpha)/F$ be a simple extension and Ω/F some other extension.

a) Let α be transcendental over F. Then for every F-homomorphism $\phi : F(\alpha) \to \Omega$, $\phi(\alpha)$ is transcendental over F and there is a one-to-one correspondence

$$\{F\text{-homomorphisms } F(\alpha) \to \Omega\} \iff \{\text{elements of } \Omega \text{ transcendental over } F\}$$

given by $\phi \mapsto \phi(\alpha)$

b) Let α be algebraic over F with minimal polynomial f. Then for every F-homomorphism $\phi : F[\alpha] \to \Omega$, $\phi(\alpha)$ is a root of f in Ω and there is a one-to-one correspondence

$$\{F\text{-homomorphisms } F[\alpha] \to \Omega\} \iff \{\text{roots of } f \text{ in } \Omega\}$$

given by $\phi \mapsto \phi(\alpha)$.

This result can be slightly generalized.

Proposition 2.2. Let $F(\alpha)/F$ be a simple extension and $\phi_0 : F \to \Omega$ a homomorphism into some other field Ω.

a) Let α be transcendental over F. then then there is a one-to-one correspondence

$$\{\text{extensions } \phi : F(\alpha) \to \Omega \text{ of } \phi_0\} \iff \{\text{elements of } \Omega \text{ transcendental over Im } \phi_0\}$$

given by $\phi \mapsto \phi(\alpha)$

b) Let α be algebraic over F with minimal polynomial f. Then then there is a one-to-one correspondence

$$\{\text{extensions } \phi : F[\alpha] \to \Omega \text{ of } \phi_0\} \iff \{\text{roots of } \phi_0 f \text{ in } \Omega\}$$

given by $\phi \mapsto \phi(\alpha)$

Note that we denote with $\phi_0 f$, then polynomial in $\Omega[X]$ obtained by applying ϕ to the coefficients of f.

Definition. *Consider a polynomial $f \in F[X]$. An extension E/F is said to split f if f factors into linear components in $E[X]$*

$$f(X) = a \prod (X - \alpha_i) \qquad \alpha_i \in E$$

If E splits f and is generated by its roots

$$E = F[\alpha_1, \ldots, \alpha_n]$$

then E is said to be a splitting field (or root field) for f.

Another way to characterise the splitting field is that it is the smallest field which splits f.

Example. Let $f(X) = aX^2 + bX + c$. The field $\mathbb{Q}[\sqrt{b^2 - 4ac}] \subseteq \mathbb{C}$ is a splitting field for f and is known as a quadratic extension.

A common goal is to compute a splitting field for a given polynomial, we will prove that this is always possible.

Proposition 2.3. Every polynomial $f \in F[X]$ has a splitting field E_f and

$$[E_f : F] \leq (\deg f)!$$

Proof. Let $F_1 = E[\alpha_1]$ be a stem field for some irreducible factor of f in F. Then let $F_2 = F_1[\alpha_2]$ be a stem field for $f/(X - \alpha_1)$ in $F_1[X]$. Continuing in this fashion gives a splitting field E_f and

$$[E_f : F] = [F_1 : F][F_2 : F_1] \cdots \leq n(n-1) \cdots = n!$$

where $n = \deg f$. □

Example. Let p be prime and $f = (X^p - 1)/(X - 1)$. If ξ is one root, then the remaining roots are $\xi^2, \xi^3, \ldots, \xi^{p-1}$ and so the splitting field is also the stem field $\mathbb{Q}[\xi]$. This is not necessarily true if p is not prime because then not all powers of ξ are outside of $\mathbb{Q}$.

Now we investigate the relationship between any field which splits f and the splitting field of f.

Proposition 2.4. Let $f \in F[X]$, E/F an extension generated by the roots of f and Ω/F some other extension which splits f.

a) There exists an F-homomorphism $\phi : E \to \Omega$, the number of such homomorphisms is at most $[E : F]$ with equality if f has distinct roots in Ω.

b) If F, Ω are both splitting fields, then every F-homomorphism $E \to \Omega$ is an isomorphism. Thus splitting fields are unique up to isomorphism.

Corollary 2.5. Let $E/F, L/F$ be extensions with E finite over F.

a) The number of F-homomorphisms $E \to L$ is at most $[E : F]$

b) There exists a finite extension Ω/L with an F-homomorphism $E \to \Omega$.

2.2 Multiple Roots

First we show that if two polynomials are relatively prime in some base field F, then they will remain relatively prime in any extension Ω/F.

Proposition 2.6. Let $f, g \in F[X]$ and Ω/F an extension. If $gcd(f, g) = r(X)$ computed in $F[X]$, then it is also the gcd in $\Omega[X]$. In particular, distinct monic irreducible polynomials in $F[X]$ do not acquire a common root in any extension of F.

Proof. Let $r_F(X), r_\Omega(X)$ be the gcd's of f, g in F and Ω respectively. Clearly $r_F \mid r_\Omega$ in $\Omega[X]$. However, we can write using Euclid's algorithm

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

where $a, b \in F[X]$. Thus we see that $r_\Omega \mid r_F$ and thus they are equal. □

This allows us to talk about *the* greatest common divisor between two polynomials without specifying the field in which we actually perform the calculation in.

Let $f \in F[X]$ be some polynomial and E/F an extension which splits f

$$f = a\prod_{i=1}^{r}(X - \alpha_i)^{m_i} \qquad \sum m_i = \deg f$$

The m_i are known as the multiplicities of the root α_i. If $m_i > 1$, then α_i is a multiple root of f, otherwise it is a simple root. We claim (without proof) that the m_i are extension-independent and thus a multiple root of one extension is a multiple root in all other extensions which split f.

Example. Let F be a field of characteristic $p \neq 0$ and $a \in F$ an element that is not a p-th power. Then $X^p - a$ is irreducible but splits in $(X - \alpha)^p$ in its splitting field. Thus irreducible polynomials may have multiple roots.

We would like a way to be able to determine when a polynomial has multiple roots. If we can factor $f = \prod f_i^{m_i}$ with each f_i irreducible, then it obviously has a multiple root if any $m_i > 1$. However if $m_i = 1$, that is all irreducible factors are distinct, then the previous proposition tells us that f has as multiple root if and only if one of the f_i has a multiple root. In other words, we just need a way to determine if an irreducible polynomial has a multiple root.

Recall the standard derivative from calculus. We will the underlying limiting process and instead state it only as the power rule

$$f(X) = \sum a_i X^i \mapsto f'(X) = \sum i a_i X^{i_1}$$

with the standard sum and product rules holding. However note that the derivative of X^p is zero in fields of characteristic p

Proposition 2.7. For a nonconstant polynomial $f\ in F[X]$, the following are equivalent

a) f has a multiple root

b) $gcd(f, f') \neq 1$

c) F has nonzero characteristic p and f is a polynomial in X^p

d) All roots of f are multiple

Proof. $a \to b$) Let α be a multiple root of f and write $f = (X-\alpha)^m g(X)$, then

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

Since $m > 1$, we see that $gcd(f, f') \neq 1$

$b \to c$) Since f is irreducible, $gcd(f, f') \neq 1$ implies that we must have $f' = 0$. For a general polynomial,

$$f = a_0 + \cdots a_d X^d \qquad f' = a_1 + \cdots + d a_d X^{d-1}$$

f' is the zero polynomial if and only if F has characteristic $p \neq 0$ and $a_i = 0$ for all i not divisible by p, i.e. $f(X) = g(X^p)$.

$c \to d$) From the hypothesis

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

and we see that all roots have multiplicity at least p.

$d \to a$) Obvious □

Proposition 2.8. For a nonconstant polynomial $f\ in F[X]$, the following are equivalent

a) $gcd(f, f') = 1$

b) All roots of f are simple

Proof. If $gcd(f, f') = 1$, then we see from the previous proof that f, f' will have no common factors, thus not common root. Therefore f will only have simple roots. Conversely, if f only has simple roots, then $gcd(f, f')$ must be constant because otherwise there will be a common root. □

Definition. *A polynomial is said to be separable if each of its irreducible factors has only simple roots.*

From the equivalent criteria of having multiple roots, a nonconstant irreducible polynomial $f \in F[X]$ is no separable if and only if F has characteristic $p \neq 0$ and f is a polynomial in X^p. More generally, if $f = \prod f_i$ with each f_i monic and irreducible. Then f is separable if and only if each f_i is distinct and separable.

If a polynomial is separable in $F[X]$, then it will remain separable as a polynomial in $E[X]$ for every extension E of F.

Definition. *A field F is perfect if it has characteristic zero or if it has characteristic p and every element of F is a p-th power.*

Thus, a field F is perfect if and only if $F = F^q$, where q is the characteristic exponent of F (1 is characteristic 0, p otherwise). The reason we care about perfect fields is because they are connected to our previous discussion of separable polynomials and multiplicity of roots.

Proposition 2.9. A field F is perfect if and only if every irreducible polynomial in $F[X]$ is separable.

Proof. The proposition is obvious is F has characteristic zero, so suppose F has characteristic $p \neq 0$. If F contains an element a that is not a p-th power, then $X^p - a$ is irreducible but not separable. Conversely, if every element of F is a p-th power, then every polynomial in X^p (i.e. not separable) can be written

$$\sum a_i X^{ip} = \left(\sum b_i X^i\right)^p \qquad a_i = b_i^p$$

and is thus not irreducible. □

Example. Every algebraically closed field (e.g. $\mathbb{C}$) is perfect. Every union of perfect fields in perfect, thus every field algebraic over $\mathbb{F}_p$ is perfect.

Example. A finite field is perfect because then the Frobenius endomorphism is bijective. If F has characteristic $p \neq 0$, then $F(X)$ is not perfect because X is not a p-th power.

2.3 Additional Exercises

Exercise 2.1. Let F be a field of characteristic $\neq 2$.

a) Let E be a quadratic extension of F and show that

$$S(E) = \left\{a \in F^\times \mid a \text{ is a square in } E\right\}$$

is a subgroup of $F^\times$ containing $F^{\times 2}$

b) Let E, E' be quadratic extensions of F, show that there exists an F-isomorphism $\phi : E \to E'$ if and only if $S(E) = S(E')$

c) Show that there is an infinite sequence of fields $E_1, E_2, \ldots$ with each E_i a quadratic extension of $\mathbb{Q}$ such that $E_i \ncong E_j$ for $i \neq j$.

d) Let p be an odd prime. Show that, up to isomorphism, there is exactly one field with p^2 elements.

Solution: a) Obvious

b)

Exercise 2.2. a) Let F be a field of characteristic p, show that if $X^p - X - a$ is reducible in $F[X]$, then it splits into distinct factors.

b) For every prime p, show that $X^p - X - 1$ is irreducible in $\mathbb{Q}[X]$.

Solution: a) Since F is characteristic p, if α is a root of $X^p - X - a$ in some splitting field, then $\alpha + 1, \ldots, \alpha + p - 1$ are the remaining roots. Thus if $\alpha \in F$, then the roots are automatically distinct. We know that this polynomial is reducible,

$$X^p - X - a = (X^r + a_1 X + \cdots + a_r)(X^{p-r} + \cdots) \qquad 0 < r < p$$

By Vieta's formula, $-a_1$ is the sum of the roots of the first factor, which is guaranteed to be in the form

$$-a_1 = r\alpha + d \qquad d \in \mathbb{Z} \cdot 1_F$$

Since $a_1 \in F$, we see that $\alpha \in F$.

b) Note that $0, 1$ are not roots of $X^p - X - 1$ in $\mathbb{F}_p$, thus there cannot be p distinct roots. Then by the previous exercise, this polynomial is irreducible in $\mathbb{F}_p[X]$ and thus $\mathbb{Z}[X], \mathbb{Q}[X]$.

Exercise 2.3. Construct a splitting field for $X^5 - 2$ over $\mathbb{Q}$, what is its degree over $\mathbb{Q}$?

Solution: The splitting field is $\mathbb{Q}[\xi, \sqrt[5]{2}]$ where ξ is a 5th root of unity

$$\xi = e^{2i\frac{n\pi}{5}} = \cos\left(\frac{2n\pi}{5}\right) + i\sin\left(\frac{2n\pi}{5}\right) \qquad n = 1, \ldots, 4$$

We can easily see that $[\mathbb{Q}[\xi] : \mathbb{Q}] = 4$ and $[\mathbb{Q}[\sqrt[5]{2}] : \mathbb{Q}] = 5$, thus the overall degree is 20.

Exercise 2.4. Find a splitting field for $X^{p^m} - 1 \in \mathbb{F}_p[X]$, what is its degree over $\mathbb{F}_p$?

Solution: Simply note that $(X-1)^{p^m} = X^{p^m} - 1$, so $\mathbb{F}_p$ is already a splitting field.

Exercise 2.5. Let $f \in F[X]$ where char $F = 0$. Let $d = gcd(f, f')$ and show that $g(X) = f(X)d(X)^{-1}$ has the same roots of $f(X)$ and they are all simple roots of $g(X)$.

Solution: Write f in its factored form

$$f = \prod_{i=1}^{r} (X - \alpha_i)^{m_i}$$

where the α_i are distinct. Then we can compute

$$f' = \prod_{i=1}^{r} m_i (X - \alpha_i)^{m_i - 1} \qquad g = \prod_{i=1}^{r} \frac{X - \alpha_i}{m_i}$$

and the roots of g are clearly simple and the same roots as f.

Exercise 2.6. Let $f \in F[X]$, where char $F = p$, be irreducible. Show that $f(X)$ can be written

$$f(X) = g\left(X^{p^e}\right)$$

where $g(X)$ is irreducible and separable. Deduce that every root of $f(X)$ has the same multiplicity p^e in any splitting field.

Solution: If f is not separable, then it is a polynomial in X^p, that is $f(X) = f_1(X^p)$ where f_1 must also be irreducible. If f_1 is not separable, then we can write $f_1(X) = f_2(X^p)$. Continuing in this fashion gives a separable and irreducible $g(X)$ such that $f(X) = g(X^{p^e})$ and

$$f(X) = \prod (X^{p^e} - \alpha_i)$$

where the α_i are distinct, so the multiplicity of every root is p^e.