Notes on Fields and Galois Theory

Prepared by Greyson C. Wesley

Spring 2022

Abstract

These notes are based on the lectures for the Algebra II course on Field and Galois Theory, delivered by Professor Andy Putman at the University of Notre Dame during the Spring 2022 semester. The content primarily focuses on the fundamentals of field theory, extensions, and the Galois correspondence.

Contents

§1 Field Theory

§1.1 Basics of Fields

Definition 1.1. A field is a nonzero ring such that for all nonzero $x \in R$ there is some $y \in R$ with $xy = 1$.

Lemma 1.2.

A field R is an integral domain.

Proof. If $xz = 0$ and x is nonzero then we can multiply by y with $xy = 1$ to get $yxz = 0 = 1z = z$, so $z = 0$ as desired. □

Lemma 1.3.

If R is a field and $xy = xy' = 1$ then $y = y'$.

Proof. We have $xy - xy' = 0$ so $x(y - y') = 0$, and since R is an integral domain by the above lemma we have $y - y' = 0$ so that $y = y'$. □

Lemma 1.4.

A ring R is a field if and only if ideals of R are exactly 0 and R.

Proof. If R is a field and $I \subseteq R$ is some nonzero ideal then there's some nonzero $x \in I$, so $1 = x^{-1}x \in I$, and hence $I = R$.

Conversely, let only the ideals of R be zero and R. Then for any nonzero $x \in R$ $(x) \neq 0$, so $(x) = R$ by the previous lemma. But then $1 \in (x)$, so there exists a y with $xy = 1$ as desired. □

Recall that an ideal $\mathfrak{m} \subseteq R$ is maximal if $\mathfrak{m} \neq R$ and the only ideals I with $\mathfrak{m} \subseteq I \subseteq R$ are $\mathfrak{m}$ and R. Zorn's lemma then implies that any ideal $J \subsetneq R$ with $J \neq R$, is contained inside some maximal ideal $\mathfrak{m}$ of R. Indeed, since we can pick a maximal element of the partially ordered set (by inclusion), i.e. by Zorn's lemma we can choose a maximal element from. $\{I \subseteq R : I \text{ an ideal}, J \subseteq I, I \neq R\}$.

Lemma 1.5.

If R is a ring with an ideal $I \subsetneq R$ then I is maximal if and only if R/I is a field.

Proof. By one of the isomorphism theorems (or the correspondence theorem) there's a bijection from proper ideals of $J \subsetneq R$. Then the latter contains 0 and R/I if and only if the former contains I and R. □

1.1.1 Characteristic of a field

It is easy to show that for any ring R there's a unique ring homomorphism $\varphi : \mathbb{Z} \to R$, namely the one determined by $\varphi(1) = 1_R$ (so that $\varphi(n) = 1_R + \cdots + 1_R$). Kernels of ring homomorphisms are equivalently ideals, so the kernel of this homomorphism is the ideal (n) for some $n \in \mathbb{Z}$ (since $\mathbb{Z}$ is a PID).

We can say even more about this when the ring is a field.

Proposition 1.6.

If F is a field and $\varphi\colon \mathbb{Z} \to F$ is a ring homomorphism then $\ker\varphi \in \{(0), (p)\}$, where p is a prime.

Proof. φ induces an injection $\mathbb{Z}/(n) \hookrightarrow F$. F has no zero divisors, so $\mathbb{Z}/(n)$ doesn't either. If $n \neq 0$ or a prime then we can write $n = k, \ell$ with $k, \ell \notin \{\pm 1, 0\}$. □

Definition 1.7 (Field characteristic)**.** The generator of the kernel of a ring homomorphism $\mathbb{Z} \to F$, denoted $\operatorname{char}\mathbb{F}$, is called the ***characteristic*** of $\mathbb{F}$.

Definition 1.8 (Prime Field)**.** If F has characteristic p for a prime p, then the image of the injective ring homomorphism $\mathbb{Z}/p\mathbb{Z} \hookrightarrow F$ is called the ***prime field***, and it is a subfield of F.

If F has characteristic 0 then $\mathbb{Z} \hookrightarrow F$, and since F is a field this extends to a unique homomorphism $\mathbb{Q} \hookrightarrow F$. We call the image of the injection $\mathbb{Q} \hookrightarrow F$ the ***prime field*** of F.

§1.2 Field Extensions

Definition 1.9 (Field extension)**.** Given fields F_1 and F_2, the only ring homomorphism $f : F_1 \to F_2$ are 0 or injections ($\ker(f)$ is an ideal in F_1, so either $\ker(f) = 0$, i.e. f is an injection, or $\ker(f) = F_1$, i.e. $f = 0$). If f is an injection, then we can identify F_1 with $f(F_1)$. So $F_1 \hookrightarrow F_2$. We call F_2 a ***field extension*** of F, and we write $F_1 \subseteq F_2$ (or sometimes F_2/F_1).

Example 1.10. Every field is a field extension of its prime field.

Example 1.11. Main examples:

1. ***Number fields***, e.g. fields K with $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$ (note this necessitates $\operatorname{char} K = 0$). For instance, $K = \mathbb{Q}, \mathbb{Q}[i], \mathbb{Q}[\sqrt{2}]$ are all number fields.

2. ***Finite fields*** k, i.e. $|k| < \infty$, which necessitates $\operatorname{char}(k) = p$. $\mathbb{F}_p \subseteq K$. We will soon show that for each r there's a unique finite field K with $|K| = p^r$ (and these are all the finite fields). Warning: For $r \geq 2$, $\mathbb{Z}/p^r\mathbb{Z}$ is ***not*** a field.

3. ***Function fields***, i.e. extensions of $\mathbb{Q}(t) = \left\{\frac{f(t)}{g(t)} : f, g \in \mathbb{Q}[t], g \neq 0\right\}$. These, of course, require $\operatorname{char}\mathbb{F} = 0$.

1.2.1 Algebraic and Transcendental Elements of Field Extensions

Definition 1.12. Let $K \subseteq L$ be a field extension and let $\alpha \in L$. We say α is ***algebraic*** over K if there exists some nonzero polynomial $f \in K[x]$ with $f(\alpha) = 0$. If α is not algebraic, we say α is ***transcendental***.

Example 1.13. $\sqrt{2} \in \mathbb{Q}$ is algebraic over $\mathbb{Q}$, $\pi \in \mathbb{R}$ is transcendental over $\mathbb{Q}$, $2\pi i \in \mathbb{C}$ is algebraic over $\mathbb{R}$ (since it's a zero of $x^2 + 4\pi^2$).

The observation here is that algebraic vs transcendental depends on the base field we're working in.

Notation 1.14. Let $K \subseteq L$ be a field extension.

- $k[\alpha]$ is the ***ring generated by k and α***, given by
$$k[\alpha] = \{c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_n\alpha^n : n \geq 0 \text{ and } c_1, \ldots, c_n \in k\}.$$
- $k(\alpha)$ is the ***field generated by k and α***, given by
$$k(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} : f, g \in k[x], g(\alpha) \neq 0 \right\}.$$

Lemma 1.15.

Let $K \subseteq L$ be a field extension. If $\alpha \in L$ is transcendental over k then $k(\alpha) \cong k(t)$.

Proof. We have $\varphi : k[t] \to t$, $f(t) \mapsto f(\alpha)$ is a ring homomorphism. Since α is transcendental, we have $\ker \varphi$ is trivial, i.e. φ is injective. Hence φ induces an injection $\psi : k(t) \to L$, $\frac{f}{g} \mapsto \frac{\varphi(p)}{\varphi(g)}$ with $\operatorname{im} \psi = k(\alpha)$. □

The above lemma therefore reduces the study to field extensions made by adjoining transcendental elements to the study of polynomial rings.

Proposition 1.16.

If $K \subseteq L$ is a field extension and $\alpha \in L$, then both $k[\alpha]$ and $k(\alpha)$ are vector spaces over k.

Proof. Trivial. □

Lemma 1.17.

If $K \subseteq L$ be a field extension with $\alpha \in L$ then α is algebraic over k if and only if the k-vector space $k[\alpha]$ is finite dimensional.

Proof. For the forward direction assume α is algebraic and $c_n\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_0 = 0$ with $c_i \in k$, $c_n \neq 0$. Thus

$$\alpha^n = \frac{c_{n-1}}{c_n}\alpha^{n-1} + \cdots + \frac{c_0}{c_n}, \tag{\dagger}$$

and hence the set $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ span $k[\alpha]$ as a k-vector space. (Use ($\dagger$) to express α^m with $m \geq n$ as a sum of lower order terms.)

Conversely, if the dimension over k of $k(\alpha)$ is finite then the infinite set $\{1, \alpha, \alpha^2, \dots, \}$ is linearly dependent. Hence we can find for sufficiently large n that

$$c_0 + c_1\alpha^1 + \cdots + c_n\alpha^n = 0,$$

i.e. α is algebraic, as desired. □

Proposition 1.18.

Let $K \subseteq L$ be a field extension and $\alpha \in L$ be algebraic over k. Then $k[\alpha] = k(\alpha)$, i.e. $k[\alpha]$ is a field.

Proof. We'll prove the claim in two separate ways.

Proof 1. This proof uses that $\dim_k(k[\alpha])$ is finite.

Consider nonzero $x \in k[\alpha]$. We must prove that there's a $y \in k[\alpha]$ such that $xy = 1$. Define $\psi : k[\alpha] \to k[\alpha]$, $\psi(z) = xz$. We must be careful since ψ is ***not*** a ring homomorphism since $\psi(z_1z_2) = xz_1z_2 \neq (xz_1)(xz_2) = \psi(z_1)\psi(z_2)$. However, ψ is k-linear—indeed,

$$\psi(z_1 + k_2) = x(z_1 + z_2) = xz_1 + xz_2 + \psi(z_1) + \psi(z_2)$$

and

$$\psi(kz) = x(kz) = k(xz) = k\psi(z).$$

A key fact here is that since there are no zero divisors, $\ker(\psi) = 0$. Hence ψ is injective as a linear map from finite-dimensional vector space to itself, and so ψ is an isomorphism. In particular, we can find $y \in k[\alpha]$ with $y \in k[\alpha]$ with $\psi(y) = 1$, i.e. $xy = 1$. □

Proof 2. This proof directly use the fact that α is algebraic.

We have a ring homomorphism $\varphi : k[x] \to k[\alpha]$ by $\varphi(f) = f(\alpha)$. φ is not injective and $k[x]$ is a PID, so there's some nonzero $f \in k[x]$ with $\ker(\varphi) = (f)$ (the ideal generated by f). We claim f is an irreducible polynomial. Indeed, if $f = f_1f_2$ is a nontrivial factorization (i.e. with both $\deg f_1, \deg f_2 \geq 1$) then

$$0 = f(\alpha) = f_1(\alpha)f_2(\alpha),$$

so either $f_1(\alpha) = 0$ or $f_2(\alpha) = 0$. Without loss of generality, suppose $f_1(\alpha) = 0$. Then $f_1 \in \ker\varphi = (f)$, contradicting the fact that $\deg(f_1) < \deg(f)$ (since the factorization is nontrivial). We now make an observation—since $f \in k[x]$ is irreducible, the ideal generated by f, (f), must be a maximal ideal. Indeed, any ideal I with $(f) \subsetneq I \subsetneq k[x]$ must be of the form $I = (g)$, and $(f) \subsetneq (g)$, so g must be a *proper* factor of f. Since (f) is a *maximal* ideal, we know that $k[x]/(f)$ is a field (has no ideals other than 0 and itself). But $k[\alpha]$ is the image of the embedding $k[x]/(f) \hookrightarrow L$, so $k[x]/(f) \cong k[\alpha]$, and since $k[x]/(f)$ is a field it follows that $k[\alpha]$ is a field as desired. □

Each of the two proofs above give that $k[\alpha]$ is a field, but we don't yet know whether or not $k[\alpha]$ coincides with $k(\alpha)$. We have $k(\alpha) = \left\{\frac{f(\alpha)}{g(\alpha)} : f, g \in [x], g(\alpha) \neq 0\right\}$. So an element of $k(\alpha)$ of the form $\frac{1}{g(\alpha)} f(x)$. If we know $\frac{1}{g(\alpha)} \in k[\alpha]$ then $\frac{1}{g(\alpha)} f(\alpha) \in k[\alpha]$, as desired. □

Notation 1.19. For fields $K \subseteq L$ and $\alpha_1, \dots, \alpha_n \in L$,

- $K[\alpha_1, \dots, \alpha_n]$ is the subring of L generated by K and $\alpha_1, \dots, \alpha_n$ $(= (K[\alpha_1, \dots, \alpha_{n-1}])[\alpha_n])$.
- $K(\alpha_1, \dots, \alpha_n)$ is the subfield of L generated by K and $\alpha_1, \dots, \alpha_n$ $(= K(\alpha_1, \dots, \alpha_{n-1}))(\alpha_n)$.

Theorem 1.20.

For fields $K \subseteq L$ and $\alpha_1, \dots, \alpha_n \in L$ algebraic over K, we have

- $K[\alpha_1, \dots, \alpha_n] = K(\alpha_1, \dots, \alpha_n)$ and
- $\dim_K K[\alpha_1, \dots, \alpha_n] < \infty$.

Proof. By induction on n. For the base case $n = 0$, there's nothing to prove.

Now let $n \geq 1$ and assume true for $n - 1$. The induction hypothesis gives

$$K[\alpha_1, \dots, \alpha_n] = (K[\alpha_1, \dots, \alpha_{n-1}])[\alpha_n] = (K(\alpha_1, \dots, \alpha_n))[\alpha_n] \tag{$*$}$$

Since α_n is algebraic over K, it is also algebraic over $K(\alpha_1, \dots, \alpha_n)$. Hence from last time we have that $(*)$ equals $(K(\alpha_1, \dots, \alpha_{n-1}))(\alpha_n) = K(\alpha_1, \dots, \alpha_n)$.

We know from last time that $\dim_{K(\alpha_1, \dots, \alpha_{n-1})} K(\alpha_1, \dots, \alpha_{n-1})[\alpha_n] < \infty$. But

$$K(\alpha_1, \dots, \alpha_{n-1})[\alpha_n] = K(\alpha_1, \dots, \alpha_n),$$

so $\dim_{K(\alpha_1, \dots, \alpha_{n-1})} K(\alpha_1, \dots, \alpha_n) < \infty$, so the dimension is some finite m. Let $b_1, \dots, b_m$ be a basis for $K(\alpha_1, \dots, \alpha_n)$ as a vector space over $K(\alpha_1, \dots, \alpha_{n-1})$. By induction we know that $\dim_K K(\alpha_1, \dots, \alpha_{n-1} < \infty$, so we can find a basis $c_1, \dots, c_\ell$ for $K(\alpha_1, \dots, \alpha_{n-1})$ as a vector space over K.

We claim that $\{c_i b_j : 1 \leq i \leq \ell, 1 \leq j \leq m\}$ *spans* $K(\alpha_1, \dots, \alpha_n)$ as a vector space over K. Indeed, consider $x \in K(\alpha_1, \dots, \alpha_n)$. We can write

$$x = \lambda_1 b_1 + \dots + \lambda_m b_m \qquad (\lambda_i \in K(\alpha_1, \dots, \alpha_n))$$

For each i we can then write

$$\lambda_i = \mu_1^i c_1 + \cdots + \mu^i c_\ell \qquad (\mu_j^i \in K)$$

Then $x = \sum_{j=1}^{\ell} \sum_{i=1}^{m} \mu_j^i c_j b_i$.

(The reverse direction: if $\dim_K[\alpha] < \infty$ then $1, \alpha, \alpha^2, \alpha^3, \ldots$ must be linearly dependent, so we can find $\lambda_0, \ldots, \lambda_{n-1} \in K$ with $\alpha^n + \lambda_{n-1}\alpha^{n-1} + \cdots + \alpha_0 \cdot 1 = 0$)

(Another argument: Define $\mu : K[\alpha] \to K[\alpha]$ by $\mu(z) = \alpha z$. Then μ is a linear map between finite dimensional vector spaces, so by the Cayley-Hamilton theorem, letting f be its characteristic polynomial, we have $f(\mu) = 0$. Thus $0 = f(\mu)(z) = f(\alpha)z$. □

Remark 1.21. We change "fields" here, but this is actually just the same as changing vector spaces since these are vector spaces.

Corollary 1.22.

For a field extension $K \subseteq L$, if $\alpha, \beta \in L$ are algebraic over K then both $\alpha + \beta$ and $\alpha\beta$ are algebraic over K.

Proof. We have

$$K \subseteq K[\alpha + \beta] \subseteq K[\alpha, \beta]$$

By the above theorem we know $\dim_K K[\alpha, \beta] < \infty$, so $\dim_K K[\alpha + \beta] < \infty$. Hence $\alpha + \beta$ are algebraic. The same argument works for $\alpha\beta$. □

1.2.2 The minimal polynomial of algebraic elements

Definition 1.23 (minimal polynomial)**.** For fields $K \subseteq L$ and $\alpha \in L$ algebraic, the ***minimal polynomial of α over K*** is a monic polynomial $f \in K[x]$ of minimal possible degree with α as a root.

Proposition 1.24.

Consider an algebraic element α of a field extension $K \subseteq L$. Then we have the following points.

1. The minimum polynomial for α is unique.
2. The minimal polynomial for α is irreducible.
3. If $g(\alpha) = 0$ for some $g \in K[x]$ then f divides g.

Proof. We prove each point.

1. The minimal polynomial generates the kernel of the map $K[x] \to L$ with $g \mapsto g(\alpha)$. Since this kernel is an ideal in $K[x]$ (thanks to $g \mapsto g(\alpha)$ being a homomorphism) and $K[x]$ is a PID, we can show that the minimal polynomial is unique—indeed, if f_1, f_2 are monic polynomials that generate the ideal, i.e. $(f_1) = (f_2)$, then f_1 divides f_2 and f_2 divides f_1, forcing $f_1 = f_2$.

2. The minimal polynomial f is irreducible in $K[x]$. Indeed, if $f = f_1 f_2$ with f_1, f_2 nonconstant, then $0 = f(\alpha) = f_1(\alpha) f_2(\alpha)$, so since $K[x]$ is an integral domain we have that either $f_1(\alpha) = 0$ or $f_2(\alpha) = 0$, contradicting the minimality of the degree of f.

3. If f is the minimal polynomial of α and g is another polynomial with $g(\alpha) = 0$ then f divides g. Indeed, $g \in \ker(K[x] \to L, g \mapsto g(\alpha))$. But this kernel is generated by f as shown in an observation above, so $g \in (f)$, and hence f divides g.

This completes the proof. □

Example 1.25 (minimal polynomial of $\sqrt{i}$ over different fields)**.** Consider $\sqrt{i} \in \mathbb{C}$. There are two of them, but they are only defined up to multiplication by ±1. We'll choose one. We now find the minimal polynomial of $\sqrt{i}$ over given fields:

- Over $\mathbb{Q}$? Let $x = \sqrt{i}$. Then $x^2 = i$, so $x^4 = -1$. Thus $f = x^4 + 1$. (However, this should be proven more rigorously)
- Over the Gaussian rationals $\mathbb{Q}[i]$? Well, if $x = \sqrt{i}$ then $x^2 = i$ so $x^2 - i = 0$, so we can take $g = x^2 - i$. This is different from $x^4 + 1$. So the minimal polynomial depends on the base field. (Note that $x^2 - i$ divides $x^4 + i$ in $\mathbb{Q}[i]$.)
- Over $\mathbb{C}$? Well it is linear since we can just take $h = x - \sqrt{i}$ (and it is an almost trivial argument that this is the minimal polynomial).

§1.3 Comparing Field Extensions

Definition 1.26. Let $K \subseteq L_1$ and $K \subseteq L_2$ be two field extensions. A ***field isomorphism relative to K*** (or a ***K-isomorphism***) is a field (ring) isomorphism $\varphi : L_1 \to L_2$ such that $\varphi|_K = \mathrm{id}_K$.

Lemma 1.27.

For field extensions $K \subseteq L_1$ and $K \subseteq L_2$, if $\varphi : L_1 \to L_2$ is a field isomorphism relative to K and $\alpha \in L_1$ is algebraic with minimal polynomial $f \in K[x]$, then $\varphi(\alpha) \in L_2$ is algebraic and also has minimal polynomial f.

Proof. (version 2 from next class) Since f is irreducible over K is enough to show $f(\varphi(\alpha)) = 0$, we can write $f(x) = x^n +_{n-1} x^{n-1} + \cdots + c_0$, where $c_i \in K$. Then

$0 = f(\alpha) = \alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_0$, so applying φ gives

$$\begin{aligned} 0 &= \varphi(\alpha)^n + \varphi(c_{n-1})\varphi(\alpha)^{n-1} + \cdots + \varphi(c_0) \\ &= \varphi(\alpha)^n + c_{n-1}\varphi(\alpha)^{n-1} + \cdots + c_0 \\ &= f(\varphi(\alpha)), \end{aligned}$$

completing the proof. □

Theorem 1.28.

Let $K \subseteq K[\alpha]$ and $K \subseteq K[\beta]$ be field extensions with $\alpha, \beta \in L$ algebraic over K for some L with $K \subseteq L$. Then $K[\alpha]$ is isomorphic to $K[\beta]$ relative to K if and only if α and β have the same minimal polynomial over K.

Proof. ($\Rightarrow$) This is the previous lemma.

($\Leftarrow$) Let $f \in K[x]$ be the common minimal polynomial of α and β. Thus $(f) \subseteq K[x]$ is the kernel of the map $K[x] \twoheadrightarrow K[\alpha]$ with $g \mapsto g(\alpha)$. Thus by the (first) homomorphism theorem we have an isomorphism $\psi_\alpha : K[x]/(f) \xrightarrow{\cong} K[\alpha]$. Similarly, we have $\psi_\beta : K[x]/(f) \xrightarrow{\cong} K[\beta]$. Define $\varphi : K[\alpha] \to K[\beta]$ via the composition

$$\varphi : K[\alpha] \xrightarrow{\psi_\alpha^{-1}} K[x]/(f) \xrightarrow{\psi_\beta} K[\beta].$$

Then φ is an isomorphism relative to K. □

Definition 1.29. Given a field extension $K \subseteq L$, the ***degree*** of L over K is $[L : K] := \dim_K(L)$, where L refers here to the vector space over K.

Lemma 1.30.

Assume $\operatorname{char}\mathbb{F} \neq 2$ and let $K \subseteq L$ be a degree 2 (quadratic) field extension. Then $L = K[\sqrt{d}]$ for some $d \in K$ that is not a perfect square.

Proof. We first prove $K[\sqrt{d}]$ has degree 2. To do this we note that

$$K[\sqrt{d}] = \left\{a + b\sqrt{d} : a, b \in K\right\},$$

meaning $\dim_K K[\sqrt{d}] \leq 2$. But it is not one since d is not a square, and hence $K[\sqrt{\delta}]$ has degree 2. These are all possibilities since, given a degree 2 extension $K \subseteq L$, if we have $\alpha \in L$ with $\alpha \notin K$ then since $\dim_K(L) = 2$ the set $\{1, \alpha\}$ must be a vector space basis.

In particular, we can write $\alpha^2 = -b\alpha - c$ for some $b, c \in K$, or that $\alpha^2 + b\alpha + c = 0$. That is, $f(x) = x^2 + bx + c$ is the minimal polynomial of α. By the quadratic formula, the roots of f are

$$x = \frac{-b \pm \sqrt{b^2 - 4c}}{2}. \qquad \text{(since we can divide by 2 because } \operatorname{char}\mathbb{F} \neq 2\text{)}$$

α is one of these, so $L = K[\alpha] = K[\sqrt{b^2 - 4c}]$. □

Remark 1.31. The previous lemma is false in higher degrees. For instance, there exist degree three field extensions $K \subseteq L$ such that L is not of the form $K[\sqrt[3]{d}]$. We will later be able to give examples of such extensions.

Lemma 1.32.

Consider a field extension $K \subseteq L$ with $L = K[\alpha]$. Let $f \in K[x]$ be the minimal polynomial of α. Then

$$[L : K] = \deg(f).$$

Proof. We have

$$f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0,$$

so

$$\alpha^n = -c_{n-1}\alpha^{n-1} - \cdots - c_0,$$

i.e. α^n is a linear combination of some lower degree alphas. Thus $\{1, \ldots, \alpha^{n-1}\}$ span $L = K[\alpha]$ as a K-vector space, and moreover this set is linearly independent—indeed, a nontrivial linear dependence $d_{n-1}\alpha^{n-1} + d_0 1 = 0$ gives a lower degree polynomial vanishing at α. □

Example 1.33. Let $L = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$. This is a degree 4 extension because all elements take the form

$$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6},$$

where $a, b, c, d \in \mathbb{Q}$. (This can be checked by showing that the product of elements of the above form is also of this form.) We claim that in fact

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

It is enough to show that $\sqrt{2} + \sqrt{3}$ is a root of an irreducible degree 4 polynomial. We have

$$\begin{aligned}
(\sqrt{2} + \sqrt{3})^0 &= 1,\\
(\sqrt{2} + \sqrt{3})^1 &= \sqrt{2} + \sqrt{3},\\
(\sqrt{2} + \sqrt{3})^2 &= 5 + 2\sqrt{6},\\
(\sqrt{2} + \sqrt{3})^3 &= 11\sqrt{2} + 9\sqrt{3},\\
(\sqrt{2} + \sqrt{3})^4 &= 49 + 20\sqrt{6}.
\end{aligned}$$

Thus $(\sqrt{2}+\sqrt{3})^4 = 10(\sqrt{2}+\sqrt{3})^3 - 1$. Hence our candidate is $f := x^4 - 10x^2 + 1$. Since f is irreducible over $\mathbb{Q}$, we have that $\mathbb{Q}[\sqrt{2}, \sqrt{3}] = \mathbb{Q}[\sqrt{2}+\sqrt{3} \cong \mathbb{Q}[x]/(x^4 - 10x^2 + 1)$.

This result means that we can write $\sqrt{2}$ and $\sqrt{3}$ in $\mathbb{Q}[\sqrt{2}+\sqrt{3}]$. How do we do this? We know that $(\sqrt{2}+\sqrt{3})^1 = \sqrt{2}+\sqrt{3}$ and $(\sqrt{2}+\sqrt{3})^3 = 11\sqrt{2}+10\sqrt{3}$. Hence

$$\sqrt{2} = \frac{(\sqrt{2}+\sqrt{3})^3 - 10(\sqrt{2}+\sqrt{3})^1}{2},$$

and similarly for $\sqrt{3}$.

In the above example we found f by expanding out powers of $(\sqrt{2}+\sqrt{3})^n$ for $0 \leq n \leq 4$. These all sit in the 4-dimensional vector space

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \left\{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in \mathbb{Q}\right\}.$$

What is a more general situation? For instance, how do we know that $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ are linearly independent in this vector space? We will give general tools for this on the coming homeworks.

More generally, consider a field extension $K \subseteq L$ and algebraic elements $\alpha, \beta \in L$ over K with minimal polynomials $f, g \in K[x]$, respectively. How do we find the minimal polynomial of $\alpha + \beta$? It would help to study the vector space $K[\alpha, \beta]$. Let $d = \deg(f)$ and $e = \deg(g)$. Then we know that α^d is in the vector space with basis $(1, \alpha, \ldots, \alpha^{d-1})$ (for instance, the polynomial $f = x^4 - 3x^3 - 2x^2 + 1$ gives $\alpha^4 = 3\alpha^3 + 2\alpha^2 - 1$). Similarly, β^e is in the vector space with basis $(1, \beta, \ldots, \beta^{e-1})$. Our question: How do we get a basis for $K[\alpha, \beta]$?

Lemma 1.34.

In the above notation, $K[\alpha, \beta]$ is spanned as a K-vector space by

$$S := \{\alpha^n \beta^m : 0 \leq n \leq d-1, 0 \leq m \leq e-1\}.$$

Warning: These are not always linearly independent!

Proof. It is clearly spanned by $T := \{\alpha^n \beta^m : n, m \geq 0\}$. But if $\alpha^n \beta^m \in T \setminus S$ then we can use the fact that $\alpha^d \in \operatorname{span}_K\{1, \ldots, \alpha^{d-1}\}$ and $\beta^e \in \operatorname{span}_{\mathbb{F}}\{1, \ldots, \beta^{e-1}\}$ to write $\alpha^n \beta^m$ as a linear combination of $\alpha^{n'}$ and $\beta^{n'}$ with either $n' < n$, $m' \leq m$ or $n' \leq n$, $m' < m$. Representing this, express all elements of T as linear combinations of elements of S. □

Remark 1.35 (Why the above lemma does not give a basis)**.** We can now expand out powers of $(\alpha + \beta)^k$ and write as linear combinations of members of the set $\{\alpha^n \beta^m : 0 \leq n \leq d-1, 0 \leq m \leq e-1\}$. By linear algebra, we can write $(\alpha + \beta)^{de}$ as a linear combination of $(\alpha + \beta)^k$, where $0 \leq k \leq de - 1$.

But f might not be irreducible! The issue is that the lemma only provides a spanning set, not a basis. So some though must be put into it after this to make sure it works out and is indeed a basis. To do this, we must factor f into a product of irreducibles in order to find the minimal polynomial.

Example 1.36. Consider the roots $\alpha_1, \alpha_2, \alpha_3$ of $f = x^3 - 2$ in $\mathbb{Q}[x]$. These are $\alpha_1 = \sqrt[3]{2}$, $\alpha_2 = \omega\sqrt[3]{2}$, $\alpha_3 = \omega^2\sqrt[3]{2}$, where $\omega = e^{2\pi i/3}$ is a third primitive root of unity. The lemma then gives us that a spanning set for $\mathbb{Q}[\alpha_1, \alpha_2]$ is $\{\alpha_1^n, \alpha_2^m : 0 \leq n \leq 2, 0 \leq m \leq 2\}$. Note that this actually has nine elements. However, we can write $\mathbb{Q}[\alpha_1, \alpha_2]$ in a different way. Namely, since $\omega = \alpha_2/\alpha_1$, we have ω is a root of $g = x^3 - 1 = (x-1)(x^2+x+1)$, so the minimal polynomial of ω is $x^2 + x + 1$. Applying the lemma to $\mathbb{Q}[\alpha_1, \omega]$, we get the K-spanning set $\{\alpha^n, \omega^m : 0 \leq n \leq 2, 0 \leq m \leq 1\}$

$$\mathbb{Q}[\alpha_1, \alpha_2] = \mathbb{Q}[\alpha_1, \omega]$$

So the original 9 elements are not linearly independent. In fact, we will later show $[\mathbb{Q} : \mathbb{Q}[\alpha_1, \omega]] = 6$.

Theorem 1.37: Multiplicative Property of the Degree.

Given nested field extensions $K \subseteq L \subseteq M$, we have

$$[M : K] = [M : L][L : K].$$

Proof. If either $[K : L]$ or $[L : M] = \infty$ then this is easy, so we assume all are finite. Let $d := [K : L], e = [L : M]$. Find a basis $(m_1, \ldots, m_e)$ for M as an L-vector space and $(\ell_1, \ldots, \ell_d)$ for L as a K-vector space. Define

$$S := \{\ell_i m_j : 1 \leq i \leq d, 1 \leq j \leq e\}.$$

Claim 1: S spans M as a K-vector space. Indeed, consider $x \in M$. Write $x = \lambda_1 m_1 + \cdots + \lambda_e m_e$ with $\lambda_i \in L$. Then write $\lambda_i = c_{i,1}\ell_1 + \cdots + c_{i,d}\ell_d$ with $c_{ij} \in K$. Then $X = \sum_{i=1}^{e} \sum_{j=1}^{d} c_{ij}\ell_j m_i$, as desired.

Claim 2: S is linearly independent. Indeed, assume $\sum_{\substack{i=1,\ldots,e \\ j=1,\ldots,d}} c_{ij}\ell_j m_i = 0$. Then

$$0 = \left(\sum\nolimits_{j=1}^{d} c_{1j}\ell_j\right) m_1 + \cdots + \left(\sum\nolimits_{j=1}^{d} c_{ej}\ell_j\right) m_e.$$

Each parenthesized term above is in L, so since $(m_1, \ldots, m_\ell)$ form a basis for M over L, we must have that each $\sum_{j=1}^{d} c_{ij}\ell_j = 0$. Since ℓ_j is a basis for L over K, we conclude $c_{ij} = 0$.

This gives that S forms a basis for M as a K-vector space, and hence the result. □

Example 1.38. Consider the roots of $f(x) = x^2 - 2$, namely $\alpha_1 = \sqrt[3]{2}$, $\alpha_2 = \omega\sqrt[3]{2}$, $\alpha_3 = \omega^2\sqrt[3]{2}$, where $\omega = e^{2\pi i/3}$ is a primitive third root of unity, we claim that

$$[\mathbb{Q} : \mathbb{Q}[\alpha_1, \alpha_2, \alpha_3]] = 6.$$

We have a sequence of extensions $\mathbb{Q} \subseteq \mathbb{Q}[\omega] \subseteq \mathbb{Q}[\omega, \alpha_1]$ and $\mathbb{Q} \subseteq \mathbb{Q}[\alpha_1] \subseteq \mathbb{Q}[\omega, \alpha_1]$. We know by the spanning lemma that $[\mathbb{Q} : \mathbb{Q}[\omega, \alpha_1]] \leq 6$ by the old lemma. But using the theorem we get that *both* $2 = [\mathbb{Q} : \mathbb{Q}[\omega]]$ and $3 = [\mathbb{Q} : \mathbb{Q}[\alpha_1]]$ divide it by the previous theorem, that it must be exactly 6, as previously claimed.

Example 1.39. Let α be a root of $x^4 - 12x^3 + 15x^2 - 3$. This is irreducible (since this is Eistenstein at $p = 3$). Set $\beta := \sqrt[3]{2}$. Set $L = \mathbb{Q}[\alpha, \beta]$. The same reasoning shows first that $[\mathbb{Q} : l] \leq 12$ because we're adjoining a degree 4 thing and a degree 3 thing, and also that it must be divisible by both 4 and 3. And hence the degree is exactly equal to 12, as desired.

Example 1.40. Let $K = \mathbb{Q}[\sqrt[4]{3}, i]$. We know that $[\mathbb{Q} : K] \leq 4 \cdot 2 = 8$, but naively applying the theorem gives that this is divisible by 2 and 4, which is not good enough to show equality. So what do we have to show? Well, we have a chain of extensions

$$\mathbb{Q} \subseteq \mathbb{Q}[\sqrt[4]{3}] \subseteq \mathbb{Q}[\sqrt[4]{3}, i].$$

The left extension above has degree 4, so we must show that the right extension above $\mathbb{Q}[\sqrt[4]{3}, i]$ has degree 2. Then the total degree is the product of 4 and 2, i.e. 8. That is, we must show that the minimal polynomial $x^2 + 1$ stays irreducible over $\mathbb{Q}[\sqrt[4]{3}]$. But this is easy since $\mathbb{Q}[\sqrt[4]{3}] \subseteq \mathbb{R}$, so it does not contain $\pm i$.

§1.4 Constructions of Fields

Up until now, all the field extensions we have constructed are of the form $\mathbb{Q} \subseteq L$ for some $L \subseteq \mathbb{C}$, e.g. $\mathbb{Q}(\sqrt{2})$. But what can we do if we don't have a large ambient field like $\mathbb{C}$?

For instance, we may want to consider extensions of finite fields like $\mathbb{F}_p$ or the field of rational functions $\mathbb{Q}(t)$? We need to develop a technology to do this.

Lemma 1.41.

If K is a field and $f \in K[x]$ is a monic irreducible then the quotient ring

$$L := K[x]/(f)$$

is a field extension of K, and f has a root in L.

Proof. If $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0$ then $K[x]/(f)$ is an n-dimensional K-vector space (since in it we have $x^n = -c_{n-1}x^{n-1} - \cdots - c_0$). Let $z \in K[x]/(f)$ be nonzero. We desire an inverse for z. Note that $\varphi_z : K[x]/(f) \to K[x](f)$ by $\varphi_z(\overline{g}) := z\overline{g}$ is a linear map between finite-dimensional K-vector spaces. We claim φ_z is injective. Indeed, $K[x]/(f)$ has no zero divisors—if it did then we could find $g, h \in K[x]$ that are not in (f) such that $gh \in (f)$, i.e. such that $gh = \lambda f$ for some $\lambda \in K[x]$. But then f divides g and h in $K[x]$, so since f is irreducible we must have that f divides g or f divides h. But then $g \in (f)$

or $h \in (f)$, a contradiction. Since φ_z is injective, it must be an isomorphism. That is, we can find some $w \in K[x]/(f)$ such that $zw = 1$. This shows that $K[x]/(f)$ is a field.

We now show that $K[x]/(f)$ is a field extension of K. Let $\alpha \in K[x]/(f)$ be the image of x. Then $f(\alpha) = 0$ in $K[x]/(f)$, so $K \subseteq K[x]/(f)$ is indeed a field extension of the form $K(\alpha)$, where α is a root of f. □

Example 1.42 (Construction of $\mathbb{C}$ from $\mathbb{R}$)**.** Note that the complex numbers $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$ is obtained from $\mathbb{R}$ by adjoining a $\sqrt{-1}$, that is, by adjoining a root of an irreducible polynomial $x^2 + 1$. That is, $\mathbb{C} = \mathbb{R}(\sqrt{-1})$. Per the above, we have in particular that

$$\mathbb{C} = \mathbb{R}[x]/(x^2 + 1),$$

and define $i \in \mathbb{C}$ to be the image of x under the canonical map $\mathbb{R}[x] \mapsto \mathbb{R}[x]/(x^2+1) =: \mathbb{C}$, giving the desired result that $\mathbb{C} = \mathbb{R}(\sqrt{-1})$.

Example 1.43 (Construction of $\mathbb{F}_4$ from $\mathbb{F}_2$)**.** Consider the irreducible polynomial $f \in \mathbb{F}_2[x]$ given by $f(x) = x^2 + x + 1$. Define $L := \mathbb{F}_2[x]/(f)$, and let $\alpha \in L$ be the image of x.

By the above we know L is a new field, and

$$L = \{a + b\alpha : a, b \in \mathbb{F}_2\}.$$

Thus $|L| = 4$, and we have the multiplication rule

$$\begin{aligned}(a + b\alpha)(c + d\alpha) &= ac + (ad + bc)\alpha + bd\alpha^2. \\ &= ac + bd + (ad + bc + bd)\alpha. \qquad \text{(since } \alpha^2 = \alpha + 1 \text{ in } \mathbb{F}_2(\alpha))\end{aligned}$$

It turns out this is the only field of order 4, which we denote by $\mathbb{F}_4$. In fact, we will soon be able to construct *all* finite fields. It should go without saying that $\mathbb{F}_4 \neq \mathbb{Z}/4\mathbb{Z}$ (since $\mathbb{Z}/4\mathbb{Z}$ has zero divisors and is thus not even a field!).

Lemma 1.44.

Let $K \subseteq L$ be a field extension and $f, g \in K[x]$ with $g \neq 0$. If division with remainder in $K[x]$ gives $f = qg + r$ for some $q, r \in K[x]$ and division with remainder in $L[x]$ gives $f = q'g + r'$, then $q' = q$ and $r' = r$.

Proof. q and r are the unique polynomials with $f = qg + r$ and $\deg(r) < \deg(g)$. This still holds when K is extended to L. (WHY?) □

Corollary 1.45.

If $K \subseteq L$ is a field extension with $f, g \in K[x]$ then g divides f in $K[x]$ if and only if g divides f in $L[x]$.

Proof. g divides f means that $f = qg + r$ has $r = 0$. But division with remainder in L yields exactly what is yielded by division with remainder in $K[x]$, so the remainder in $K[x]$ iff the remainder in $L[x]$ is zero. □

Corollary 1.46.

If $K \subseteq L$ is a field extension and $f, g \in K[x]$ then the greatest common divisor of f and g are the same in $K[x]$ and $L[x]$.

Proof. We find $\gcd(f, g)$ using the Euclidean algorithm. Recall that to do this we set

$$f = q_1 g + r_1 \qquad (\deg(r_1) < \deg(g))$$

Anything that divides both f and g must also divide r_1, so we then have that $g = q_2 r_1 + r_2$ with $\deg(r_2) < \deg(r_1)$

$$f = q_1(q_2 r_1 + r_2) + r_1. \qquad (\deg(r_2) < \deg(r_1))$$

Repeating, we get $r_1 = q_3 r_2 + r_3$ where $\deg(r_3) < \deg(r_2)$, we get

$$f = q_1(q_2(q_3 r_2 + r_3) + r_2) + (q_3 r_2 + r_3), \qquad (\deg(r_3) < \deg(r_2))$$

and so on, until we get

$$r_{n-1} = q_n r_n + 0,$$

which implies that $r_n = \gcd(f, g)$. At each step we divided with remainder, which doesn't depend on whether we work in $K[x]$ or $L[x]$ per the previous results, as desired. □

Lemma 1.47.

If $K \subseteq L$ is a field extension and $f, g \in K[x]$ have a common root $\alpha \in L$ then f and g are *not* relatively prime in $K[x]$.

In particular, this means we can write $f = hf_1$ and $g = hg_1$ with h irreducible. It will follow from the proof that then $h(\alpha) = 0$.

Proof. Suppose for a contradiction that f and g are relatively prime in $K[x]$. We can then write

$$1 = a(x)f(x) + b(x)f(x),$$

with $a, b \in K[x]$. Then

$$1 = a(\alpha)f(\alpha) + b(\alpha)g(\alpha) = 0 + 0 = 0,$$

a contradiction. □

Notation 1.48 (Terminology)**.** Let K be a field and let $f \in K[x]$ have $\deg(f) \geq 1$. A ***splitting field for f*** is a field L containing K such that f splits into linear factors

$$f(x) = c(x - \lambda_1) \cdots (x - \lambda_n)$$

where $c, \lambda_i \in L$ and for which L is generated by λ_i. (Note that c is the leading coefficient of f and so in fact $c \in K$).

Proof. Write

$$f = f_1 \cdots f_n \tag{$*$}$$

with $f_i \in K[x]$ are irreducible. If $\deg(f_i) = 1$ for each i then we're done. Otherwise let L_1 be an extension of K such that one of of the f_i with $\deg(f_i) > 1$ has a root. In L_1, f_i factors as $(x - \lambda)g_i$s. So the irreducible factorization of f in $L[x]$ strictly refines the factorization $(*)$. Continuing this process, we extend

$$K \subseteq L_1 \subseteq L_2 \subseteq \cdots \subseteq L_m$$

such that at each step $(*)$ factors further. We're done when only linear factors remain. □

§1.5 Ruling out separability

1.5.1 Formal Derivative of a Polynomial

Let K be a field and $f \in K[x]$. Writing $f = c_n x^n + c_{n-1}x^{n-1} + \cdots + c_0$, define the ***derivative*** of f, denoted f', by the expected formal procedure, namely

$$f' := nc_n x^{n-1} + (n-1)c_{n-1}x^{n-2} + \cdots + c_1.$$

The derivative satisfies the usual formal properties that are expected, e.g. $(fg)' = f'g + fg'$ and the chain rule. The reason we introduced derivatives is because of the very useful following lemma. First recall that, where $K \subseteq L$ is a field extension, an element $\alpha \in L$ is a ***multiple root*** of f if $f = (x - \alpha)^k h$ for some $k \geq 2$, $h \in K[x]$.

Lemma 1.49.

Let K be a field with $f \in K[x]$, $\alpha \in K$. α is a multiple root of f if and only if α is a root of both f and f'.

Proof. If α is a multiple root we have $f = (x - \alpha)^k h$ for some $k \geq 2$ and $h \in K[x]$, so $f(\alpha) = 0$ and $f' = k(x - \alpha)^{k-1}h + (x - \alpha)^k h'$, so $f'(\alpha) = 0^{k-1}h(\alpha) + 0^k h'(\alpha) = 0$.

Conversely, if $f(\alpha) = f(\alpha') = 0$ then $f(\alpha) = 0$ implies $f = (x - \alpha)g$ for some $g \in K[x]$. Then $f' = g + (x - \alpha)g'$, so $0 = f'(\alpha) = g(\alpha) + 0$, i.e. $g(\alpha) = 0$, so we can write $g(x) = (x - \alpha)h$, and hence $f = (x - \alpha)^2 h$. □

1.5.2 Separable Polynomials

Definition 1.50. For a field K, we say $f \in K[x]$ is ***separable*** if f has no multiple roots in any field extension $K \subseteq L$.

The following lemma helps us detect separability in polynomials.

Lemma 1.51.

If K is a field and $f \in K[x]$ then f is separable if and only if f and f' are relatively prime.

Proof. For the reverse implication, if f, f' are relatively prime then we can write $1 = rf + sf'$ for some $r, s \in K[x]$. Then for any field extension $K \subseteq L$ and any $\alpha \in L$ we cannot have that $f(\alpha) = f'(\alpha) = 0$ since then we would have $1 = r(\alpha)f(\alpha) + s(\alpha)f'(\alpha) = 0$, a contradiction, meaning α cannot be a multiple root.

For the forward implication, suppose f, f' are not relatively prime. Then there's an irreducible polynomial $\varphi \in K[x]$ that divides both f and f'. But if we consider a field extension $K \subseteq L$ with φ having a root $\alpha \in L$ (i.e. if we take $L = K[x]/(\varphi)$) then $\varphi(\alpha) = 0$, so since φ divides both f and f' we have $f(\alpha) = 0$ and $f'(\alpha) = 0$, so α is a multiple root of f. □

But is is possible to have an irreducible polynomial that is not separable?

Corollary 1.52.

If K is a field then an irreducible polynomial $f \in K[x]$ is separable if and only if $f' \neq 0$.

Proof. If $f' \neq 0$ then f, f' are relatively prime since any common factor $\varphi \in K[x]$ must be a factor of f and f'. But then φ is a factor of f' means $\deg(\varphi) \leq \deg(f') < \deg(f)$, which contradicts f is irreducible. □

Example 1.53 (nonseparable irreducible polynomial)**.** Consider $\mathbb{F}_p(t)$, the field of rational functions with coefficients in the characteristic p field $\mathbb{F}_p$. (Note this is an infinite field of characteristic p.) Define $f := x^p - t \in \mathbb{F}_p(t)[x]$. Then f is irreducible since there is no pth root of t in this field, but $f'(x) = px^{p-1} - 0 = 0$, so f is irreducible but not separable!

1.5.3 Separable Field Extensions

Definition 1.54 (separable element/separable field extension)**.** Let $K \subseteq L$ be a field extension and let $\alpha \in L$.

- We say that α is ***separable over K*** if α is algebraic over K and the minimal polynomial $f \in K[x]$ of α does not have a multiple root at α.

- We say that $K \subseteq L$ is a ***separable field extension*** if every element is separable.

Notice that α being separable is "better" than being algebraic. Moreover, just as being algebraic, we will not prove this, but the set of separable elements are closed under addition and multiplication and $\alpha \mapsto 1/\alpha$ (so the set of separable elements form a subfield, just as the algebraic elements do).

We will present a non-separable extension here and then never study separable extensions again since they can be a nightmare.

Example 1.55 (non-separable field extension)**.** As in the previous example consider the field $K = \mathbb{F}_p(t)$. Let $L := K[\sqrt[p]{t}] = K[x]/(x^p - t)$. Then L is an inseparable extension of K since the pth root of t has minimal polynomial that is not a separable polynomial as we showed in the example of a nonseparable polynomial.

1.5.4 Perfect Fields

The fields we will study are referred to as perfect fields, which avoid examples such as in the above.

Definition 1.56 (perfect field)**.** A field K is ***perfect*** if any algebraic field extension is separable over K.

Lemma 1.57.

A field K is perfect if and only if all irreducibles $f \in K[x]$ have $f' \neq 0$.

Proof. For the converse, note that if any $f \in K[x]$ has $f' \neq 0$ then f is separable. This applies to the minimal polynomials of all elements of an algebraic field extensions $K \subseteq L$, so L is a separable extension.

For the forward direction, if K is perfect then consider an irreducible polynomial $f \in K[x]$. We want to show $f' \neq 0$. Define $L = K[x]/(f)$. Then L is an algebraic extension and hence separable. Letting $\alpha \in L$ be the image of x we have that the minimal polynomial of α is f, and thus by separability we must have f is a separable polynomial. Thus the derivative $f' \neq 0$, as desired. □

Given the previous examples is not hard to see that $\mathbb{F}_p(t)$ is a non-perfect field. Luckily, most of the fields we care about are perfect, as is shown by the following lemma which shows that whenever the field characteristic is zero, $\deg(f')$ is exactly one less than $\deg(f)$.

Lemma 1.58.

If $\operatorname{char}(K) = 0$ then K is perfect.

Proof. If $f = c_n x^n + \cdots + c_0$ is irreducible with $c_n \neq 0$ then $f' = nc_n x^{n-1} + \cdots + c_1$, and $nc_n \neq 0$ since $\operatorname{char} \mathbb{F} = 0$. □

We will eventually use perfect fields to prove the primitive element theorem, which says that if $K \subseteq L$ is a finite separable field extension then it has a primitive element, i.e. there's some element α with $L = K[\alpha]$.

1.5.5 The Frobenius Homomorphism

Let K be a field of characteristic p. Recall the "freshman's dream" identity for fields of characteristic p: when $a, b \in K$, we have $(a+b)^p = a^p + b^p$. Indeed,

$$(a+b)^p = a^p + \binom{p}{1} a^{p-1}b^1 + \binom{p}{2} a^{p-2}b^2 + \cdots + \binom{p}{p-1} a^1 b^{p-1} + b^p,$$

where

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p(p-1)\cdots(p-k+1)}{k(k-1)\cdots(1)}.$$

But if $1 \leq k \leq p-1$, all the terms appearing except for p are $\leq p-1$, so they are not divisible by p. Hence, the p in each such term never cancels out, meaning all these terms are identically zero since K is a field of characteristic p. This is what makes characteristic p fields special and interesting. As a consequence of this, we can define a set map

$$\begin{aligned} F : K &\longrightarrow K, \\ a &\longmapsto a^p \end{aligned}$$

Then F is a ring homomorphism! Indeed, it is straightforward that

- $F(ab) = a^p b^p = F(a)F(b)$
- $F(a+b) = (a+b)^p = a^p b^p = F(a) + F(b)$ (shown above)
- $F(0) = 0^p = 0$
- $F(1) = 1^p = 1$

The ring homomorphism F is called the ***Frobenius*** homomorphism. The Frobenius holds the secrets of the characteristic p field. We will use this extensively in the next section, where we completely characterize perfect fields.

1.5.6 Characterization of Perfect Fields

Lemma 1.59.

If $\mathrm{char}(K) = p$ and $a \in K$ has no pth root then $f = x^p - a$ is irreducible in $K[x]$.

Proof. The hypothesis gives f has no roots (equivalently, that f has no linear factors), so it suffices to show f cannot have any higher degree factors.

Suppose g is an irreducible factor of $x^p - a$ and set

$$L = K[\sqrt[p]{a}] = K[x]/(g).$$

Let $b \in L$ be $\sqrt[p]{a}$. Then $f(b) = 0$. In fact, we have something even better: by Frobenius we have

$$(x - p)^p = x^p - b^p = x^p - a.$$

Thus all irreducible factors in L are just $(x - b)$. it follows that the only possible factors of f in $K[x]$ are $(x - b)^k$ with $1 \le k \le p$. Since $(x - b)^k = x^k - kbx^{k-1}$ plus lower order terms and $b \notin K$ and $k \in K$, it follows that we must have $kb = 0$ (if it werent zero then we could just divide by k and it would work out). Hence $k = p$. □

We now have enough to achieve our goal.

Theorem 1.60: Characterization of Perfect Fields.

A field K is perfect if and only if $\operatorname{char}(K) = 0$ or $\operatorname{char}(K) = p$ with all $a \in K$ having a pth root.

Proof. Suppose $a \in K$ has no pth root. Then $x^p - a$ is an irreducible in $K[x]$, so $K \subseteq K[\sqrt[p]{a}] = K[x](x^p - a)$ is a non-separable extension because, letting $b := \sqrt[p]{a}$, the minimal polynomial of b is $x^p - a = x^p - b^p = (x - b)^p$.

Conversely, if all $a \in K$ have a pth root then consider a polynomial $f \in K[x]$ with $f' = 0$. To show K is perfect, it suffices to show that $f(x)$ is *not* irreducible (since f is perfect if and only if no irreducible polynomial f has $f' = 0$).

Now, since $f' = 0$, all the exponents appearing in f must be multiples of p. So $f = a_n x^{pn} + a_{n-1}x^{p(n-1)} + \cdots + a_1 x^p + a_0$. Let b_i be a pth root of a_i. Then by Frobenius we have

$$\begin{aligned}(b_n x^n + \cdots + b_0)^p &= b_n^p x^{pn} + b_{n-1}^p x^{p(n-1)} + \cdots + b_0^p \\ &= a_n x^{pn} + \cdots + a_0 \\ &= f(x),\end{aligned}$$

contradicting f is irreducible. □

Corollary 1.61.

All finite fields are perfect.

Proof. We need to show all elements of K have a pth root. That is, we must show that the Frobenius ring homomorphism $F : K \to K$ by $F(a) = a^p$. F is a ring homomorphism with $\ker(F) = 0$, so F is injective. Since K is finite, F must be surjective. □

We now know that fields of characteristic zero and finite fields are all perfect fields. Since these are perfect fields, it is safe to say that, for our purposes, we can rule out the use of imperfect fields going forward.

§1.6 Classification of Finite Fields

Theorem 1.62.

If K is a field then a finite subgroup G of $K^\times$ is is cyclic.

In particular, $\mathbb{F}_p^\times = \mathbb{F}_p \setminus \{0\}$ is a finite cyclic group under multiplication.

Proof. Set $n := |G|$. For $d \mid n$, elements of $\{x \in G : x^d = 1\}$ are all roots of $x^d - 1$. So the set has $\leq d$ elements, so it suffices to prove the following lemma.

Lemma 1.63.

If $|G| = n$ and $\operatorname{card}(\{g \in G : g^d = 1\}) \leq d$ for $d \mid n$ then G is cyclic.

Proof. For $d \mid n$, let $G_d := \{g \in G : (\operatorname{ord}_G(g) =)|g| = d\}$. (Note that G_d is *not* a subgroup of G). For $y \in G_d$, there are d elements in the cyclic group $\langle y \rangle$ generated by y. Since we're given that $\operatorname{card}(\{g \in G : g^d = 1\}) \leq d$, we have that

$$\langle y \rangle = \{g \in G : g^4 = 4\},$$

meaning G_d is the set of generators for $\langle y \rangle$. Thus G_d is the set of generators for $\langle y \rangle \cong C_d$, the cyclic group of order d. This implies that $|G_d| = \phi(d)$, where ϕ is the Euler totient function, which we recall is the total number of m such that $1 \leq m \leq d$ with $\gcd(m, d) = 1$. We then know that either $G_d = \varnothing$ or $|G_d| = \phi(d)$. Note

$$\begin{aligned} n = |G| &= \textstyle\sum_{d|n} |G_d| \\ &\text{(by just arranging the set of elements of } G \text{ according to their order)} \\ &\leq \textstyle\sum_{d|n} \phi(d) \\ &= n, \end{aligned} \tag{$*$}$$

where we still need to prove $(*)$. Assuming $(*)$ for now, the above gives that the inequality on the second line must be equality, and hence all the G_d are nonempty. In particular, $G_d \neq \varnothing$ so G has an element of order n, which is the order of G itself, so G is cyclic.

It then only remains to prove $(*)$, that is, that $\sum_{d|n} \phi(d) = n$. To show this, we run the proof for $G = C_n$, the cyclic group of order n, but we now know that none of the G_d are empty, so in this group there exist elements of order d for all d dividing n. Thus $|G|_d = \phi(d)$ for all d, so $n = |G| = \sum_{d|n} |G_d| = \sum_{d|n} \phi(d)$. □

This completes the proof of the theorem. □

Let $\mathbb{F}$ be a finite field. Then $\operatorname{char}(\mathbb{F})$ must be some prime p, so $\mathbb{F}_p \subseteq \mathbb{F}$ is a finite extension. Our goal is to classify all such fields $\mathbb{F}$. $\mathbb{F}$ is a finite-dimensional vector space over $\mathbb{F}_p$, so $|\mathbb{F}| = |\mathbb{F}_p^n| = p^n$ for some $n \geq 1$. Before proving the main theorem we present some examples. The basic construction is to pick an irreducible polynomial $f \in \mathbb{F}_[x]$ and set $\mathbb{F} = \mathbb{F}_p[x]/(f)$. If $n = \deg(f)$ then $|\mathbb{F}| = p^n$ (WHY?). Although it is not obvious, we will eventually we're going to show that all finite fields are products of this construction.

Example 1.64 ($p = 2$)**.** Let $f = x^2 + x + 1 \in \mathbb{F}_2[x]$. f is irreducible since it has no root in $\mathbb{F}_2$ and is quadratic. Then let $\mathbb{F} := \mathbb{F}_2[x]/(f)$, where we identify x in this quotient with the element $\alpha \in \mathbb{F}$. Then $\mathbb{F} = \{x + y\alpha : x, y \in \mathbb{F}_2\}$. And $\alpha^2 = -\alpha - 1 = \alpha + 1$. This gives the multiplication rule $(x+y\alpha)(z+w\alpha) = xz+(xw+yz)\alpha+yw\alpha^2 = (xz+wy)+(xw+yz+yw)\alpha$. This is similar to multiplying elements of $\mathbb{Q}[i]$, where $i^2 = -1$.

Example 1.65 (p an odd prime)**.** Let p be an odd prime and $r \in \mathbb{F}_p$ an element that is not a square, e.g. in $\mathbb{F}_3$ we have $0^2 = 0$, $1^2 = 1$, $2^2 = 1$, so we can take $r = 2$. Then the polynomial $x^2 - r$ is irreducible in $\mathbb{F}_p[x]$. Then set

$$\mathbb{F} := \mathbb{F}_p[x]/(x^2 - r) = \mathbb{F}_p[\sqrt{r}]$$

So $\mathbb{F} = \{x + y\sqrt{r} : x, y \in \mathbb{F}_p\}$. We multiply using $(\sqrt{r})^2 = r$. At first glance this gives many fields of size p^2, but it turns out that they are all isomorphic, and it is a good exercise to show why. Note that we can also have $\mathbb{C} = \mathbb{R}[\sqrt{-1}] = \mathbb{R}[\sqrt{-2}]$, etc.

That was for degree 2. For degree 3 there are two irreducible cubics in $\mathbb{F}_2[x]$. One is $f(x) = x^3 + x + 1$ the other is $x^2 + x + 1$. If these were irreducible they would have linear factors but these have no roots in $\mathbb{F}_2$, so these are irreducible. This gives us two fields of size $2^3 = 8$, namely

$$\mathbb{F} = \mathbb{F}_2[x]/(f) \qquad \mathbb{F}' = \mathbb{F}_2[x]/(g),$$

where we understand α in $\mathbb{F}$ to be the image of x in $\mathbb{F}(?)$ and β to be the image of x in $\mathbb{F}$. Then $\alpha^3 = \alpha + 1$, $\beta^3 = \beta^2 + 1$, which allows multiplication in this field. It turns out that $\mathbb{F}_2[\alpha] \cong \mathbb{F}' = \mathbb{F}_2[\beta]$, and it is left as an exercise to the reader to verify this.

Theorem 1.66: Classification of Finite Fields.

There exists a unique field of order p^n for each prime p and $n \geq 1$.

Proof. Let p be a fixed prime, n a fixed number, $q := p^n$ Our goal is to construct such a field and show it is unique. We prove the theorem in a series of steps.

Lemma 1: If $\mathbb{F}$ is a field of size $q = p^n$ then for all $x \in \mathbb{F}$ we have $x^q = x$.

Proof. This clearly holds for $x = 0$, so consider nonzero x. $\mathbb{F}^\times = \mathbb{F} \smallsetminus \{0\}$ an abelian group of order $q - 1$. We proved last time that $\mathbb{F}^\times$ is cyclic of order $q - 1$. It follows that for $x \in \mathbb{F}^\times$ the order of x must divide $q-1$. Thus $x^{q-1} = 1$, meaning $x^q = x$. □

Lemma 2: Let $\mathbb{F}$ be a field of size q which is equal to p^n. Then the polynomial $x^q - x$ factors into a product of linear factors. Moreover,

$$x^q - x = \prod\nolimits_{\alpha\in\mathbb{F}}(x - \alpha). \qquad (*)$$

Proof. By the previous lemma we know that each $\alpha \in \mathbb{F}$ is a root of $x^q - x$, so $x - \alpha$ is a factor for all $a \in \mathbb{F}$. Since q choices of α, we see that $(*)$ must hold. □

Lemma 3: Let $\mathbb{F}_p \subseteq \mathbb{L}$ be a field extension such that $x^q - x$ splits in $\mathbb{L}[x]$ as a product of linear factors. Set

$$\mathbb{F} := \{\alpha \in \mathbb{L} \text{ such that } \alpha^q - \alpha = 0\}.$$

Then $\mathbb{F}$ is a subfield of $\mathbb{L}$ with $|\mathbb{F}| = q$.

Proof. We have to show that $\mathbb{F}$, the set of all roots, is closed under addition, multiplication, multiplication by -1, and inversion ($\alpha \mapsto 1/\alpha$). The first three shows it is a ring and the final one shows it is a field.

- *Addition*: Assume $\alpha^q - \alpha = 0$ and $\beta^q - \beta = 0$. Then $(\alpha+\beta)^q = ((\alpha+\beta)^p)^{p^{n-1}}$, which by Frobenius is $(\alpha+\beta)^{p^{n-1}}$. Continuing this process inductively, we conclude $\alpha + b$. This shows addition.
- *Multiplication*: If $\alpha^q - \alpha = 0$ and $\beta^q - \beta = 0$, then $(\alpha\beta)^1 = \alpha^q\beta^q = \alpha\beta$. For multiplication by -1, we must check that -1 is a root of $x^q - x$:
  - If $p = 2$ then $-1 = 1$ and $q^1 = 1$, so we're good.
  - If p is odd then q is odd and so $(-1)^q = -1$.
- *Inversion*: If $\alpha^q = \alpha$ and $\alpha \neq 0$ then $(1/\alpha)^q = 1/\alpha^q = 1/\alpha$.

Thus $\mathbb{F}$ is a field. □

Lemma 4 (Uniqueness): Let $\mathbb{F}$ and $\mathbb{F}'$ be fields with $|\mathbb{F}| = |\mathbb{F}'| = q$. Then $\mathbb{F} \cong \mathbb{F}'$.

Proof. Last class we showed that $\mathbb{F}^\times$ is isomorphic to the cyclic group of order $q-1$. Let $\alpha \in \mathbb{F}^\times$ be a generator. Then every element of $\mathbb{F}^\times$ is of the form α^k for some k. Generators of this type are called ***primitives***. This implies that $\mathbb{F} = \mathbb{F}_p[\alpha]$. Let $f \in \mathbb{F}_p[x]$ be the minimal polynomial of α. α is an algebraic element since α is a root of $x^q - x$, so this is a finite extension. This implies

$$\mathbb{F} \cong \mathbb{F}_p[x]/(f).$$

Also we know that in our other field $\mathbb{F}'$ we have the polynomial $x^q - x$ has q roots. In particular, f has a root $\beta \in \mathbb{F}'$ (so f is the minimal polynomial of β). This implies $\mathbb{F}_p[\beta] \subseteq \mathbb{F}'$. But $\mathbb{F}_p[x]/(f) \cong \mathbb{F}_p[\beta] \subseteq \mathbb{F}'$. Since $\langle \mathbb{F}_p[x]/(f) \rangle = q = |\mathbb{F}'|$, we in fact have that the subset must be an equality, meaning

$$\mathbb{F}' \cong \mathbb{F}_p[x]/(f) \cong \mathbb{F},$$

giving the result. □

This completes the proof of the classification theorem for finite fields. □

As a consequence of the main theorem and its proof we have two things summarized in the following corollary which follows immediately from the above proof.

Corollary 1.67.

We have the following two points.

- All finite fields come from the construction presented at the beginning of the section.
- For all $n \geq 1$ there exists an irreducible $f \in \mathbb{F}_p[x]$ with $\deg(f) = n$.

§1.7 Proof of the Primitive Element Theorem

Example 1.68. Consider the field extension $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{2}, \sqrt{3}]$. We proved before that $\sqrt{2} + \sqrt{3}$ is a primitive element of this field with the following procedure.

- Finding the minimal polynomial f for $\sqrt{2} + \sqrt{3}$ by looking at powers $(\sqrt{2} + \sqrt{3})^n$.
- We noticed that $\deg(f) = 4$, so $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{2} + \sqrt{3}]$ is a degree 4 extension, so since $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ also is a degree 4 extension, it must be that $\mathbb{Q}[\sqrt{2}+\sqrt{3}] = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$.

Theorem 1.69: Primitive Element Theorem.

If $K \subseteq L$ is a separable field extension of finite degree then there exists some $\gamma \in L$ such that

$$L = K[\gamma].$$

We call any such element γ a ***primitive element***.

Proof. The proof in the case the field is finite is different than the proof in the case the field is infinite. In fact, we've already proven the finite case—although we didn't make this explicit. We do this now:

Case 1: K is a finite field. Then $K \subseteq L$ is a finite extension, so L is finite (WHY?), say $|L| = n$, where n is a power of $p = \text{char}(K)$. We know that $L^\times = L \smallsetminus \{0\}$ is a group under multiplication. Then $L^\times$ is a cyclic group as we've proven in the section on fields and groups. Let $\gamma \in L^\times$ be a generator for this cyclic group, that is, a ***primitive element*** of this cyclic group. Thus $K[\gamma]$ contains γ^n for all $n \geq 1$, so it contains all nonzero elements of L. Hence $K[\gamma] = L$. (Note we never used separability but we've already proven that every element of n is a pth root.)

Case 2: K is an infinite field. First consider a finite separable extension $K \subseteq L$, so we can write $L = K[\alpha_1, \ldots, \alpha_n]$.

We'll prove by induction on n. Of course the base case $n = 1$ gives that $K = K[\alpha_1]$, so $\gamma := \alpha_1$ is a primitive element. For the induction step, assume $N \geq 2$ and that the theorem holds for fewer elements. By the induction hypothesis we can write

$$K[\alpha_1, \ldots, \alpha_{n-1}] = K[\alpha].$$

(Where α is the primitive element for $K[\alpha_1, \dots, \alpha_{n-1}]$ given by the induction hypothesis.) Let $\beta := \alpha_n$, so that $K[\alpha_1, \dots, \alpha_n] = K[\alpha, \beta]$. We'll prove that for all but finitely many choices of *nonzero* $c \in L$, $\gamma := \alpha + c\beta$ is a primitive element for $K[\alpha_1, \dots, \alpha_n]$. Then we use that K is infinite to conclude there must exist a $c \in L$ for which γ as defined is a primitive element.

Let $f, g \in K[x]$ be the minimal polynomials of α, β. Now let a different field $\mathbb{L}$ be a splitting field for the product fg. f and g split into linear factors in $\mathbb{L}[x]$. Let $\alpha = \alpha_1, \dots, \alpha_h$ and $\beta = \beta_1, \dots, \beta_k$ be the roots of f and g in $\mathbb{L}$. Define

$$h(x) := f(\gamma - cx) \in (K[\gamma])[x]$$

Now we attempt to answer the question which asks what the common roots of h and g are. There is an obvious one—$h(\beta) = f(\gamma - c\beta)$, but $\gamma = \alpha + c\beta$ means that $\alpha = \alpha + c\beta - c\beta = \gamma - c\beta$ so that $h(\beta) = f(\gamma - c\beta) = f(\alpha)$. We will prove that if we exclude finitely many bad choices of c then β is the only common root. This will then imply that γ is a primitive element because f and g split in $\mathbb{L}[x]$ into *linear* factors. So $h(x) = f(\gamma - cx)$ also splits into linear factors, and thus in $\mathbb{L}[x]$ we can compute the gcd, namely

$$\gcd(h, g) = \prod\nolimits_{\substack{\text{common} \\ \text{roots } \lambda}} (x - \lambda) = x - \beta.$$

We are using here that g has no repeated roots because our extension is given to be separable. $h, g \in (K[\gamma])[x]$; we have proven that we can compute the gcd by repeatedly using the Euclidean algorithm, and moreover we can do this in either the extension field or the smaller field. We will use the smaller field $K[\gamma]$. So we have

$$x - \beta \in (K[\gamma])[x] \implies \beta \in K[\gamma] \implies \alpha = \gamma - c\beta \in K[\gamma] \implies K[\gamma] = K[\alpha, \beta].$$

So, what do we need from c for β to be the only common root of g and $h(x) = g(\gamma - cx)$? Well, we know that $\alpha = \alpha_1, \dots, \alpha_h$ are the roots of f and $\beta = \beta_1, \dots, \beta_k$ are the roots of g. We now study the roots of h: We need that $\gamma - cx = \alpha_i$. We have that $\alpha_1 + c\beta_1 - cx = \alpha_i$, i.e. that $x = \frac{1}{c}(\alpha_1 + c\beta_1) - \alpha_i)$. Hence we need for all choices of i and j with $j \geq 2$ that

$$\frac{1}{c}(\alpha_1 + c\beta_1 - \alpha_i) \neq \beta_j.$$

Rearranging, this is equivalent to needing for each i and j with $j \geq 2$, we exclude one value of c (since this is a linear equation and hence has one solution), namely $c = \frac{\alpha_i - \alpha_1}{\beta_1 - \beta_j}$ (since $\alpha_1 + c\beta_1 - \alpha_i = c\beta_j$ implies $c(\beta_1 - \beta_j) = \alpha$).

Hence, since $\beta_j \neq \beta_1$ for $j \geq 2$, we're done since this excludes only finitely many.

This completes the proof of the primitive element theorem. □

§1.8 Algebraically Closed Fields

Definition 1.70 (algebraically closed field)**.** A field K is ***algebraically closed*** if for all nonconstant $f \in K[x]$ there's some $a \in K$ with $f(a) = 0$.

Equivalently, for all monic $f \in K[x]$, we can write $f(x) = (x - a_1) \cdots (x - a_n)$ for some $a_1, \ldots, a_n \in K$.

Theorem 1.71: Fundamental Theorem of Algebra.

$\mathbb{C}$ is algebraically closed.

Equivalently, if $\mathbb{R} \subseteq K$ is a finite field extension then $[K : \mathbb{R}] = 1$ or 2.

If $[K : \mathbb{R}] = 2$ then letting $\alpha \in K$ be a primitive element (so $K = \mathbb{R}[\alpha]$), which always exists by the primitive element theorem (since $\operatorname{char} \mathbb{R} = 0$ and hence $\mathbb{R}$ is perfect). Then the minimal polynomial f of α has degree 2, i.e. $f = x^2 + bx + c$ and $\alpha = \frac{1}{2}\left(-b \pm \sqrt{b^2 - 4c}\right)$ implies $K = \mathbb{R}[\alpha] = \mathbb{R}[\sqrt{b^2 - rc}] \cong \mathbb{C}$, where $b^2 - 4c < 0$ since f has no roots in $\mathbb{R}$.

The easy step in the proof:

Theorem 1.72.

$\mathbb{R}$ has no odd degree extensions (other than 1)

Proof. If $[K : \mathbb{R}] = n$ is odd then we'll show $n = 1$. Let $\alpha \in K$ be primitive for the extension. Then $K = \mathbb{R}[\alpha]$, and if f is the minimal polynomial for α then $\deg(f)$ is odd. f is irreducible over $\mathbb{R}$, so it has no real roots. But since f is an odd degree polynomial we have $f \to \infty$ as $x \to \infty$ and $f \to -\infty$ as $f \to -\infty$. Then the intermediate value theorem says x has a root, contradicting f is irreducible. Hence f must be of even degree. □

To rule out even extensions, we need Galois theory (and the Sylow theorems).

Definition 1.73. Let K be a field. An extension $K \subseteq L$ is an ***algebraic closure*** if L is algebraic over K (equivalently, every element of L has a minimal polynomial) and L is algebraically closed over K.

Example 1.74. Some examples.

- Assuming the fundamental theorem of algebra, $\mathbb{C}$ is an algebraic closure of $\mathbb{R}$.
- $\mathbb{C}$ is *not* an algebraic closure of $\mathbb{Q}$ since $\mathbb{C}$ is not an algebraic extension of $\mathbb{Q}$ (e.g. there are elements in $\mathbb{C}$ such as π which are transcendental over $\mathbb{Q}$, i.e. not algebraic over $\mathbb{Q}$).

  Let $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} : \alpha \text{ is algebraic over } \mathbb{Q}\}$. This is a field (since $\overline{\mathbb{Q}}$ is exactly the algebraic numbers, which we have shown is a field). Hence the field extension $\mathbb{Q} \subseteq \overline{\mathbb{Q}}$ is an algebraic closure.

Theorem 1.75: Steinitz.

For a field K there exists an algebraic closure $K \subseteq L$, and if $K \subseteq L$, and $K \subseteq L_2$ are both algebraic closures, there exists isomorphisms $\varphi : L_1 \to L_2$ such that $\varphi|K = \mathrm{id}_K$.

Proof. We first prove existence and then uniqueness up to isomorphism.

Proof of Existence: Let $\mathscr{P}$ be the set of all monic polynomials over K. Let $\{t_f\}_{f\in\mathscr{P}}$ be the set of formal symbols (that is, the set of "variables," each one corresponding to a unique polynomial $p \in \mathscr{P}$). Then define

$$R := K\Big[\bigcup\nolimits_{f\in\mathscr{P}} t_f\Big]$$

(so R is the ideal generated by the variables t_f for each $f \in \mathscr{P}$). Then R is a (huge) polynomial ring in infinitely many variables. Let I be the ideal of R generated by $f(t_f)$ for all monic $f \in K[x]$. (For instance, if $K = \mathbb{Q}$ then I contains the elements like $(t_{x^2+1})^2 + 1$, and elements like $(t_{x^3-x+2})^3 - t_{x^3-x+2} + 2$.)

We now show that I is a proper ideal of R. Indeed, suppose otherwise, i.e. that we can write

$$1 = a_1 f_1(t_{f_1}) + \cdots + a_n f_n(t_{f_n}) \tag{$\dagger$}$$

for some $a_1, \ldots, a_n \in R$ and monic polynomials $f_1, \ldots, f_n \in K[x]$. Pick an algebraic extension $K \subseteq L$ such that there are $\lambda_1, \ldots, \lambda_n \in L$ with $f_i(\lambda_i) = 0$ for $1 \le i \le n$. Define a ring homomorphism $\varphi : R \to L$ which satisfies

- $\varphi|K$ is the inclusion map $K \hookrightarrow L$,
- $\varphi(t_{f_i}) = \lambda_i$ for $1 \le i \le n$, and
- $\varphi(t_g) = 0$ for all $g \in \mathscr{P}$ that are *not* one of the $f_1, \ldots, f_n$.

Then using ($\dagger$), we have

$$\begin{aligned} 1 = \varphi(1) &= \varphi(a_1)\varphi(f_1(t_{f_1})) + \cdots + \varphi(a_n)\varphi(f_n(t_{f_n})) \\ &= \varphi(a_1)f_1(\varphi(t_{f_1})) + \cdots + \varphi(a_n)f_n(\varphi(t_{f_n})) \\ &= \varphi(a_1)f_1(\lambda_1) + \cdots + \varphi(a_n)f_n(\lambda_n) \\ &= 0, \end{aligned}$$

contradicting the fact that $1 \neq 0$. Hence I is a proper ideal as claimed.

Recall that if I is a proper ideal of R then it is contained inside some maximal ideal $\mathfrak{m} \subseteq R$ by Zorn's lemma. Let $F := R/\mathfrak{m}$, which is a field since $\mathfrak{m}$ is a maximal ideal of R. We now know that $K \subseteq F$ is a field extension and that for all monic polynomials $f \in K[x]$ there's an $a \in F$ with $f(a) = 0$, namely a is the canonical image of $t_f \in R$ in F. The reason is that we can choose I to be an ideal in R generated by $f(t_f)$ for all monic $f \in K[x]$ such that $f(t_p)$ goes to 0 in R/I.

We now want to show that F is in fact algebraically closed. It seems like it, but F may not be algebraically closed since as of now we can only talk about polynomials

over K, and hence so too in $F = R/\mathfrak{m}$.
But this doesn't guarantee F is algebraically closed (WHY?). Thus we will iterate this construction to get a sequence of field extensions $K = K_1 \subseteq K_2 \subseteq K_3 \subseteq \cdots$ such that for all monic $f \in K_n[x]$ there exists $a \in K_{n+1}$ with $f(a) = 0$.
Define

$$\mathbb{F} := \bigcup\nolimits_{n=1}^{\infty} K_n.$$

Then $\mathbb{F}$ is a field and $K \subseteq \mathbb{F}$ is a field extension. We claim $\mathbb{F}$ is algebraically closed. Indeed, any monic $f \in \mathbb{F}[x]$ lives in some $K_n[x]$,, so we can find some $a \in K_{n+1} \subseteq \mathbb{F}$ with $f(a) = 0$.
But F might be a transcendental extension (that is, it may contain transcendental elements over K). Thus

$$\overline{K} = \{a \in \mathbb{F} : a \text{ is algebraic over } K\}.$$

Proof of Uniqueness: We first prove an auxiliary lemma.

Lemma 1.76.

If $K \subseteq \overline{K}$ is an algebraic closure and $K \subseteq L$ is an algebraic extension then there is some field homomorphism $\varphi : L \to \overline{K}$ such that $\varphi|K = \mathrm{id}_K$ (so $\ker\varphi$ is a proper ideal of L), so $\ker\varphi = 0$ and φ is injective.

Proof. We will again use Zorn's lemma. Define

$$\mathscr{P} = \left\{(F, \psi) : \substack{K \subseteq F \subseteq L \text{ are field extensions and } \psi : F \to \overline{K} \\ \text{is a field homomorphism with } \psi|K = \mathrm{id}_K}\right\}.$$

Note that $\mathscr{P}$ is a partially ordered set with order $(F_1, \psi_1) \leq (F_2, \psi_2)$ iff $F_1 \subseteq F_2$ and $\psi_2|F_1 = \psi_1$. We will show that $\mathscr{P}$ contains (L, φ) for some φ.
Observe that if $C \subseteq \mathscr{P}$ is a linearly ordered chain then C has an upper bound, namely $F = \bigcup_{(F_i,\psi_i)\in C} F_i$ and $\psi : F \to \overline{K}$ is given by $\psi|F_i = \psi_i$ for each $(F_i, \psi_i) \in C$.
Note that $\mathscr{P}$ is not the empty set because (K, the inclusion map $K \hookrightarrow \overline{K}$) $\subseteq \mathscr{P}$.[1]
Then by Zorn's lemma $\mathscr{P}$ has a maximal element, call it (F, ψ).
We now claim $F = L$. To show this, suppose that instead $F \neq L$. Then $K \subseteq F \subsetneq L$. Pick $\alpha \in L$ such that $\alpha \notin F$. Let $g \in F[x]$ be the minimal polynomial of α. Thus $\psi(g) \in \overline{K}[x]$ splits completely, say as $\psi(g) = (x-\lambda_1)\cdots(x-\lambda_n)$ with $\lambda_1, \ldots, \lambda_n \in \overline{K}$.
Define

$$F' := F[x]/(g),$$
$$\psi^1 : F^1 \to \overline{K}, \psi^1|F = \psi, \psi^1(\alpha) = \lambda_1.$$

[1] We need to show $\mathscr{P}$ if we wish to apply Zorn's lemma since the empty set is a partially ordered set that does not have a maximal element since it doesn't have any elements at all.

Since $\psi^1(\alpha)$ is a root of $\psi(g)$, this makes sense. Then $(F\psi) \underset{x}{<} (F^1, \psi^1)$, contradicting maximality. □

The previous lemma then has as a consequence the following corollary:

Corollary 1.77.

If K is a field and both $\overline{K} \subseteq \overline{K}_1$ and $\overline{K} \subseteq \overline{K}_2$ are both algebraic closures of K, then there exists a field isomorphism $\varphi : \overline{K}_1 \to \overline{K}_2$ with $\psi|_K = \mathrm{id}_K$.

Proof. By the lemma, there exists a field homomorphism $\varphi : \overline{K}_1 \to \overline{K}_2$ with $\varphi|K = \mathrm{id}_K$. φ is necessarily injective, and $\varphi(\overline{K}_1) \subseteq \overline{K}_2$ is an algebraic extension. Since $\overline{K}_1 \cong \varphi(\overline{K}_1)$ is algebraically closed, must have $\varphi(\overline{K}_1) = \overline{K}_2$, i.e. φ is surjective. □

§2 Galois Theory

§2.1 The Cubic Formula

We now tone back the abstractness and revisit something more familiar to us.

Lemma 2.1.

If $f := x^n + c_{n-1}x^{n-1} + \cdots + c_0 \in K[x]$ splits as $(x - \lambda_1) \cdots (x - \lambda_n)$ then

$$c_{n-1} = -(\lambda_1 + \cdots + \lambda_n).$$

Proof. Just expand out $(x - \lambda_1) \cdots (x - \lambda_n)$. □

Corollary 2.2.

If $f := x^n + c_{n-1}x^{n-1} + \cdots + c_0$ and $f(x - d) = x^n + c'_{n-1}x^{n-1} + \cdots + c'_0$ then

$$c'_{n-1} = c_{n-1} - nd.$$

Proof. Extend the field such that f splits completely, say as $(x - \lambda_1) \cdots (x - \lambda_n)$. Then $f(x - d) = (x - (d + \lambda_1)) \cdots (x - (d + \lambda_n))$, and then apply the lemma above. □

A consequence is that given a polynomial $f \in K[x]$ where K is a field of characteristic zero, we can always do a linear change of variables, namely $f \mapsto f(x - c_{n-1}/n)$, such that

$$f = x^n + c_{n-2}x^{n-2} + \cdots + c_0,$$

where in particular f has no term of order $n - 1$. If we apply this reasoning to a quadratic then we reduce to solving something of the form $x^2 + c_0 = 0$, which gives $x = \pm\sqrt{c_0}$, and re-substituting back in the original x before changing variables gives us the quadratic formula). So in a sense, the above consequence is a higher order version/generalization of completing the square.

2.1.1 Solving the cubic

Our next goal is to solve a cubic equation, which we now see reduces to solving equations of the form

$$x^3 + bx + c = 0.$$

To solve, let us substitute $x = y + z$ and try to separate into single variable equations of y and z. We get

$$0 = (y+z)^3 + b(y+z) + c = y^3 + 3y^2z + 3yz^2 + z^3 + by + bz + c = 0,$$

so

$$(y^3 + z^3 + c) + (3yz + b)(y + z) = 0.$$

It is enough for both $y^3 + z^3 + c = 0$ and $3yz + b = 0$. Then $y^3 + z^3 = -c$ and $yz = -b/3$.

Cubing the latter gives $y^3z^3 = -b^3/27$, so we know what both the sum and the product of $y^3 + z^3$. Making the substitution $s = y^3$, $t = z^3$, we have

$$\begin{bmatrix} s + t = -c \\ st = -b^3/27 \end{bmatrix}.$$

We then know s and t are the roots of some quadratic equation, namely of the quadratic (in variable w given by $(w+s)(w-t) = w^2 - (s+t)w + st = 0$. Using the system gives

$$w^2 + cw - b^3/27 = 0,$$

which of course gives two roots; $y^3 = s$ and $z^3 = t$ means y and z are cube roots of s and t, respectively. But each has three cube roots, giving nine possible choices, but there are only supposed to be three solutions! This is resolved by the fact that we only take solutions with $yz = -b/3$ rather than $y^3z^3 = -b^3/27$ since we cubed the former to get the latter.

2.1.2 Quartic Equation

There is a quartic equation (similar, but more complicated), though it is most easily understood using algebraic geometry.

§2.2 The First Triumph of Galois Theory

There does *not* exist a similar solution to polynomials of degree ≥ 5. This was first proven by Abel and Ruffini without explicitly using Galois theory, and soon after Galois developed his theory to put the methods of their proof into a broader context. We now develop this theory.

Definition 2.3. A field extension $K \subseteq L$ is called ***solvable*** if it can be factored into a sequence of extensions

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n = L$$

such that $K_{i+1} = K_i\big[\sqrt[r_i]{d_i}\big]$, where $r_i \geq 2$ and $d_i \in K_i$ does not have an r_ith root in K_i. (More precisely, $K_1 = K_i[x]/(x^{r_i} - d_i)$.

Example 2.4. Some examples.

- $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{2}]$
- $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{2}] \subseteq \mathbb{Q}[\sqrt[3]{\sqrt{2}+7}]$

By the quadratic equation, the roots of $x^2 + bx + c$ sit inside either $\mathbb{Q}$ or $\mathbb{Q}[\sqrt{b^2 - 4c}]$ depending on whether $b^2 - 4c$ is a square in $\mathbb{Q}$ or not. Then the roots of a quadratic equation lie in a solvable extension, either in the trivial extension of a quadratic extension. What about a cubic extension? By our solution to the cubic equation $x^3 + ax^2 + bx + c = 0$, we solved by

- Step 1: Making a linear change of variables
- Step 2: Solving a quadratic equation
- Step 3: Taking two cube roots (of y and z)

Hence, in the worst case, the solutions sit inside a field extension

$$\mathbb{Q} \overset{\text{linear change}}{=} \mathbb{Q} \overset{\text{quadratic equation}}{\subseteq} \mathbb{Q}[\sqrt{?}] \overset{\text{taking cube roots}}{\subseteq} \mathbb{Q}[\sqrt{?}, \sqrt[3]{??}, \sqrt[3]{???}].$$

Thus the roots of a cubic equation sit inside a solvable extension.

The same is true for the roots of a quartic equation. But we have the following, which we will be able to prove after developing Galois theory.

Theorem 2.5: Galois.

For all $n \geq 5$ there exist degree n polynomials $f \in \mathbb{Q}[x]$ whose roots do not sit in a solvable extension of $\mathbb{Q}$.

This is one of the triumphs of nineteenth-century mathematics and was the impetus for the development of abstract algebra (e.g. groups, etc.). In fact, similar treatment will show the following:

Theorem 2.6.

$\mathbb{R}$ has no degree $n \geq 3$ extensions. In particular, we show the fundamental theorem of algebra.

How would you prove such theorems?

Definition 2.7. Given a finite field extension $K \subseteq L$, the ***Galois group*** of the extension, $\operatorname{Gal}(L/K)$, is the set of automorphisms

$$\operatorname{Gal}(L/K) := \{\varphi : L \to L : \varphi \text{ is a field automorphism and } \varphi|K = \mathrm{id}_K\}.$$

Example 2.8. For instance, consider the following examples:

- $\operatorname{Gal}(\mathbb{C}/\mathbb{R}) \cong C_2$, where the generator is the complex conjugation map $\varphi(a+bi) = a-bi$.
- $\operatorname{Gal}(\mathbb{Q}[\sqrt{d}])/\mathbb{Q}) \cong C_2$ for d not a square, where the generator is the map $\varphi(a+b\sqrt{d}) = a - b\sqrt{d}$.

We will soon prove that $\operatorname{Gal}(L/K)$ is *always* a finite group, and for sufficiently interesting field extensions $K \subseteq L$, which we will call ***Galois extensions***, there is a bijection between ***intermediate fields*** F—that is, $K \subseteq F \subseteq L$—and subgroups of $\operatorname{Gal}(L/K)$. This is significant since it reduces questions about field extensions to questions about group theory.

2.2.1 Symmetric Polynomials

A ***symmetric polynomial*** in n variables over a field K is a polynomial $f \in K[x_1, \dots, x_n]$ such that the value of f is unchanged by permuting variables. More precisely, letting S_n be the symmetric group on n generators (so $S_n = \left\{\sigma : \{1, \dots, n\} \overset{\cong}{\to} \{1, \dots, n\}\right\}$) we require $f(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = f(x_1, \dots, x_n)$ for all $\sigma \in S_n$.

Example 2.9. We give some examples of symmetric polynomials:

- $x_1 + \cdots + x_n$ (symmetric in n variables)
- $x_1^m + \cdots + x_n^m$ (symmetric in n variables)
- $x_1x_2 + x_1x_3 + x_2x_3$ (symmetric in 3 variables)

We now demonstrate a process to construct several symmetric polynomials. Given any $g \in K[x_1, \dots, x_n]$, define the ***symmetrization*** of g to be

$$f(x_1, \dots, x_n) := \sum\nolimits_{\sigma \in S_n} g(x_{\sigma(1)}, \dots, x_{\sigma(n)}).$$

Example 2.10. The symmetric polynomial $x_1^m + \cdots + x_n^m$ from the previous example is *almost* the symmetrization of $g := x_1^m$, but the symmetrization of x_1^m is $(n-1)!(x_1^m + \cdots + x_n^m)$.

For instance, in 3 variables we have

$$S_3 = \{\mathrm{id}, (12), (13), (23), (123), (132)\}.$$

Symmetrizing $x_1^4 \in K[x_1, \dots, x_n]$ gives

$$x_1^4 + x_{(12).1}^4 + x_{(13).1}^4 + x_{(23).1}^4 + x_{(123).1}^4 + x_{(132).1}^4 = x_1^4 + x_2^4 + \\ x_3^4 + x_1^4 + x_2^4 + x_3^4 = 2(x_1^4 + x_2^4 + x_3)^4.$$

2.2.2 Elementary Symmetric Polynomials

What are all the symmetric polynomials? To answer this question we first notice that the symmetric polynomials over K, denoted $K[x_1, \dots, x_n]^{S_n}$, a subset of $K[x_1, \dots, x_n]$, is a ring. The goal theorem is to show that there exist symmetric polynomials $s_1, \dots, s_n$ such that $K[x_1, \dots, x_n]^{S_n} \cong K[s_1, \dots, s_n]$, where s_i are themselves symmetric polynomials. We can see this concretely with the following example:

Example 2.11 (1 variable)**.** $K[x_1]^{S_1} = K[x_1]$, so we see that here $s_1 = x_1$.

Example 2.12 (2 variables)**.** $K[x_1, x_2]^{S_2} = K[x_1 + x_2, x_1x_2]$ (we will prove this soon).

Definition 2.13. The ***elementary symmetric polynomials*** in n variables are

$$s_k = \sum\nolimits_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} x_{i_1} x_{i_2} \cdots x_{i_n}.$$

For instance, $s_1 = x_1 + \cdots + x_n$ and $s_2 = \sum_{1 \leq i < j \leq n}^{n} x_i$.

Example 2.14 (3 variables)**.** We have then that $s_1 = x_1 + x_2 + x_3$, $s_n = x_1x_2 + x_1x_3 + x_2x_3$, $s_3 = x_1x_2x_3$.

Why are we doing this? Well, the answer to that depends on the following fundamental observation: Consider $a_1, \dots, a_n \in K$ and write

$$(z - a_1) \cdots (z - a_n) = z^n + c_{n-1}z^{n-1} + \cdots + c_0.$$

Then $c_{n-1} = -s_1(a_1, \dots, a_n) = -(a_1 + \cdots + a_n)$. $c_{n-2} = s_2(a_1, \dots, a_n) = a_1a_2 + a_1a_3 + \cdots$, $\dots$, $c_{n-k} = (-1)^k s_k(a_1, \dots, a_n)$, $\dots$, $c_0 = (-1)^n s_n(a_1, \dots, a_n) = (-1)^n a_1 \cdots a_n$. Rephrasing this observation, this gives us another way to define the elementary symmetric polynomials.

Remark 2.15 (important observation)**.** A polynomial is a function of its roots over a field containing them. More precisely, if we regard a polynomial as a function of its roots then *the coefficients are the elementary symmetric functions*, up to sign.

Theorem 2.16: Gauss.

The elementary symmetric polynomials form a basis for the symmetric polynomials.

Proof. We prove the theorem by induction on the number of variables. The base case $n = 1$ is $K[x_1] = K[s_1]$, where $s_1 = x_1$ is symmetric in one variable (since all polynomials of one variable are symmetric).

For the induction step, we assume the claim holds for $n - 1$ variables and seek to prove the claim for n variables. We do this by induction on the degree of the polynomial (so induction within an induction). The base case is degree 0, in which case there is nothing to prove (since the polynomial is just a constant and hence are symmetric). For the induction step, we assume the case of degree $m - 1$ holds and we desire to prove the case of degree m. Consider a degree m symmetric polynomial $f \in K[x_1, \dots, x_n]$. Define $f_0 = f(x_0, \dots, x_{n-1}, 0) \in K[x_1, \dots, x_{n-1}]$. Letting $s_{k,0} := s_k(x_1, \dots, x_{n-1}, 0)$, we note that $s_{k,0}$ is the kth elementary symmetric polynomial in $n-1$ variables (for instance, $n = 3$ and $k = 2$ gives $s_2 = x_1x_2 + x_1x_3 + x_2x_3$, $s_{2,0} = s_2(x_1, x_2, 0) = x_1x_2$). Invoking the induction hypothesis, there exists a $g \in K[x_1, \dots, x_{n-1}]$ such that $f_0 = g(s_{1,0}, \dots, s_{n-1,0})$. We can regard g as an element of $K[x_1, \dots, x_n]$ that doesn't involve x_n. Our first guess is that $f = g(s_1, \dots, s_n)$, which of course is not true, but we note that if we set $h := f - g(s_1, \dots, s_n)$ then h is a symmetric polynomial and $h(x_1, \dots, x_{n-1}, 0) = f_0(x_1, \dots, x_{n-1}) - g(s1, 0, \dots, s_{n-1,0}) = 0$. By symmetry, $h(x_1, \dots, x_n)$ is 0 wherever you set any of the x_k to 0. This implies that you get 0 when you plug in $x_k = 0$, which implies $h = x_k q$ for some q. Thus $h = x_1 \cdots x_n \varphi(x_1, \dots, x_n) = s_n \varphi(x_1, \dots, x_n)$. φ is then a symmetric polynomial of degree at most $m - n$ since $\deg h \leq \deg(f) = m$. Applying our induction hypothesis we get that we can write $h = g_1(s_1, \dots, s_n)$ for some $g_1 \in K[x_1, \dots, x_n]$. This implies $f = g(s_1, \dots, s_n) + h = g(s_1, \dots, s_n) + g_1(s_1, \dots, s_n)$, as desired. This completes the proof up to uniqueness.

But if we trace through each step of the proof, each choice we could make was unique, so the result $g + g_1$ is unique. This completes the proof of the theorem. □

Example 2.17. Consider $x_1^2 + \cdots + x_n^2 = (x_1 + \cdots + x_n)^2 - 2(x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n) = s_1^2 - 2s_2$.

Example 2.18. We want to write $f := x_1x_2^2 + x_1x_3^2 + x_2x_1^2 + x_2x_3^2 + x_3x_1^2 + x_3x_2^2$ as a polynomial of the elementary symmetric polynomials.

First guess: We have $s_1s_2 = (x_1 + x_2 + x_3)(x_1x_2 + x_1x_3 + x_2x_3)$. This has all the terms of f, along with some extra terms. For instance, we don't want the product of x_1 (from the left parenthesized term) and x_2x_3 (from the right parenthesized term). There are three terms of this form, namely x_i from the first parenthesized term and x_jx_k from the second parenthesized term. We then get $f = s_1s_2 - 3s_3$.

We now make an important observation. If we expand out the polynomial $(z - a_1) \cdots (z - a_n) \in K[z]$. The coefficients are symmetric polynomials in the a_i since if we expand this out we get $z^n + c_1z^{n-1} + c_2z^{n-2} + \cdots + c_n$, the coefficients are symmetric polynomials in the a_i. In fact,

$$\begin{multline*}(z - a_1) \cdots (z - a_n) = z^n - s_1(a_1, \dots, a_n)z^{n-1} \\ + s_2(a_1, \dots, a_n)z^{n-2} - \cdots \pm s_n(a_1, \dots, a_n).\end{multline*}$$

As a consequence, the elementary symmetric polynomials are the roots of the polynomial. This gives the following.

Corollary 2.19.

Given a polynomial $f \in K[x]$, pick any extension $K \subseteq L$ in which f factors completely, say as $f = (x - a_1) \cdots (x - a_n)$. Then any symmetric function $h(a_1, \ldots, a_n)$ is a polynomial in the coefficients of f. In particular, $h(a_1, \ldots, a_n) \in K$.

Proof. (of the corollary). We can write our symmetric function h as

$$h(a_1, \ldots, a_n) = g(s_1(a_1, \ldots, a_n), \ldots, s_n(a_1, \ldots, a_n)).$$

The coefficients of f sit inside K, and hence so does the above. □

Example 2.20. Let the roots of $f := x^3 + bx + cx + d$ in some extension field L be $a_1, a_2, a_3 \in L$. Then we have

$$a_1 + a_2 + a_3 = -b.$$

Also note $a_2^2 + a_2^2 + a_3^2 \neq b^2 = (a_1 + a_2 + a_3)^2$, so we need to get rid of the extra cross terms. After doing this we get since $c = a_1a_2 + a_1a_3 + a_2a_3$ that

$$a_2^2 + a_2^2 + a_3^2 = b^2 - 2c.$$

2.2.3 The Discriminant

Let $f \in K[x]$ be monic. The ***discriminant*** of f, denoted $\Delta(f) \in K$, is defined by taking an extension field $K \subseteq L$ so that f splits completely, say as $f = x(x-a_1) \cdots (x-a_n)$ with the $a_i \in L$, and setting

$$\Delta(f) := \prod\nolimits_{1 \leq i < j \leq n} (a_i - a_j)^2.$$

Note that in particular, this is a symmetric function in the roots, so this is in K. We, therefore, know from before that $\Delta(f)$ can be written as a polynomial in the coefficients of f, but this is hard to do.

Example 2.21. Consider $f := x^2 + bx + c$. Let f have roots a_1 and a_2. Then $b = -a_1 - a_2$ and $c = a_1a_2$. Thus $\Delta(f) = (a_1 - a_2)^2 = a_1^2 - 2a_1a_2 + a_2^2 = b^2 - 4c$. In summary,

$$\Delta(ax^2 + bx + c) = b^2 - 4c.$$

In general, finding a formula for $\Delta(f)$ in the coefficients of f is hard for higher-degree polynomials. However, there is an exception. If f is a cubic without a quadratic term. In particular,

$$\Delta(x^3 + px + q) = -4p^3 - 27q^2.$$

This is indeed, a homogeneous[2] degree six polynomial in the a_i, namely $p = a_1a_2 + a_1a_3 +$

[2] We mean homogeneous degree six to mean that *all terms* have degree six.

a_2a_3, $q = a_1a_2a_3$, so p^3 has degree six and q^2 has degree six. We will not do the explicit calculation, but we will describe how to do it, that is a general technique. We know the discriminant is a degree six monic in the a_is and is also a polynomial in p and q. p has degree 3 and q has degree 2. Thus a monomial p^nq^m has degree $3n+2m$, which can be six only if $(n,m) \in \{(2,0),(0,3)\}$. We thus know $\Delta(f) = \lambda p^3 + \delta q^2$ for some constants λ and δ. We can solve for λ and δ by trying specific polynomials, e.g. $f := x(x+1)(x-1) = x^3 - x$, so

$$\Delta(f) = (0-1)^2(0+1)^2(1+1)^2 = 4.$$

Then $q = 0$ and $p = -1$ and thus $4 = \Delta(f) = \lambda p + \delta q = \lambda(-1) = -\lambda$, so we see that $\lambda = -4$ as desired. δ may be found by doing the same thing with other polynomials, noting that we must choose one where q is nonzero.

Properties of the discriminant:

- $\Delta(f) \in K$ is a polynomial in the coefficients of f.
- $\Delta(f) = 0$ iff f has a multiple root in some field extension (i.e. iff f is not separable over K).

Example 2.22. $f := x^2 + bx + c$ has $\Delta(f) = b^2 - 4c$, which is zero iff x has a multiple root, i.e. iff

$$x = \frac{-b \pm \sqrt{b^2 - 4c}}{2} = \frac{-b}{2} \pm 0,$$

which are the same.

2.2.4 Splitting Fields

Recall that given field extensions $K \subseteq L$ and $K \subseteq L'$, an isomorphism relative to K from L_1 to L_2 is a field isomorphism $\varphi : L_1 \overset{\cong}{\to} L_2$ such that $\varphi|K = \mathrm{id}_K$. An ***automorphism of $K \subseteq L$ relative to K*** is a field isomorphism $\varphi : L \to L$ with $\varphi|K = \mathrm{id}$. The ***Galois group*** of extensions $K \subseteq L$ is

$$\mathrm{Gal}(L/K) = \{\text{automorphisms of } L \text{ relative to } K\},$$

which is also denoted $\mathrm{Aut}(L/K)$.

Example 2.23 (midterm, letting $d = -1$)**.** Complex conjugation $\varphi : \mathbb{C} \to \mathbb{C}$ with $\varphi(z) = \overline{z}$ is an element of $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$, and in fact $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}, \varphi\} \cong \mathbb{Z}/(2)$. More generally, if $d \in K$ is not a square then

$$\mathrm{Gal}(K[\sqrt{d}]/K) = \{\mathrm{id}, \varphi\} \cong \mathbb{Z}/(2),$$

with $\varphi : K[\sqrt{d}] \to K[\sqrt{d}]$, $\varphi(a + b\sqrt{d}) = a - b\sqrt{d}$.

Basic construction: If $K \subseteq L_1 = K[\alpha]$ and $K \subseteq L_2 = K[\beta]$ and if α, β have the same minimal polynomial $f \in K[x]$ then we can define an isomorphism relative to K in the following way, namely with

$$\varphi : L_1 \to L_2$$
$$K[x]/(f) \cong K[\alpha] = L_1 \xrightarrow{\varphi} L_2 = K[\beta] \cong K[x]/(f),$$

and if f_1 is the left isomorphism and f_2 is the right isomorphism then

$$\varphi(x) = f_2^{-1}(f_1(x)) \in L_2.$$

For a monic polynomial $f \in K[x]$, a ***splitting field*** for f is an extension $K \subseteq L$ such that $f = (x - a_1) \cdots (x - a_n)$ for $a_1, \dots, a_n \in L$, and $L = K[a_1, \dots, a_n]$. In other words, L is the smallest field extension of K such that f splits completely.

Recall that we can construct a splitting field L above by adjoining roots of irreducible factors of f until it splits completely.

Lemma 2.24.

If $K \subseteq F$ is a field extension and $f \in K[x]$ then there exists at most one splitting field $K \subseteq L$ for f with $L \subseteq F$.

Proof. If a splitting field exists inside F then we can write $f = (x - a_1) \cdots (x - a_n)$ with $a_1, \dots, a_n \in F$ and the splitting field *must* be $K[a_1, \dots, a_n]$. □

Theorem 2.25.

If K is a perfect field, $f \in K[x]$ is monic, then if $K \subseteq L_1$ and $K \subseteq L_2$ are splitting fields for f then there exists an isomorphism $\varphi : L_1 \overset{\cong}{\to} L_2$ relative to K.

In other words, then f has a unique splitting field up to isomorphism.

Proof. Since K is perfect there's a primitive element $\gamma \in L_1$ so that $L_1 = K[\gamma]$. Let the minimal polynomial for γ be $g \in K[x]$. Let $L_2 \subseteq F$ be a field extension such that there is some $\gamma' \in F$ with $g(\gamma') = 0$. We can use the basic construction (of fields from quotienting out ideals generated by irreducible polynomials) to find an isomorphism $\varphi : L_1 = K[\gamma] \to K[\gamma'] \subseteq F$ relative to our base field K.

In fact, $\operatorname{im}(\varphi) \cong L_1$ and L_2 are subfields of F that are splitting fields for f. But then the trivial lemma above implies that $\operatorname{im}(\varphi) = L_2$, so $\varphi : L_1 \to L_2$ is an isomorphism relative to K. □

We will soon show something shocking about splitting fields.

Lemma 2.26.

Let $K \subseteq L$ be any finite extension. Then we can find an extension $L \subseteq F$ such that $K \subseteq F$ is a splitting field for some $f \in K[x]$.

Proof. $K \subseteq L$ is a finite extension, so there exist elements $a_1, \dots, a_n \in L$ such that $L = K[a_1, \dots, a_n]$. Let f_i be the minimal polynomial of a_i, and set $g := f_1 f_2 \cdots f_n$. We can adjoin roots of g to L to make $L \subseteq F$ such that g splits completely, so $K \subseteq F$ is a splitting field for g. □

Theorem 2.27: Fundamental Theorem of Splitting Fields.

If $K \subseteq L$ is a splitting field for some $f \in K[x]$ then any monic irreducible with a root in L splits completely in L.

Proof. L is a splitting field for f, so $L = K[a_1, \dots, a_n]$ with $f = (x - a_1) \cdots (x - a_n)$. We can find some $p_1 \in K[x_1, \dots, x_n]$ such that $\beta = p_1(a_1, \dots, a_n)$.

Let $p_1, \dots, p_\ell$ ($\ell = n!$) be all the ways of reordering the variables inside the p_is.

For instance, if $n = 3$ and $p_1 = x_1^2 + x_2x_3$ then $p_1 = x_1^2 + x_2x_3$, $p_2 = x_1^2 + x_3x_2$, $p_3 = x_2^2 + x_3x_1$, $p_4 = x_2^2 + x_3x_1$, $p_5 = x_3^2 + x_1x_2$, $p_6 = x_3^2 + x_2x_1$ (corresponding to the six different orderings of (123).

Set $\beta_i := p_i(a_i, \dots, a_n)$ so that $\beta = \beta_1$. Key observation: Regard the β_i as functions of the a_j. Then any symmetric function $\varphi(\beta_1, \dots, \beta_m)$ is also symmetric in the a_js (that is, permuting the a_js just permutes the p_is and thus the β_is). Thus, letting $h := (x - \beta_1) \cdots (x - \beta_m) \in L[x]$. The coefficients of h are symmetric functions of the β_is, and thus are also symmetric functions in the a_js. In other words, if c is a coefficient of $h(x)$ then we can write $c = \varphi(\beta_1, \dots, \beta_m)$, where φ is a symmetric polynomial, and thus

$$c = \varphi(p_1(a_1, \dots, a_n), \dots, p_m(a_1, \dots, a_n))$$

is a symmetric function evaluated at $a_1, \dots, a_n$. Since $f = (x - a_1) \cdots (x - a_n) \in K[x]$, any symmetric function in the a_js is a polynomial in the coefficients of f, and thus sits in K. Hence the coefficients of h sit inside K.

Now, we're given that $g \in K[x]$ is irreducible and shares a root $\beta = \beta_1$ with $h \in K[x]$. Thus, g must divide h, and in particular, the roots of g are among the roots of h (though of course h may have more roots overall than g). In other words, g factors as a product of some of the linear factors of $h = (x - \beta_1) \cdots (x - \beta_m)$. □

This is devilishly clever.

Convention 2.28.

Henceforth all fields are perfect unless otherwise stated.

Fix a field F of characteristic zero (and assume for today that all fields are characteristic zero unless otherwise stated). Recall the Galois group of K/F, denoted $\mathrm{Gal}(K/F)$, is the group F-automorphisms of K.

Definition 2.29 (Galois extension)**.** A finite field extension K/F is a ***Galois extension*** if $[K:F] = |\operatorname{Gal}(K/F)|$.

Definition 2.30 (fixed field)**.** If K is a field and H is any group of automorphisms of K, then the ***fixed field*** of H, denoted K^H, is the set of elements of K which are fixed by every element of H. It is easy to check that K^H is a subfield. It is also easy to check that H is a subgroup of $\operatorname{Gal}(K/K^H)$.

We will soon show that H actually coincides with the Galois group.

Theorem 2.31: Artin Theorem 16.5.2.

Let $F := K^H$. Where K is a field, H is a finite group of automorphisms of K, and $\beta_1 \in K$. What is the orbit of $\beta_1 \in K$ in H? If $(\beta_1, \ldots, \beta_r)$ is the orbit of β_1 under H (which must be finite since H is finite), then we have the following points:

(1) The minimal polynomial of β_1 over F is $f(x) = (x - \beta_1) \cdots (x - \beta_r)$.

(2) β_1 is algebraic over F, $\deg \beta_1$ over F is r, and r divides $|H|$.

Proof. That (2) implies (1) follows from the orbit-stabilizer theorem (with the group H acting on the set G), the details for which are left to the reader.

We now prove (1). If $f = x^r + b_1 x^{r-1} + b_2 x^{r-2} + \cdots + b_r$. The b_i are symmetric functions of the β_i. If $\sigma \in H$ then since σ permutes the set $\{\beta_1, \ldots, \beta_r\}$ we have $\sigma(f(x))$. Hence the "roots" of f are in $K^H = F$. Thus $f \in F[x]$ as claimed.

We now want to show that f is irreducible. Let $h \in F[x]$ such that $h(\beta_1) = 0$. We will show $f(x)$ divides $h(x)$. We want to show that each factor of f is a factor of h over K. $h(\beta_1) = 0$, so $(x - \beta_1)$ is a factor of h. To get that the other linear factors $(x - \beta_i)$ of f are factors of h, we let the $\sigma \in H$ act on the $\{\beta_1, \ldots, \beta_r\}$. More precisely, if σ is an element of the automorphism group then since h is a polynomial over F we know σ fixes the coefficients of H, so from $h(\beta_1) = 0$ we get $\sigma(h(\beta_1)) = \sigma(0) = 0$, and since σ fixes the coefficients of h this gives that $h(\sigma(\beta_1)) = 0$. Hence for every i in the orbit $h(\beta_i) = 0$, so $(x - \beta_i)$ divides h in $K[x]$. Thus f divides $h(x)$ in $K[x]$.

Since $f, h \in F[x]$ it follows that f divides h over F, so in other words $f(x)$ generates the principal ideal of polynomials that have β_1 as a root, so f is the minimal polynomial of β_1 over F. □

Recall that a field extension K/F is algebraic if all its elements are algebraic over K.

Lemma 2.32.

Let $[K:F] = \infty$ be an algebraic field extension. Then there exist elements in K that have arbitrarily large degree over F.

This is not an obvious assertion. The above lemma may not be true in general, and it is almost surprising that it is true even for characteristic zero. The reason this is not obvious is that in principle we could think of adding field extensions of an element of some bounded degree k countably many times so that each time it increases the degree of the field extension while keeping bounded the degree of the elements.

Proof. Let $\alpha_1 \in K$, $\alpha_1 \notin F$. Consider the extension $F \subseteq F(\alpha_1)$. α_1 is algebraic over F by assumption, so the degree $[F(\alpha_1) : F] < \infty$. In particular, $F \subseteq F(\alpha) \subsetneq K$ ($(*)$ where the right extension is proper because $F(\alpha)$ has finite degree over F and K has infinite degree over F, so $F(\alpha) \neq K$). Thus we can find $\alpha_2 \in K$ with $\alpha_2 \notin F(\alpha_1)$. Consider

$$F \subseteq F(\alpha_1) \subseteq F(\alpha_1, \alpha_2) \subsetneq K.$$

The left extension has finite degree > 1. The middle extension has finite degree > 1. The next extension is proper by applying $(*)$ above to $F(\alpha_1, \alpha_2)$.

We then proceed inductively to construct an infinite sequence of finite degree extensions to get a chain of field extensions,

$$F \subsetneq F_1 \subsetneq F_2 \subsetneq F_3 \subsetneq \cdots,$$

and since $\operatorname{char} F = 0$ we know that for each i there is some $\beta_i \in F_i$ such that $F_i = F(\beta_i)$. Hence the degree of β_i over F is $[F_i : F]$ and, by construction, $[F_i : F]$ can be made arbitrarily large. □

Theorem 2.33: Fixed Field Theorem.

If K is a field, H is a group acting on K is a finite automorphism group and $F = K^H$. Then $F \subseteq K$ is a finite extension and in fact $[K : F] = |H|$.

Proof. Set $n := |H|$. We use the previous theorem to get that every element of K has degree over F dividing n. Then every element of K is algebraic over F, so K/F is an algebraic extension. Notice $[K : F] < \infty$, so we don't have elements of arbitrarily large degree by the above point, so K has a primitive element since this is a finite extension (on a field of characteristic zero). Let γ be such a primitive element. Then $K = F(\gamma)$.

Let $\sigma \in H$. What is $\sigma(\gamma)$? Either if fixes or moves γ, so for a moment let's consider the case that σ fixes γ. In this case we have $\sigma = \mathrm{id}_K$ (since $K = F(\gamma)$ and $\sigma|F = \mathrm{id}$), so the stabilizer of γ is $\{1\}$ (the identity of the group). Then the orbit of γ under H has order n, so by the first theorem from today we have that the degree of γ over $F = K^H$ is the order of the orbit of γ, so the degree of γ over F is n, so $[K : F] = [F(\gamma) : F] = n$.

If σ doesn't fix γ then it moves it to n different places so we're good. □

Then we immediately have

Corollary 2.34.

In the above notation, we have $\text{Gal}(K/F^H) \cong H$.

§2.3 Galois Extensions

Convention 2.35.

Henceforth unless otherwise stated, all fields are perfect (e.g. finite fields or of zero characteristic)

We will frequently use that

(1) Irreducibles $f \in K[x]$ have no repeated roots in any extension field.

(2) All finite extensions $K \subseteq L$ have primitive elements, i.e. $\gamma \in L$ with $L = K[\gamma]$.

Recall the fundamental theorem of splitting fields, which states that for finite field extension $K \subseteq L$, the following are equivalent:

(a) If $f \in K[x]$ irreducible and f has root in L, then f splits completely in $L[x]$.

(b) L splitting field for some $g \in K[x]$.

Finally recall the fixed field theorem, that if L is a field and G is the finite group of automorphisms of L, and $K = L^G = \{x \in L : g(x) = x \text{ for all } x \in G\}$, then $K \subseteq L$ is a finite extension with $|G| = [L : K]$.

Lemma 2.36.

If $K \subseteq L$ is a finite extension and $G = \text{Gal}(L/K)$ then $|\text{Gal}(L/K)|$ divides $[L : K]$.

Proof. We want to apply the fixed field theorem, so we need to show that G is finite. Let γ_1 be a primitive element of $K \subseteq L$. Let f be the minimal polynomial for γ_1 over K. Let $\gamma_1, \ldots, \gamma_r$ be the roots of f in L. For $g \in G$, $g(\gamma_i)$ a root of f for all i, so g permutes $\{\gamma_1, \ldots, \gamma_r\}$. Moreover, if $g_1(\gamma_1) = g_2(\gamma_2)$, then $g_1^{-1}g_2(\gamma_1) = \gamma_1$, so $g_1^{-1}g_2$ fixes $L = K[\gamma_1]$ and thus $g_1 = g_2$, so $|G| \leq r$.

We now apply the fixed field theorem. Let $F = L^G$, so $K \subseteq F \subseteq L$. We have by the fixed field theorem that $|G| = [L : K] = [L : F][F : K]$, we conclude $|G|$ divides $[L : K]$. □

Lemma 2.37.

If G is a finite group of automorphisms of a field L and $K = L^G$ then $G = \text{Gal}(K/L)$.

Proof. We know $G \subseteq \mathrm{Gal}(K/L)$ and by the fixed field lemma $|G| = [L : K]$, but the above lemma shows that $|\,\mathrm{Gal}(K/L)|$ divides $[L : K]$. Thus $|G| = |\,\mathrm{Gal}(K/L)|$, so they must coincide. □

Lemma 2.38.

Let $K \subseteq L$ be a finite extension with primitive element $\gamma_1 \in L$, so $L = K[\gamma_1]$. Just as above, let $\gamma_1, \ldots, \gamma_r$ be the roots of f that sit in L.

Then $G = \mathrm{Gal}(L/K)$ has order r, and for $1 \leq i \leq r$ there exists a unique $g \in G$ with $g(\gamma_1) = \gamma_i$.

Proof. Running the proof of the previous claim above, we see it is enough to prove the second claim, namely that $1 \leq i \leq r$ exists and $g \in G$ with $g(\gamma_1) = \gamma_i$.

Since γ_i and γ_1 have the same minimal polynomial, there exists an isomorphism $\varphi : K[\gamma_1](= L) \to K[\gamma_i](\subseteq L)$ (since $K[\gamma_1] \cong K[x]/(f) \cong K[\gamma_i]$).

Since φ fixes the subfield K, we know that the index $[K[\gamma_1] : K] = [K[\gamma_i] : K]$.

Thus we must have that $K[\gamma_1] = L$. Hence $\varphi \in \mathrm{Gal}(L/K)$. □

Theorem 2.39: Definition/Characterization of Galois Extension.

Let $K \subseteq L$ be a finite extension and let G be its Galois group, i.e. $G := \mathrm{Gal}(L/K)$. Then the following are equivalent.

(a) $|G| = [L : K]$ (probably most unintuitive)

(b) $L^G = K$ (says the Galois group isn't too small)

(c) $K \subseteq L$ is a splitting field (easiest to check/work with, i.e. of more practical use)

A finite extension $K \subseteq L$ is a ***Galois extension*** if any of the three (equivalent) conditions above hold.

Proof. We first prove (a) iff (b). Let F be the fixed field of G, i.e. $F = L^G$. Then $K \subseteq F \subseteq L$. Then the fixed field theorem says $|G| = [L : F]$. Thus $K = F = L^G$ iff $|G| = [L : K]$.

We now prove (a) iff (c). Let γ_1 be a primitive element for $K \subseteq L$ and $f \in K[x]$ be its minimal polynomial. Thus $\deg(f) = [L : K]$ (where $L = K[\gamma_1]$. So (a) is equivalent to $|G| = \deg(f)$. But by a previous lemma the order $|G|$ is the number of roots of f that sit inside L. Thus $|G| = \deg(f)$ iff f splits completely in $L[x]$, i.e. iff L is a splitting field over K. (Note that this argument requires perfection of the field since we rely on the assumption that f has no repeated roots inside L). □

Galois theory is the study of Galois extensions.

Lemma 2.40.

For any finite extension $K \subseteq L$ there exists an $L \subseteq F$ such that $K \subseteq F$ is a Galois extension.

Proof. We proved earlier that all field extensions can be extended to splitting fields. □

The above lemma tells us that being Galois just means that the extension isn't too small. Everything can be made a bit bigger to make it a Galois extension.

Lemma 2.41.

If $K \subseteq L$ is a Galois extension and $K \subseteq F \subseteq L$ is a subfield then $F \subseteq L$ is a Galois extension.

Proof. This is true for splitting fields, so since perfect fields are splitting fields if and only if they are Galois extensions the result follows. □

Remark 2.42. In the above, the Galois group $\text{Gal}(L/F)$ is a subgroup of $\text{Gal}(L/K)$, since an automorphism of F fixing L definitely fixes K since K is smaller. We will actually prove that these subgroups are actually in one-to-one correspondence with intermediate fields, which will be known as the fundamental theorem of Galois theory.

Definition 2.43. Let S_n be the symmetric group on $\{1 \ldots, n\}$. A subgroup G of S_n is called ***transitive*** if it acts transitively on $\{1, \ldots, n\}$. That is, if for all $i, j \in \{1, \ldots, n\}$ there exists some $g \in G$ with $g(i) = j$.

Informally, then, a subgroup H of S_3 acts ***transitively*** on a set X if any two elements are "connected" by some $h \in H$.

Remark 2.44 (Important Observation)**.** Let $K \subseteq L$ be a Galois extension with $n = [L : K]$. Then $\text{Gal}(L/K)$ is isomorphic to a *transitive* subgroup of S_n.

Proof. Indeed, let $\gamma_1 \in L$ be a primitive element and let $f \in K[x]$ be its minimal polynomial. Then we know $n = \deg(f)$, and f splits completely in $L[x]$ since it is a splitting field.

We proved earlier that $\text{Gal}(L/K)$ acts transitively on the set $\{\gamma_1, \ldots, \gamma_n\}$ of roots of $f(x)$ in L, so this identifies the Galois group $\text{Gal}(L/K)$ with a transitive subgroup of S_n. □

Notation 2.45. For a polynomial $f \in K[x]$, the Galois group of f is the Galois group of the splitting field for f. This is written $\text{Gal}(f)$.

§2.4 Main Theorem of Galois Theory

Theorem 2.46: Main Theorem of Galois Theory.

If $K \subseteq L$ is a Galois extension and $G := \operatorname{Gal}(L/K)$. Then there is a bijection

$$\begin{aligned} \{\text{fields } F : K \subseteq F \subseteq L\} &\overset{\sim}{\longleftrightarrow} \{\text{subgroups of } G\}, \\ L^H &\longleftarrow H \\ F &\longmapsto \operatorname{Gal}(L/F) \end{aligned}$$

This bijection is called the ***Galois correspondence***.

Proof. Consider $K \subseteq F \subseteq L$. Set $H = \operatorname{Gal}(L/F)$. We must prove $F = L^H$. $K \subseteq L$ is a Galois extension (e.g. since $K \subseteq L$ is a splitting field, so is $F \subseteq L$, and another characterization of Galois is $L^{\operatorname{Gal}(L/F)} = F$.

Consider a subgroup H of G. Set $F = L^H$. We must show $H = \operatorname{Gal}(L/F)$. Again, $F \subseteq L$ is a Galois extension and yet another characterization of a Galois extension is that $|\operatorname{Gal}(L/F)| = [L : F]$. Then by the fixed field theorem we have $|H| = [L : L^H] = F$ since H is a subgroup of $\operatorname{Gal}(L/F)$ and $|H| = |\operatorname{Gal}(L/F)|$, so we have $H = \operatorname{Gal}(L/F)$. □

If $K \subseteq L$ is Galois and $K \subseteq F \subseteq L$ then $K \subseteq F$ need not be a Galois extension. But the question is—when is it? There is a beautiful answer to this in terms of the Galois correspondence: it turns out that Galois extensions correspond to normal subgroups!

Theorem 2.47.

Let $K \subseteq L$ be a Galois extension and let F be an intermediate field $K \subseteq F \subseteq L$. Let $G := \operatorname{Gal}(L/K)$ and let $H := \operatorname{Gal}(L/F)$ (so H is a subgroup of G). Then

$$H \text{ is a normal subgroup of } G \iff K \subseteq F \text{ is a Galois extension}$$

Moreover, if $K \subseteq F$ is Galois, then The Galois group is isomorphic to the quotient group of G by H, that is, $\operatorname{Gal}(F/K) \cong G/H$.

Proof. Let γ_1 be a primitive element of $K \subseteq F$ and suppose $f \in K[x]$ is its minimal polynomial. The assumption that $K \subseteq L$ is a Galois extension and $f(\gamma_1) = 0$ implies that f splits completely in $E[x]$. Let $\gamma_1, \dots, \gamma_n$ be its roots. Since $\gamma_1 \in F$, $K \subseteq L$ is Galois (i.e. is a splitting field) if and only if $\gamma_1, \dots, \gamma_n \in F$. So our first goal is to show the following:

Claim 2.48. $\gamma_1, \dots, \gamma_n \in F$ if and only if H is a normal subgroup of G.

Proof. $G = \operatorname{Gal}(L/K)$ acts transitively on $\{\gamma_1, \dots, \gamma_n\}$. Let G_γ be the G-stabilizer of γ_1, $F = K[\gamma_1]$, and $H = \{g \in G : g_F = \mathrm{id}\}$ (part of the Galois correspondence). For $g \in G$ we have $g(\gamma_1) \in F$ if and only if $F = K[g(\gamma_1)]$, so since $F = L^H$ we have $g(\gamma_1) \in F$ if and only if $G_{g(\gamma_1)} = H$.

We have the key fact that $G_{g(\gamma_1)} = gG_{g(\gamma_1)}g^{-1}$, which is because

$$gG_{g(\gamma_1)}g^{-1}(g(\gamma_1)) = gG_{g(\gamma_1)}(\gamma_1) = g(\gamma_1).$$

Therefore, $g(\gamma_1) \in F$ if and only if $H = gG_{\gamma_1}g^{-1} = gHg^{-1}$ since all γ_i are of this form sit in F if and only if $gHg^{-1} = H$ for all $g \in G$, i.e. H is a normal subgroup. □

Now, assume $K \subseteq F$ is Galois so that $\gamma_1, \ldots, \gamma_n \in F$. For $g \in G$, the action of g on L takes $F = K[\gamma_1]$ to $K[g(\gamma_1)] = F$, i.e. restricting the action of G on L to F gives a homomorphism $\varphi : G \to \mathrm{Gal}(F/K)$.

φ is surjective, since it is an element of $\mathrm{Gal}(F/K)$ determined by where it sends the generator γ_1, and G can send γ_1 to *any* root γ_i of f. Also, $\ker(\varphi) = H$ by definition. implies φ descends to an isomorphism $G/H \cong \mathrm{Gal}(F/K)$. □

Corollary 2.49.

For any finite extension $K \subseteq L$ there are finitely many intermediate fields F

Proof. We can enlarge L, so assume $K \subseteq L$ is a splitting field and hence a Galois extension. Thus $G = \mathrm{Gal}(L/K)$ is a finite group, so it has finitely many subgroups by the fundamental theorem for Galois theory. (Note that this argument fails if K is not perfect, and in fact, the claim is *false* in the case K is not perfect. □

2.4.1 Applications of the Galois Correspondence

The Galois correspondence has several features.

(1) A field corresponding to the trivial subgroup is $L^I = L$ itself.

(2) The field F corresponding to $H = G$ is $L^G = F$.

(3) More generally, the correspondence reverses inclusions: For H_1, H_2 subgroups of G, we have

$$H_1 \subseteq H_2 \Leftrightarrow L^{H_2} \subseteq L^{H_1}.$$

(4) With regards to topology, this should remind you of the correspondence between covers and subgroups of the fundamental group π_1. This is no accident...

Example 2.50. The only Galois groups we know right now are the quadratic extensions, namely if $d \in K$ is not a square then $K \subseteq K[\sqrt{d}]$ is a quadratic extension, and its Galois group $\mathrm{Gal}(K[\sqrt{d}]/K)$ are 1 and $\mathbb{Z}/(2) \cong C_2$, which as no nontrivial intermediate fields.

To get a more interesting example, however, we can adjoin two square roots.

Example 2.51. The extension $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ is a degree 4 extension, and it is the splitting field for $f := (x^2 - 2)(x^2 - 3)$, and hence is a Galois extension.

Let $G := \mathrm{Gal}(\mathbb{Q}[\sqrt{2}, \sqrt{3}]/\mathbb{Q})$. We know $|G| = 4$, and the only groups of order 4 are $\mathbb{Z}/(4) = \{0, 1, 2, 3\} \cong C_4$ or $C_2 \oplus C_2 \cong V$, the Klein-4 group.

Which one is it? Well, C_4 has only one nontrivial subgroup, namely $\{0, 2\} \cong C_2$. On the other hand, $C_2 \oplus C_2$ has three nontrivial subgroups, namely $C_2 \oplus 0$, $0 \oplus C_2$, and the diagonal subgroup $\langle (1, 1) \rangle \cong C_2$.

There are at least three intermediate fields:

$$\mathbb{Q} \subseteq \substack{\mathbb{Q}[\sqrt{2}] \\ \mathbb{Q}[\sqrt{3}] \\ \mathbb{Q}[\sqrt{6}]} \subseteq \mathbb{Q}[\sqrt{2}, \sqrt{3}].$$

Each corresponds to a subgroup of G, so, therefore, it must be the case that $G \cong C_2 \oplus C_2$, since this is the unique group of order 4 with three nontrivial subgroups.

As an application of this, we have for any $a, b \in \mathbb{Q}$ that the intermediate field $\mathbb{Q}[a\sqrt{2} + b\sqrt{3}]$ must be one of the three fields. If $a, b \neq 0$, then it can't be any of $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{3}]$, or $\mathbb{Q}[\sqrt{6}]$.

To see why e.g. it is not $\mathbb{Q}[\sqrt{6}]$, note that if $a\sqrt{2} + b\sqrt{3} \in \mathbb{Q}[\sqrt{6}$ then we have $a\sqrt{2} + b\sqrt{3} = c\sqrt{6} + d$, which is not possible for any $a, b \in \mathbb{Q}$. Similar reasoning rules out $\mathbb{Q}[\sqrt{2}]$ and $\mathbb{Q}[\sqrt{3}]$. It therefore must be that $\mathbb{Q}[a\sqrt{2} + b\sqrt{3}] = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ if $a, b \neq 0$.

§2.5 Cubic Polynomials Revisited

Example 2.52. Let $f := x^3 + ax^2 + bx + c$ be an irreducible cubic in $\mathbb{Q}[x]$. Let L be the splitting field of f.

$\mathbb{Q} \subseteq L$ is a Galois extension since it is a splitting field. The goal here is to understand $G := \mathrm{Gal}(L/\mathbb{Q})$. Let $\alpha_1, \alpha_2, \alpha_3 \in L$ be roots of f, so $f = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$. Since $\alpha_1 + \alpha_2 + \alpha_3 = -a \in \mathbb{Q}$, we have $L = \mathbb{Q}[\alpha_1, \alpha_2, \alpha_3] = \mathbb{Q}[\alpha_1, \alpha_2]$ since $\mathbb{Q}_3 = -a - \alpha_1 - \alpha_2$. G acts transitively on $\{\alpha_1, \alpha_2, \alpha_3\}$, so G is a subgroup of S_3, the symmetric group on three elements. It is a *transitive subgroup*. There are two transitive subgroups of S_3, those being S_3 itself (corresponding to a degree six extension) and A_3 (corresponding to a degree three extension), where $A_3 = \ker(S_3 \xrightarrow{\sigma} \{\pm 1\}) \cong C_3 \cong \langle (123) \rangle$. Thus

$$\mathbb{Q} \overset{\deg=3}{\subseteq} \mathbb{Q}[\alpha_1] \subseteq \mathbb{Q}[\alpha_1, \alpha_2] = L,$$

where the second inclusion has an arrow saying "in $\mathbb{Q}[\alpha_1]$ min. poly of α_2 is $(x - \alpha_2)(x - \alpha_3)$ since $f(x) = (x - \alpha_1)(\text{min poly of } \alpha_2)$." The degree is either 1 or 2 depending on whether $(x - \alpha_2)(x - \alpha_3)$ has a root in $\mathbb{Q}(\alpha_1)$. Thus $G = S_3$ if and only if $\mathbb{Q}[\alpha_1] \subseteq \mathbb{Q}[\alpha_1, \alpha_2] = L$ is a nontrivial extension.

Example 2.53. $f(x) = x^3 + 3x + 1$ is a strictly increasing since $f' = 3x^2 + 3$. Has one real root α_1 and two complex roots α_2, α_3 that are complex conjugates of each other. $\mathbb{Q}[\alpha_1] \subseteq \mathbb{R}$, so cannot contain α_2, α_3, so the Galois group is isomorphic to S_3.

Note that the complex conjugation map $\mathbb{C} \to \mathbb{C}$ restricts to an element $\varphi \in \mathrm{Gal}(L/\mathbb{Q})$ of order 2, and $\varphi(\alpha_1) = \alpha_1$, φ exchanges α_2 and α_3 since Gal contains order 2 element cannot be $A_3 \cong C_3$. $L^{\{i\alpha,\varphi\}} \cong C_3$.

Let $f \in \mathbb{Q}[x]$ be a monic irreducible cubic, L its splitting field, and $\alpha_1, \alpha_2, \alpha_3$ its roots. Then $L = \mathbb{Q}[\alpha_1, \alpha_2, \alpha_3]$. Writing $f = x^3 + ax^2 + bx + c$, $\alpha_1 + \alpha_2 + \alpha_3 = -\alpha \in \mathbb{Q}$. Then

$$\mathbb{Q} \overset{\text{deg=3}}{\subseteq} \mathbb{Q}[\alpha_1] \overset{\text{deg=?}}{\subseteq} L.$$

Claim 2.54. $\mathbb{Q}[\alpha_1] \subseteq \mathbb{Q}[\alpha_1, \alpha_2]$ has degree 1 or 2 in $(\mathbb{Q}[\alpha_1])[x]$.

Proof. $f = (x - \alpha_1)g(x)$ with α_2, α_3 roots of $g(x)$, $g(x)$ quadratic. Degree 2 if g irreducible, degree 1 if g factors, so $\alpha_2 \in \mathbb{Q}[\alpha_1]$. $G = \mathrm{Gal}(L/\mathbb{Q})$ and G acts transitively on $\{\alpha_1, \alpha_2, \alpha_3\}$, so $G \subseteq S_3$. Transitivity implies $G = S_3$ or $A_3 \cong C_3$, A_3 being generated by the three-cycle (123). □

Example 2.55. Last time we proved $G = S_3$ for $f = x^3 + 3x + 1$. $f = x^3 - 3x + 1$ has three real roots. What is the nature of these roots? Let α be a root of f. By tedious algebra we can show that $\alpha^2 - 2$ is also a root:

$$\begin{aligned} f(\alpha^2 - 2) &= (\alpha^2 - 2)^3 - 3(\alpha^2 - 2) + 1 \\ &= (\alpha^3 - 3\alpha - 1)(\alpha^3 - 3\alpha + 1) = 0. \end{aligned}$$

It follows that the roots are $\alpha, \alpha^2 - 2, (\alpha^2 - 2) - 2 = \alpha^4 - 4\alpha^2 + 2$. Hence, the splitting field is $\mathbb{Q} \overset{\text{deg=3}}{\subseteq} \mathbb{Q}[\alpha] = L$, and therefore $G = \mathrm{Gal}(L/\mathbb{Q}) = A_3 \cong C_3$.

Is there a more general way to tell whether $G = S_3$ or A_3, i.e. how do we tell whether or not there is an algebraic relationship between the roots?

Well, if $\mathrm{Gal}(L/\mathbb{Q}) = S_3$ then it has A_3 as a normal subgroup. Then we can consider $K := L^{A_3}$, so $\mathbb{Q} \subseteq K \subseteq L$, and since A_3 is normal we know by a recent theorem that $\mathbb{Q} \subseteq K$ is a Galois extension with $\mathrm{Gal}(K/\mathbb{Q}) = S_3/A_3 \cong C_2$. This implies $\mathbb{Q} \subseteq K$ is a quadratic extension.

In fact, the converse is also true—if we have $\mathbb{Q} \subseteq K \subseteq L$ with $\mathbb{Q} \subseteq K$ a quadratic extension, then we know that the degree of $\mathbb{Q} \subseteq L$ must be even by the multiplicative property of the degree. Hence the Galois group can't be $A_3 \cong C_3$, so it must be S_3.

Recall the discriminant of f, $\Delta(f) = (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2$. We know $\Delta(f)$ is a symmetric function, and we know that if we take any symmetric function then we get a rational number, so the discriminant of f is a rational number. Define $\lambda := (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)$. Then λ is a square root of the discriminant, so $\lambda \in L$ and $\lambda^2 = \Delta(f) \in \mathbb{Q}$.

It follows that if $\Delta(f) \in \mathbb{Q}$ is *not* a square then λ does not sit in $\mathbb{Q}$, and

$$\mathbb{Q} \overset{\text{deg=2}}{\subseteq} \mathbb{Q}[\lambda] = \mathbb{Q}[\sqrt{\Delta(f)}] \subseteq L.$$

Therefore, if $f \in \mathbb{Q}[x]$ is an irreducible cubic with $\Delta(f) \in \mathbb{Q}$ is not a square, then the Galois group of its splitting field in S_3.

This is wonderful since we know how to compute the discriminant. But we can know even more—although not obvious, the converse is also true.

Claim 2.56. If $f \in \mathbb{Q}[x]$ is an irreducible cubic whose discriminant $\Delta(f) \in \mathbb{Q}$ is a square then the Galois group of the splitting field is A_3.

Proof. Let L be the splitting field for f. If $\Delta(f)$ is a square, then $\lambda = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)$ is rational. Thus, since elements of the Galois group $\operatorname{Gal}(L/\mathbb{Q})$ must fix the base field $\mathbb{Q}$, we know $\lambda \in \mathbb{Q}$ is fixed by the action of the Galois group $\operatorname{Gal}(L/\mathbb{Q})$ does nothing to λ. Using a transpose as opposed to only three cycles would have the action of swapping one of α_1 and α_2, α_1 and α_3, or α_2 and α_3, which multiplies λ by -1, so the action of $\operatorname{Gal}(L/\mathbb{Q})$ on $\{\alpha_1, \alpha_2, \alpha_3\}$ cannot include a transposition. Hence $\operatorname{Gal}(L/\mathbb{Q}) \cong C_3$. □

§2.6 Quartic Polynomials

Exercise 2.57. As an assignment, read the section in Artin on degree 4 polynomials. It is not "hard", though it is similar to this. It involves Lagrange resolvant, etc. It is too intricate to lecture about clearly, so it is better to read it on your own. The next problem set will contain problems on this topic.

§2.7 Finite Fields Revisited

Recall that if p is prime and $n \geq 1$ then there exists a unique field $\mathbb{F}_{p^n}$ of order p^n. We found the following key facts:

- $\mathbb{F}_{p^n}^\times = \mathbb{F}_{p^n} \setminus \{0\}$ is a cyclic group under multiplication, and so has order $p^n = 1$. Let $\tau \in \mathbb{F}_{p^n}^\times$ be a generator.
- Recall the Freshman's dream: $(x+y)^p = x^p + y^p$ for all $x, y \in \mathbb{F}_{p^n}$ which holds since all other terms in the binomial expansion have terms divisible by p.

Theorem 2.58.

$\mathbb{F}_p \subseteq \mathbb{F}_{p^n}$ is a Galois extension, and

$$\operatorname{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong C_n.$$

Proof. Define $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ by $f(x) = x^p$. As a result of the Freshman's dream, we know f is a field automorphism, which we recall is called the Frobenius.

For $x \in \mathbb{F}_p$ we have that $x^p = x$ since $\mathbb{F}_p^\times$ is cyclic of order $p-1$ (and $0^p = 0$), so $f|_{\mathbb{F}_p} = \operatorname{id}_{\mathbb{F}_p}$. Thus $f \in \operatorname{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. Since $f(0) = 0$ and for $x \in \mathbb{F}_{p^n}^\times$ we have $f^n(x) = x^{p^n} = x$, we know f has order at most n. We claim that f in fact has order n. In the above notation, the generator $\tau \in \mathbb{F}_{p^n}^\times$ has order exactly p^n, in fact $f^m(\tau) = \tau^{p^m} \neq \tau$ for $1 \leq m < n$. Thus f must have order *exactly* n, as claimed.

Since $|\operatorname{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)| \leq [\mathbb{F}_{p^n} : \mathbb{F}_p] = n$, with equality if and only if the extension is a Galois extension. It is a Galois extension, and the Galois group $\operatorname{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is the cyclic group of order n generated by the Frobenius. □

§2.8 Fundamental Theorem of Algebra Using Galois Theory

In this section, we strive to prove the fundamental theorem of algebra with the tools from Galois theory. Before we do this, however, we review some concepts from group theory.

2.8.1 Group theory background

Recall the Sylow theorems, namely that if p is prime and $|G| = p^k m$ for some m relatively prime to p and then there's a subgroup $H < G$ with $|H| = p^k$. (H is called a ***p*-Sylow subgroup**).

Example 2.59. Consider the group $G := S_8$. Then $|G| = 8!$, which is $3^2 m$ for some m such that $3 \nmid m$. G has a subgroup $H = \langle (123), (456) \rangle$ (these commute) $\cong (\mathbb{Z}/(3))^2$. $|H| = 9$, and H is a 3-Sylow subgroup.

Challenge: $|S_9| = 3^4 m$. Find the 3-Sylow subgroup...

Lemma 2.60.

If G is a finite group with $|G| = p^k$ with p prime. Let $Z(G)$ be the center of G. That is, $\{g \in G : gh = hg \text{ for all } h \in G\}$. Then $Z(G) \neq 1$.

Proof. Let $C_0, C_1, \ldots, C_r$ be the conjugacy classes of G, ordered such that $C_0 = \{1\}$. G acts on C_i transitively, so letting $x \in C_i$ we have

$$|C_i| = [G : C_G(x)] = \frac{|G|}{|C_G(x)|} = p^{n_i},$$

with $n_i = 0$ iff $C_G(x) = G$, i.e. $x \in Z(G)$. We have $G = C_0 \oplus C_1 \oplus \cdots \oplus C_r$, so $|G| = \sum_{i=0}^r |C_i| = 1 + \sum_{i=1}^r p^{n_i}$, where 1 corresponds to $|C_0|$. Since $p \mid |G|$ but $p \nmid 1$, we must have $p \nmid \sum_{i=1}^r p^{n_i}$. We therefore must have $n_{i_0} = 0$ for some $1 \leq i_0 \leq r$, i.e. $|C_{i_0}| = 1$. Letting $x \in C_{i_0}$, we have that $x \in Z(G)$ is nontrivial. □

Corollary 2.61.

If $|G| = p^c$ for p prime and $k \geq 1$ then there exists a surjection $\varphi \twoheadrightarrow \mathbb{Z}/(p)$.

Proof. We induct on k, the base case $k = 1$ being trivial since then $G \cong \mathbb{Z}/(p)$. For the induction step, let $k \geq 2$ and suppose the claim holds for smaller groups. If G is abelian then the corollary follows from the classification of finitely generated abelian groups. If G is not abelian then $Z(G) \neq G$, and the lemma says $Z(G) \neq 1$. Thus since $G' := G/Z(G)$ is a finite group with $|G'| = p^{k'}$ for some $1 \leq k' \leq k$.

Then by the induction hypothesis we can find $\varphi' : G' \twoheadrightarrow \mathbb{Z}/(p)$, so we define $\varphi : G \twoheadrightarrow \mathbb{Z}/(p)$ by $G \twoheadrightarrow G/Z(G) \xrightarrow{\varphi'} \mathbb{Z}/(p)$. □

Corollary 2.62.

If $|G| = p^k$ then there exists a chain of normal subgroups

$$1 = G_0 \lhd G_1 \lhd \cdots \lhd G_k = G$$

such that $G_i/G_{i-1} \cong \mathbb{Z}/(p)$ for all $1 \leq i \leq k$.

Proof. Set $G_k = G$. By the previous corollary we can find $G_{k-1} \lhd G_k$, namely the kernel of the surjective homomorphism $G_k \twoheadrightarrow \mathbb{Z}/(p)$, with $G_k/G_{k-1} \cong \mathbb{Z}(p)$. $|G_{k-1}| = p^{k-1}$. Applying the corollary again, we can find $G_{k-2} \lhd G_{k-1}$. □

We now see an example of a filtration tool.

Example 2.63. Consider the ***Heisenberg group***, given by

$$G = \left\{ \begin{bmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{bmatrix} : x, y, z \in \mathbb{F}_p \right\}.$$

Note $|G| = p^3$. Observe that

$$1 = G_0 \lhd G_1 = \begin{bmatrix} 1 & 0 & * \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \lhd G_2 = \begin{bmatrix} 1 & * & * \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \lhd G_3 = \begin{bmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{bmatrix} = G,$$

and indeed $G \cong \mathbb{Z}/(p)$ with center $G/G_1 \cong (\mathbb{Z}/(p))^2$ generated by $\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$.

2.8.2 The Proof

Theorem 2.64: Fundamental Theorem of Algebra.

$\mathbb{C}$ is algebraically closed.

Proof. It suffices to show that if $R \subseteq L$ is a nontrivial finite field extension then $[L : \mathbb{R}] = 2$, and thus $L \cong \mathbb{C}$. Without loss of generality, suppose $\mathbb{R} \subseteq L$ is a Galois extension (since we can always enlarge it to be). Set $G := \mathrm{Gal}(L/\mathbb{R})$. We seek to show $G \cong \mathbb{Z}/(2)$. We will use the Sylow theorem, the corollary of the corollary, and the Galois correspondence.

We'll first use the Sylow theorems to show $|G| = 2^n$ for some n. Let $H < G$ be a 2-Sylow subgroup (which exists since every group has a 2-Sylow subgroup, and in particular if the group has odd order then the 2-Sylow subgroup is trivial. We want to show $G = H$. Let F denote the fixed field of H, i.e. $F := L^H$. Then $\mathbb{R} \subseteq F \subseteq L$ and $F \subseteq L$ is a Galois extension with $\mathrm{Gal}(L/F) = H$. Thus $[L : F]$ is the maximal power of 2 dividing $|G| = [L : \mathbb{R}]$. Since $[L : \mathbb{R}] = [L : F][F : \mathbb{R}]$, it follows that $[F : \mathbb{R}]$ is odd. Let $\gamma \in F$ be a primitive element and let $f \in \mathbb{R}[x]$ be its minimal polynomial. If $F \neq \mathbb{R}$ then the degree of γ is an odd number, but by the intermediate value theorem we have since f is cubic it must have a real root. Hence f has a linear factor in $\mathbb{R}$ and thus f is not irreducible. Hence f has a linear factor in $\mathbb{R}$ and is thus not irreducible, contradicting the irreducibility of f. Thus we must have $\deg(f) = 1$, so $F = \mathbb{R}$, forcing $H = G$. (Note that using the intermediate value theorem to show that any odd-degree polynomial has a real root is the only piece of analysis in this proof.)

We now claim that in fact $|G| = 2$. Since $|G| = 2^n$, the corollary to the corollary gives us that there exists a chain of normal subgroups

$$1 = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$$

such that $G_k/G_{k-1} \cong \mathbb{Z}/(2)$ for all k. Then by the Galois correspondence, we have a chain of subgroups corresponding to the chain of subfields, namely

$$\mathbb{R} = L_n \subseteq L_{n-1} \subseteq \cdots \subseteq L_0 = L,$$

where $L_i = L^{G_i}$. Moreover, since $G_{k-1} \lhd G_k$, we have that $L_k \subseteq L_{k-1}$ is a Galois extension with $\mathrm{Gal}(L_{k-1}/L_k) = G_k/G_{k-1} = \mathbb{Z}/(2)$. Thus $L_k \subseteq L_{k-1}$ is a degree 2 extension for all k. We, therefore, have a chain of degree 2 extensions

$$\mathbb{R} = L_n \subseteq L_{n-1} \subseteq \cdots \subseteq L_0 = L.$$

It follows that $L_{n-1} \cong \mathbb{C}$. Since $\mathbb{C}$ has no degree 2 extensions by the quadratic formula, it follows that this terminates at L_{n-1}, so $n = 1$ as desired. Thus $G \cong (\mathbb{Z}/(2))^1 = \mathbb{Z}/(2)$. □

§2.9 Roots of Unity Revisited

Notation 2.65. The ***nth roots of unity*** are

$$\mu_n = \{z \in \mathbb{C} : z^n = 1\}.$$

For instance, $\mu_1 = \{1\}$, $\mu_2 = \{\pm 1\}$, $\mu_4 = \{\pm 1, \pm i\}$, etc.

Letting

$$\zeta_n := e^{2\pi i}/n,$$

we have $\mu_n = \{\zeta_n^k : 0 \leq k < n\}$, that is, $\mu_n = \langle \zeta_n \rangle$ is the cyclic group of order n generated by ζ_n. In other words, ζ_n generates the ***primitive*** nth roots of unity, which are elements of

$$\{\zeta_n^k : 0 \leq k < n, \gcd(k, n) = 1\}$$

2.9.1 Cyclotomic Fields

The ***nth cyclotomic field*** is $\mathbb{Q}[\mu_n] = \mathbb{Q}[\zeta_n]$. This is the splitting field for $x^n - 1 \in \mathbb{Q}[x]$, so $\mathbb{Q} \subseteq \mathbb{Q}[\mu_n]$ is a Galois extension.

Our goal is to prove $\mathrm{Gal}(\mathbb{Q}[\mu_n]/\mathbb{Q}) \cong (\mathbb{Z}/(n))^\times$. This is abelian, and although we won't prove it we present the following amazing and deep theorem.

Theorem 2.66: Kronecker-Weber.

If $\mathbb{Q} \subseteq K$ is a finite Galois extension with abelian Galois group $\mathrm{Gal}(K/\mathbb{Q})$ then $K \subseteq \mathbb{Q}[\mu_n]$ for some n.

For instance, this implies for all square-free $d \in \mathbb{Z}$ that $\mathbb{Q}[\sqrt{d}] \subseteq \mathbb{Q}[\mu_n]$ for some n. We will prove this directly. Of course, $\mathrm{Gal}(\mathbb{Q}[\mu_n]/\mathbb{Q})$ acts on μ_n. What are the orbits? We claim

$$\text{orbits} \longleftrightarrow \text{irreducible factors of } x^n - 1.$$

Example 2.67. For instance

- $x^1 - 1$ is irreducible and $\mu_1 = \{1\}$.
- $x^2 - 1 = (x+1)(x-1)$, $\mu_2 = \{\pm 1\}$. The Galois group of $\mathbb{Q}[\mu_2] = \mathbb{Q}$ over $\mathbb{Q}$ is trivial, so two orbits.
- $x^4 - 1 = (x^2+1)(x+1)(x-1)$. $\mathbb{Q}[\mu_4] = \mathbb{Q}[i]$. $\mathrm{Gal}(\mathbb{Q}[u]/\mathbb{Q}) \cong C_2$, with generator complex conjugation. Then the orbits are $\{\pm i\}$, $\{1\}$, and $\{-1\}$ (the latter two meaning the orbit is just fixing it)
- $x^p - 1$ for p prime has
$$x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \cdots + 1).$$
Recall that if $\phi_p = x^{p-1} + \cdots + 1$ then we proved $\phi_p(x+1)$ is Eisenstein at $p = 2$, so $\phi_p(x+1)$ and hence ϕ_p is irreducible. It follows that the Galois group acts transitively on the roots of $x^{p-1} + \cdots + 1$. It follows that the Galois group acts transitively on the roots of $x^{p-1} + \cdots + 1 = \phi_p$ since all have the same minimal polynomial (Why?). Thus the orbits on μ_p are $\{1\}$ and the roots of ϕ_p, i.e. the primitive pth roots of unity.

Define

$$\Phi_n := \prod_{\substack{\zeta \in \mu_n \\ \zeta \text{ primitive}}} (x - \zeta).$$

The Galois group of $\mathbb{Q}[\mu_n]$ permutes the primitive nth roots of unity, so it must fix the coefficients of Φ_n. Hence $\phi_n \in \mathbb{Q}[x]$ since the only elements of $\mathbb{Q}[\mu_n]$ fixed by the Galois group are the base field $\mathbb{Q}$. Thus Φ_n is a factor of $x^n - 1 \in \mathbb{Z}[x]$ in $\mathbb{Q}[x]$, so by Gauss's lemma on factoring we have $\Phi_n \in \mathbb{Z}[x]$.

Theorem 2.68.

Φ_n is irreducible for all $n \geq 1$.

Proof. (Van der Waerden? Emmy Noether?) We first need an auxiliary lemma.

Lemma 2.69.

Let $\zeta \in \mu_n$ and p be a prime not dividing n. Let $f \in \mathbb{Q}[x]$ be the minimal polynomial for ζ. Then f is also the polynomial of ζ^p.

Proof. Assume this is false, so $f(\zeta) = 0$ but $f(\zeta^p) \neq 0$. If $g \in \mathbb{Z}[x]$ is the minimal polynomial for ζ^p then $g \neq f$ then f and g are distinct factors of $x^n - 1$. Thus we can find $h \in \mathbb{Z}[x]$ such that $x^n - 1 = fgh$. Reducing modulo p, we have $\overline{x}^n - 1 = \overline{f}(x)\overline{g}(x)\overline{h}(x)$ in $\mathbb{F}_p[x]$. p does not divide n, so the derivative of $\overline{x}^n - 1$ is nonzero. Hence $\overline{x}^n - 1$ has no repeated roots in $\overline{\mathbb{F}_p}[x]$. It follows that (†) $\overline{f}$ and $\overline{g}$ are relatively prime in $\mathbb{F}_p[x]$.

We now show that this is a problem. We have $g(\zeta^p) = 0$ implies ζ is a root of $g(x^p)$, so since f is the minimal polynomial of ζ we have that f divides $g(x^p)$ in $\mathbb{Z}[x]$.

Write $g(x^p) = f(x)\varphi(x)$ for some $\varphi \in \mathbb{Z}[x]$. Again reducing modulo p, we find that $\overline{f}(x)\overline{\varphi}(x) = \overline{g}(x^p)$, which by the Freshman's dream is $(\overline{g}(x))^p \in \mathbb{F}[x]$. This contradicts (†), which says $\gcd(\overline{f}, \overline{g}) = 1$. □

Recall that $\Phi_n(x) = \prod_{\substack{\zeta \in \mu_n \\ \zeta \text{ primitive}}} (x - \zeta) \in \mathbb{Z}[x]$ and also recall that $\zeta_n = e^{2\pi i/n}$. We now return to the proof of the theorem that Φ_n is irreducible for all $n \geq 1$, so $\mu_n = \{\zeta_n^a : 0 \leq a < n, \gcd(a, n) = 1\}$. It suffices to show all such ζ_n^a have the same minimal polynomial.

Write a as a product of primes p_i, i.e. $a = p_1 \cdots p_r$, where $p_i \nmid n$. By the lemma we know that the following have the same minimal polynomial: ζ_n, $\zeta_n^{p_1}$, $\zeta_n^{p_1 p_2}$, $\ldots$, $\zeta_n^{p_1 \cdots p_r} = \zeta_n^a$, completing the proof. □

The above theorem would be insane without Galois theory. Although the theorem doesn't use the Galois correspondence, we used properties of the orbits of the Galois group.

Corollary 2.70.

The irreducible factorization of $x^n - 1 \in \mathbb{Q}[x]$ is

$$x^n - 1 = \prod_{d|n} \Phi_n(x).$$

Proof. We have

$$x^n - 1 = \prod_{\zeta \in \mu_n} (x - \zeta)$$

$$= \prod\nolimits_{d|n} \Big(\prod\nolimits_{\zeta \in \mu_d, \zeta \text{ primitive}} (x - \zeta) \Big) = \qquad = \prod\nolimits_{d|n} \Phi_d(x).$$

(each $\zeta \in \mu_n$ is a primitive dth root of unity for some $d \mid n$)

□

Example 2.71. $x^6 - 1 = \Phi_1\Phi_2\Phi_3\Phi_6 = (x-1)(x+1)(x^2+x+1)(x^2-x+1)$, the last factor reelfecting the fact that there are exactly two primitive sixth roots of unity, those being ζ_6, ζ_5.

Our goal is to compute $G := \mathrm{Gal}(\mathbb{Q}[\mu_n]/\mathbb{Q})$. $\mathbb{Q}[\mu_n]/\mathbb{Q}$ is Galois since it is the splitting field for $x^n - 1$ over $\mathbb{Q}$. We first start by analyzing things we know about this extension:

Lemma 2.72.

If $\sigma \in G$ then $\sigma(\zeta) = \zeta^a$ for all $\zeta \in \mu_n$ and some $a \geq 1$ with $\gcd(a, n) = 1$

Proof. We have $\sigma(\zeta_n)^n = \sigma(\zeta^n)_n) = \sigma(1) = 1$ and $\sigma(\zeta_n)^k \neq 1$ for $1 \leq k \leq n$, so $\sigma(\zeta_n)$ is a primitive nth root of unity. Hence $\sigma(\zeta_n) = \zeta_n^a$ for some $a \geq 1$ with $\gcd(a, n) = 1$. All other $\zeta \in \mu_n$ are $\zeta = \zeta_n^k$ for some k, so

$$\sigma(\zeta) = \sigma(\zeta_n^k) = (\zeta_n^a)^k = \zeta^a.$$

This completes the proof □

Note that this is well-defined modulo n and sits in $(\mathbb{Z}/(n))^\times$ since $\gcd(a, n) = 1$. We will write $a(\sigma) := a \in (\mathbb{Z}/(n))^\times$.

Lemma 2.73.

The map $G \to (\mathbb{Z}/(n))^\times$ by $\sigma \mapsto \sigma(a)$ is an injective homomorphism.

Proof. $\sigma_1, \sigma_2 \in G$ and $a(\sigma_1\sigma_2)$ is characterized by $(\zeta_n^{a(\sigma_2)})^{(a\sigma_1)} = \sigma_1(\zeta_n^{a(\sigma_2)}) = \sigma_1\sigma_2(\zeta_n) = \zeta_n^{a(\sigma_1\sigma_2)}$. □

Thus $a(\sigma_1\sigma_2) = a(\sigma_2)a(\sigma_1)$, so it is a homomorphism. It is injective since for $\sigma \in G$ in the kernel we have $1 = \sigma(\zeta_n) = \zeta_n^{a(\sigma_1)}$, so $a(\sigma)$ is identically zero modulo n.

Corollary 2.74.

$G := \mathrm{Gal}(\mathbb{Q}[\mu_n]/\mathbb{Q})$ is abelian.

Remark 2.75. The same proof works to show that for any perfect field for K that $\mathrm{Gal}(K[\mu_n]/K) \hookrightarrow (\mathbb{Z}/(n))^\times$ is abelian. Of course, $K[\mu_n]/K$ is also a Galois extension (because it is the splitting field for $x^n - 1$ over K).

However, the following theorem is special for $\mathbb{Q}$:

Theorem 2.76.

For any $n \geq 1$ we have

$$\mathrm{Gal}(\mathbb{Q}[\mu_n]/\mathbb{Q}) \cong (\mathbb{Z}/(n))^\times$$

Proof. The primitive nth roots of unity are given by $\{\zeta_n^a : a \geq 1, \gcd(a,n) = 1\}$, i.e. $a \in (\mathbb{Z}/(n))^\times$. Thus what we want to show is that for any primitive nth root of unity ζ, there exists a $\sigma \in G$ with $\sigma(\zeta_n) = \zeta$. But this follows from the fact that ζ_n and ζ are both roots of the irreducible polynomial Φ_n, i.e. have the same minimal polynomial over $\mathbb{Q}$. □

Remark 2.77. More on the proof: For primitive $\zeta \in \mu_n$, $\mu_n = \{\zeta^k : k \geq 1\}$, so

$$\mathbb{Q}[\mu_n] = \mathbb{Q}[\zeta] \cong \mathbb{Q}[x]/(\Phi_n), \qquad \text{(minimal polynomial of } \zeta \text{ is } \Phi_n)$$

and the same is true for ζ_n, so the element of G that we seek is

$$\mathbb{Q}[\mu_n] = \mathbb{Q}[\zeta_n] \cong \mathbb{Q}[x]/(\Phi_n) \cong \mathbb{Q}[\zeta] = \mathbb{Q}[\mu_n]$$

Remark 2.78. The above theorem is *false* if $\mathbb{Q}$ is replaced by, say, $\mathbb{R}$. For $n \geq 3$, $\mathbb{R}[\mu_n]$, $\zeta_n \in \mathbb{C} \setminus \mathbb{R}$, so $\mathbb{R}[\mu_n] = \mathbb{C}$ and $\mathrm{Gal}(\mathbb{R}[\mu_n]/\mathbb{R}) \cong C_2$ since we're just reproducing the complex numbers, i.e. $|\mathbb{R}[\mu_n] : \mathbb{R}| = 2$.

This is a nice concrete place to think about subgroups of the Galois group and intermediate fields.

Example 2.79 (Example of the Galois Correspondence)**.** Let p be an odd prime and $G := \mathrm{Gal}(\mathbb{Q}[\mu_p]/\mathbb{Q}) \cong (\mathbb{Z}/(p))^\times$ the cyclic group of order $p-1$ generated by some $t \in (\mathbb{Z}/(p))^\times$.

$$(\mathbb{Z}/(p))^\times = \{t^k : k \geq 1\}$$

This contains an index 2 subgroup H, where

$$H = \{t^{2k} : k \geq 1\} \subseteq G$$

It is normal since it has index 2 (or alternatively since G is abelian). Let F be the fixed field $F = (\mathbb{Q}[\mu_p])^H$. Then $\mathbb{Q} \subseteq F \subseteq \mathbb{Q}[\mu_p]$, and $\mathbb{Q} \subseteq F$ is a Galois extensions (which follows from the fact that H is a normal extension) with

$$\mathrm{Gal}(F/\mathbb{Q}) \cong G/H \cong C_2,$$

meaning $\mathbb{Q} \subseteq F$ is a quadratic extension. In other words, we have the following theorem.

Theorem 2.80.

In the above notation, if $p \equiv 1 \pmod 4$ then $F = \mathbb{Q}[[\sqrt{p}]$.

If $p \equiv 3 \pmod 4$ then $F = \mathbb{Q}[\sqrt{-p}]$.

Proof. Rather than providing the proof in whole, we give a special case. The whole proof is the special case but with more cumbersome notation.

Example 2.81 ($p = 7$)**.** If $p = 7$ then $p \equiv 3 \pmod 4$, so we should get $F = \mathbb{Q}[\sqrt{-7}$. $G = \mathrm{Gal}(\mathbb{Q}[\mu_n]/\mathbb{Q}) \cong (\mathbb{Z}/(7))^\times$ is a cyclic group of order 6 generated by 3, namely

$$G = \langle 3 \rangle = \{3, 2 = 9, 6, 4 = 18, 5 = 12, 11 = 15\},$$

so our subgroup H is generated by $3^2 = 9$ to get

$$H = \langle 9 \rangle = \{2, 4, 1 = 8\}.$$

Then $F = \mathbb{Q}[\mu_7]^H$ is generated by $\alpha_1 = \zeta_7 + \zeta_7^2 + \zeta_7^4$,

(??) and the powers not in H are summed in $\alpha_2 = \zeta_7^3 + \zeta_7^5 + \zeta_n^6$(??).

Recall that $x^7 - 1 = (x-1)(x-\zeta_7)(x-\zeta_7)^2 \cdots (x-\zeta_7)^6$, and expanding this out we find $\alpha_1 + \alpha_2 = -1$ since $1 = \zeta_7^0 + \alpha_1 + \alpha_2 = -(\text{coefficient of } x^p - 1 \text{ in } x^7 - 1) = 0$.

The product $\alpha_1\alpha_2 = (\zeta_7 + \zeta_7^2 + \zeta_7^4)(\zeta_7^3 + \zeta_7^5 + \zeta_7^6)$. Expanding this out we get this is equal to $2\zeta_7^0 + (\zeta_7^0 + \zeta_7^1 + \cdots + \zeta_7^6) = 2$. This implies that $(x - \alpha_1)(x - \alpha_2) = x^2 + x + 2$. Therefore, using the quadratic formula on $x^2 + x + 2$ knowing that the roots must be α, we find $\alpha_1, \alpha_2 = \frac{-1 \pm \sqrt{1-8}}{2} = \frac{-1 \pm \sqrt{-7}}{2}$.

Exercise 2.82. Note that Artin does two more numerical examples and they are worth looking at. It would be useful to look at these to see how this works and get a feeling for the Galois correspondence.

□

If we were to be able to continue to develop Galois theory, we need to look at ***class field theory***, which classifies abelian (i.e. abelian Galois group) extensions of nice fields K (e.g. $K = \mathbb{Q}$ on a finite extension of $\mathbb{Q}$). This is the crowning achievement of early 20th-century developments in this field.

Informally, the ***Langlands program*** is an attempt to generalize class field theory from abelian extensions to non-abelian extensions! What we will talk about today is a baby case, i.e. the easiest case of this. This is called ***Kummer theory***.

For fields K of characteristic zero (there is another theory by a different name for the characteristic p version of this) such that K contains a primitive nth root of unity, this classifies Galois extensions $K \subseteq L$ such that $\mathrm{Gal}(L/K)$ is abelian and all elements $g \in \mathrm{Gal}(L/K)$ satisfy $g^h = \mathrm{id}$. We won't do this today—if we had an extra lecture we would. But we will do the easiest case of this—the one in which the Galois group is cyclic.

Our goal: Understand such extensions $K \subseteq L$ such that $\mathrm{Gal}(L/K) \cong C_n$.

Definition 2.83 (character)**.** For an abelian group G and a field K, a ***character*** of G is a homomorphism $\chi : G \to K^\times$ $(= K \setminus \{0\})$.

Example 2.84. For any nonzero $a \in K$ we have a character (letting $G = K^\times$, which is of course an abelian group since multiplication is commutative) $\chi : K^\times \to K^\times$ via $\chi(x) := ax$.

Given a field extension $K \subseteq L$ and $\sigma \in \mathrm{Gal}(L/K)$, we can define a character $\chi : L^\times \to L^\times$ with $\chi(x) := \sigma(x)$.

Example 2.85. For a prime p, we have a character $\chi : (\mathbb{Z}/(p))^\times \to \{\pm 1\}$ $(\subseteq \mathbb{C}^\times)$ such that $\chi(x)$ is given by a ***Legendre symbol***, i.e.

$$\chi(x) := \left(\frac{x}{p}\right) = \begin{bmatrix} 1 & \text{if } x \text{ is a square} \\ -1 & \text{otherwise} \end{bmatrix}$$

Showing this is a homomorphism is an exercise.

We have the following wonderful fact about characters thanks to Dedekind, which comes with a beautiful proof:

Theorem 2.86: Dedekind.

Let G be an abelian group and K be a field. Suppose $\chi_1, \ldots, \chi_n :\to K^\times$ be *distinct* characters. Then the χ_i are linearly independent, i.e. if $c_1, \ldots, c_n \in K$ satisfy

$$c_1\chi_1(g) + \cdots + c_n\chi_n(g) = 0$$

for all $g \in G$, then $c_1 = \cdots = c_n = 0$.

Proof. Suppose otherwise. Choose $c_1, \ldots, c_n$ so that

$$c_1\chi_1 + \cdots + c_n\chi_n = 0 \tag{$\dagger$}$$

but the c_i are not all zero such that there is the minimal number of nonzero c_i.

Since $\chi_i \neq 0$ (by definition of a character), there must be at least two nonzero c_i. Relabel the indices such that $c_1 \neq 0$ and $c_2 \neq 0$. The χ_i are distinct, so $\chi_1 \neq \chi_2$; then we can find $h \in G$ such that $\chi_1(h) \neq \chi_2(h)$.

For $g \in G$, we have

$$\begin{aligned} 0 &= c_1\chi_1(hg) + \cdots + c_k\chi_n(hg) \\ &= c_1\chi_1(h)\chi_1(g) + \cdots + c_n\chi_n(h)\chi_n(g). \end{aligned}$$

Then

$$c_1\chi_1(h)\chi_1 + c_2\chi_2(h)\chi_2 + \cdots + c_n\chi_n(h)\chi_n = 0. \tag{$*$}$$

Multiplying through $(\dagger)$ by $\chi_1(h)$ $(\neq 0)$ gives that

$$c_1\chi_1(h)\chi_1 + c_2\chi_1(h)\chi_2 + \cdots = 0. \tag{$**$}$$

Subtracting $(*)$ from $(**)$ gives us that

$$0\chi_1 + c_2(\chi_1(h) - \chi_2(h))\chi_2 + \cdots = 0.$$

This has *fewer* nonzero coefficients than $(\dagger)$. By minimality, *all* coefficients of this must be zero. In particular, $c_2(\chi_1(h) - \chi_2(h)) = 0$. Since $\chi_1(h) \neq \chi_2(h)$, this implies that $c_2 = 0$, a contradiction. □

Example 2.87. For *distinct* nonzero $a_1, \ldots, a_n \in K$, looking at the characters $\chi_i : \mathbb{Z} \to K^\times$, $\chi_i(k) = a_i^k$ (which is indeed a character since it is a group homomorphism), we conclude that only $c_1, \ldots, c_n \in K$ such that

$$c_1 a_1^k + \cdots + c_n a_n^k = 0$$

for all $k \in \mathbb{Z}$ are $c_1 = \cdots = c_n = 0$.

The following corollary of linear independence of characters is the baby version of Hilbert's theorem 90:

The reason this is called Hilbert's theorem 90 is that he write an account of number theory/Galois theory as were known at the time. In this piece, his theorems were numbered consecutively, and this (a more generalized version of this) was the 90th one.

The real version says that, given a field with cyclic Galois extension, characterizes when you can write element of the field of quotient sigma(x)/x, and the condition is when the "absolute norm" of the element is one (which the roots of unity have).

Corollary 2.88: Baby Hilbert's Theorem 90.

Let K be a field and ζ_n a primitive nth root of unity. Consider the Galois extension $K \subseteq L$ such that $\mathrm{Gal}(L/K) \cong C_n$, generated by σ. Then there exists $x \in L$ such that

$$\zeta_n = \frac{\sigma(x)}{x}.$$

Proof. Regard L as a vector space over K. The automorphism $\sigma : L \to L$ is K-linear since for all $c \in K$ and $x, y \in L$ we have $\sigma(x+y) = \sigma(x) + \sigma(y)$ and $\sigma(cx) = \sigma(c)\sigma(x) = c\sigma(x)$, the last equality since $\sigma|_K = \mathrm{id}$.

What we need to show is that ζ_n is an eigenvalue of σ (since then $\sigma(x) = \zeta_n x$, giving the result).

Let $p \in K[x]$ be the minimal polynomial of σ. Since $\sigma^n = \mathrm{id}$ (because the Galois group is cyclic of order n, i.e. isomorphic to C_n), we have $\sigma^n - 1 = 0$. So $p(x)$ divides $x^n - 1$.

We now claim $p(x) = x^n - 1$. Indeed, this follows from the linear independence of characters—$\sigma^0 = \mathrm{id}, \sigma^1, \ldots, \sigma^{n-1} : L \to L$ are distinct characters since σ generates $\mathrm{Gal}(L/K) \cong C_n$. Thus they're linearly independent, so we cannot find $c_0, \ldots, c_{n-1} \in K$ such that when $c_0 + c_1\sigma^1 + \cdots + c_{n-1}\sigma^{n-1} = 0$ we have $c_0, \ldots, c_{n-1}$ are not all zero. Thus the minimal polynomial p has degree *at least* n, so $p(x) = x^n - 1$. But this implies $|L : K| = n$, so $\dim_K(L) = n$, so it follows that the characteristic polynomial of σ must be $x^n - 1$.

Then since the characteristic polynomial of σ has degree n, by Cayley-Hamilton, we know since $f(\sigma) = 0$. In particular, ζ_n is a *root* of the characteristic polynomial, and hence an eigenvalue. □

Recall Baby Hilbert 90 shows how the Galois group of a cyclic extension acts.

Corollary 2.89.

If K is a field and $\zeta_n \in K$ a primitive nth rot of unity and $K \subseteq L$ with $\mathrm{Gal}(L/K) \cong \mathbb{Z}/(n)$ then there exists some $a \in K$ such that

$$L = K[\sqrt[n]{a}]$$

Proof. Let σ be a generator of the Galois group $\mathrm{Gal}(L/K)$. Then by Hilbert 90 there exists an $t \in L^\times$ with $\sigma(t) = \zeta_n t$. Thus $\sigma(t^n) = (\sigma(t))^n = \zeta_n^n t^n = t^n$. σ generates the Galois group, so t^n is fixed by the Galois group. But then t^n must sit in the base field since σ (which generates the whole Galois group) fixes it and hence all of the Galois group fixes it.

Let $a = t^n$, i.e. $t = \sqrt[n]{a}$. Then we have $K \subseteq K[t] = K[\sqrt[n]{a}]$, it is enough to prove that $K \subseteq K[t]$ is an extension of degree n. The element t is a root of $x^n - a$. To show $K \subseteq K[t]$ has degree n, we need to show $x^n - a$ is the minimal polynomial of t. We can factor

$$x^n - a = (x-t)(x-\zeta_n t)(x-\zeta_n^2 t)\cdots(x-\zeta_n^{n-1}t).$$

But $\zeta_i t = \sigma^i(t)$ by observation of the definitions of t and σ, so the above becomes

$$x^n - a = (x-t)(x-\sigma(t))(x-\sigma^2(t))\cdots(x-\sigma^{n-1}(t)).$$

If this could factor, then the roots of the factorization must be permuted by $\mathrm{Gal}(L/K)$. But σ fixes them, so we conclude that we cannot nontrivially factor, so $x^n - a$ is irreducible, as desired. □

Remark 2.90. The converse is *almost* true. More precisely, we can show that if K is a field containing a (primitive) nth root of unity and $a \in K$ then $K \subseteq K[\sqrt[n]{a}]$ is a Galois extension with Galois group $\mathbb{Z}/(m)$ for some m dividing n.

Proof. Probably on the final exam (with hints, though not that hard). □

§2.10 Inverse Galois Problem

The ***inverse Galois problem*** is a famous open problem that asks the following question: For any finite group G, do there exist finite extensions $\mathbb{Q} \subseteq K$ such that $\mathrm{Gal}(K/\mathbb{Q}) = G$?

If we are free to choose any field instead of $\mathbb{Q}$ then this is not hard to show. Though some things are known here, we will focus on explaining the baby case of this.

If $\mathbb{Q} \subseteq K$ is a Galois extension of degree n with primitive element $a \in K$, so $K = \mathbb{Q}[a]$, then letting $f(x)$ be the minimal polynomial of a, the Galois group acts transitively on the roots $\{a_1, \ldots, a_n\}$ of $f(x)$. $f(x)$ is then a degree n polynomial and has at least one root $a = a_1$. This gives a group homomorphism $\varphi : \mathrm{Gal}(K/\mathbb{Q}) \to S_n$. This is injective since if $\sigma \in \ker\varphi$ then $\sigma(a) = a$, so $\sigma = \mathrm{id}$ since $K = \mathbb{Q}[a]$. The image of φ is a transitive subgroup of S_n, and so we ask the question: Can φ be surjective (so that $\mathrm{Gal}(K/\mathbb{Q}) = S_n$)?

The answer is yes! This is the first case of the inverse Galois problem that was solved, and this was even known in the nineteenth century. However, the proofs of this are still very complicated (e.g. look it up). So, we will just prove a special case of this:

Theorem 2.91: Subcase of a Special Case of the Inverse Galois Problem.

Fix a prime p. Let $f \in \mathbb{Q}[x]$ be an irreducible polynomial of degree p such that f has $p-2$ real roots and 2 (complex conjugate) roots, counting multiplicities. If K is the splitting field of f, then $\mathrm{Gal}(K/\mathbb{Q}) \cong S_p$.

Proof. Set $G := \mathrm{Gal}(K/\mathbb{Q})$. Then $G \leq S_p$ (when both are understood by their actions on the roots of f). We have $|G| = |K : \mathbb{Q}|$ from the characterization of a Galois extension. Letting the roots of f be $\left\{a_1, \ldots, a_{p-2}, b, \overline{b}\right\}$, we know that $\mathbb{Q} \subseteq \mathbb{Q}[a_1]$ has degree p (since f is the monomial polynomial of a). $\mathbb{Q} \subseteq \mathbb{Q}[a_1] \subseteq K$, we conclude that the degree of the extension $\mathbb{Q} \subseteq K$ is divisible by p, so p divides $|G|$ by the first Sylow theorem. Hence G has an element of order p.

Recall that every element of S_p has a decomposition into cycles —e.g. in S_5, writing elements in the fashion of $(2,3)(1,4,5))$, which has order $\mathrm{lcm}(2,3) = 6$. Since p is a prime, the only element of order p in S_p is a p-cycle, so we know G contains a p-cycle.

We also know that G contains an involution since complex conjugation is an element of G which fixes $a_1, \ldots, a_{p-2}$ (since these are the real roots as we said in the beginning)., and ϕ and $\overline{\phi}$, i.e.. is a 2-cycle.

It follows from this that it suffices to show for prime p that $\sigma \in S_p$ a p-cycle and $\tau \in S_p$ a transposition.

We can choose the ordering on $\{1, \ldots, p\}$ such that $\sigma = (1, 2, \dot{;}p)$ and $\tau = (i, j)$ for some $1 \leq i < j \leq p$.

Then considering the group generated by $G := \sigma, \tau$, i.e. $\langle \sigma, \tau \rangle$, it suffices to show that G contains all transpositions.. $\sigma(1, \ldots, p)(i, j)(1, \ldots, p) = (i+1, j+1) \in G$, so $\sigma^k \tau \sigma^{-k} = (i+j, j+k) \in G$. Translating all the way to the left, we have for $m = j - i$ that $(1, m) \in G$. We also have $(m, 2m-1) \in G$. Since $(m, 2m-1)(1, m) = (1, 2m-1)$. We have $(1, 2m-1) \in G$. This can be shifted to give $(2m-1, 3m-2)$ since we added $m-1$ to it, so $(2m-1, 3m-2)(1, 2m-1) = (1, 3m-2 \in G$. Repeating this process, we get $(1, cm - c + 1) \in G$, and $cm - c + 1 = c(m-1) + 1$ for all c. Since p is prime and $m - 1 \not\equiv 0 \pmod{p}$, we can find c such that $c(m-1) + 1 \equiv 2 \pmod{p}$. Thus $(1, 2) \in G$, shifting we can get $(2, 3) \in G$, $(3, 4) \in G<$ etc., with adjacent transpositions. For $1 \leq a < b \leq p$, we have $(a, b) = (b-1, b)(b-2, b-2) \cdots (a, a+1)$. □

Last time we constructed a Galois extension $\mathbb{Q} \subseteq K$ such that $\mathrm{Gal}(K/\mathbb{Q}) \cong S_p$ for a given prime p. The other thing we did was to show a field K containing a primitive nth root of unity and a Galois extension $K \subseteq L$ with $\mathrm{Gal}(L/K) \cong C_n$, there exists an $a \in L$ such that $L = K[\sqrt[n]{a}]$. We also asserted the following lemma:

Lemma 2.92.

Let K be a field and $\zeta_n \in K$ be a primitive nth root of unity. Let $a \in K$ and let $L = K[\sqrt[n]{a}]$. Then $K \subseteq L$ is Galois, and $\mathrm{Gal}(L/K) \cong C_m$ for some m with $m \mid n$.

Proof. $K \subseteq L$ is a Galois extension since it is generated by the nth root of a and is a splitting field for $x^n - a$ since

$$x^n - a = \prod\nolimits_{k=0}^{n-1} (x - \zeta_n^k t).$$

For $\sigma \in \mathrm{Gal}(L/K)$, we have $\sigma(t) = \zeta_n^{\varphi(\sigma)} t$ for some $\varphi(\sigma) \in C_n$. For $\sigma_1, \sigma_2 \in \mathrm{Gal}(L/K)$, we have

$$\zeta_n^{\varphi(\sigma_2)+\varphi(\sigma_1)} t = \zeta_n^{\varphi(\sigma_2)} \zeta_n^{\varphi(\sigma_1)} t = \zeta_n^{\varphi(\sigma_2)} \varphi(t) = \sigma_1(\zeta_n^{\varphi(\sigma_2)} t) = \sigma_1\sigma_2(t) = \zeta_n^{\varphi(\sigma_1\sigma_2)} t,$$

so $\varphi(\sigma_1\sigma_2) = \varphi(\sigma_1) + \varphi(\sigma_2)$, i.e. $\varphi : \mathrm{Gal}(L/K) \to C_2 \cong \mathbb{Z}/(n)$ is a group homomorphism. φ is injective since $\sigma \in \ker(\varphi)$. We must fix t, so fixes $L = K[t]$ for $t = \sqrt[n]{a}$ and $\sigma = \mathrm{id}$. Thus $\mathrm{Gal}(L/K) \cong \mathrm{im}(\varphi) \subseteq \mathbb{Z}(n)$, so isomorphic to $\mathbb{Z}/(m)$ for some $m \mid n$ since the subgroups of $\mathbb{Z}/(n)$ are exactly these. □

This is all the beginnings of Kummer theory.

§2.11 Insolvability of the Quintic

2.11.1 Solvable Galois Extensions

A Galois extension $\mathbb{Q} \subseteq L$ is ***solvable*** if there exists a sequence of Galois extensions

$$\mathbb{Q} \subseteq K_0 \subseteq K_1 \subseteq \cdots \subseteq K_r = L$$

such that for $1 \leq i \leq r$, there is some element $a \in K_{i-1}$ and $n_i \geq 2$ such that $K_i = K_{i-1}[\sqrt[n_i]{a}]$. This should remind the reader of Kummer theory.

We say a polynomial $f \in \mathbb{Q}[x]$ is ***solvable*** if the splitting field of f is solvable.

Example 2.93. The quadratic formula implies that all degree two $f \in \mathbb{Q}[x]$ are solvable.

Example 2.94. The solution to the cubic shows that for a degree three polynomial $f \in \mathbb{Q}[x]$, the splitting field of f is of the form

$$\mathbb{Q} \subseteq \mathbb{Q}[\Delta(f)] \subseteq (\mathbb{Q}[\Delta(f)])[\sqrt[3]{-}],$$

so f is solvable.

More generally, solvability for f is a precise way of saying that there is some formula for the roots of $f(x)$ just involving iterated taking of n_ith roots for some n_is.

2.11.2 The Quintic

Our final goal this semester is to give a group-theoretic condition that completely characterizes the Galois group of $L/\mathbb{Q}$ is equivalent to $\mathbb{Q} \subseteq L$ being solvable (this condition is what we will see the notion of a solvable group is, cf. below). We will prove two things: that every subgroup of S_4 is solvable (and so there exists a "formula" for the solution of a degree 4 polynomial), but no S_n is solvable for $n \geq 5$ (and consequently for degree 5 polynomials f with splitting field S_5 there is no "formula" for the roots of a degree 5 polynomial).

Our goals:

1. Find group theoretic condition for solvability (which will remind us of Kummer theory and actually use Kummer theory to prove that it is equivalent to solvability in the polynomial sense)
2. Every subgroup of S_4 is solvable
3. Prove for each $n \geq 5$ that S_n is not solvable.

Definition 2.95 (solvable group)**.** A group G is ***solvable*** if there exists a sequence of subgroups

$$1 = G_0 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_r = G$$

such that G_{k+1}/G_k is abelian for all $0 \leq k \leq r-1$.

Example 2.96. Obviously, any abelian group is solvable. Meanwhile, the only abelian symmetric groups are S_1 and S_2.

Example 2.97. S_3 is solvable. Recall that $A_3 = \ker(S_3 \ni \sigma \overset{\text{sign}}{\longmapsto} \{\pm 1\})$. Recall that $A_3 \cong C_3$ and is generated by the cycle (123).

Then notice that

$$1 \lhd A_3 \lhd S_3$$

and $S_3/A_3 \cong C_2$, $A_3/(1) \cong C_3$, all of which are abelian, so S_3 is solvable.

Example 2.98. S_4 is solvable. Note $A_4 = \ker(S_4 \ni \sigma \overset{\text{sign}}{\longmapsto} \{\pm 1\})$. Set

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

Then V is a subgroup, e.g. $((12)(34))((13)(24)) = (14)$. In fact, for $\sigma_1, \sigma_2 \in V$ that are not the identity, we have that $\sigma_1\sigma_2 = \sigma_3$, where $V = \{1, \sigma_1, \sigma_2, \sigma_3\}$. Thus $V \cong C_2 \oplus C_2$, the Klein-4 group, and is abelian. In fact, $(12)(34) \mapsto (1,0)$, $(13)(24) \mapsto (0,1)$, $(14)(23) \mapsto (1,1)$.

Observe that V is a normal subgroup of S_4 and hence also of A_4. V is a normal subgroup of S_4 (and hence also of A_4), e.g. for $\sigma \in S_4$ we have

$$\sigma(12)(34)\sigma^{-1} = (\sigma(1)\sigma(2))(\sigma(3)\sigma(4)).$$

We have $|A_4| = 12$ and $|V| = 4$, so $|A_4/V| = 2$, so $A_4/V \cong \mathbb{Z}/(3) \cong C_3$, which is abelian. Thus

$$1 \lhd V \lhd A_4 \lhd S_4$$

and $S_4/A_4 \cong C_2$, $A_4/V \cong C_3$, $V/1 \cong C_2 \oplus C_2$, all of which are abelian, so S_4 is solvable.

Lemma 2.99.

If G is a solvable group then any subgroup H of G is solvable.

Proof. Let G be solvable. Then there's a chain

$$1 = G_0 \lhd G_1 \lhd \cdots \lhd G_r = G$$

such that G_i/G_{i-1} is abelian for each $1 \leq i \leq r-1$. Then by the (group) isomorphism theorems, we have

$$1 = G_0 \cap H \lhd G_1 \cap H \lhd \cdots \lhd G_r \cap H$$

and also that $(G_i \cap H)/(G_{i-1} \cap H)$ is a subgroup of G_i/G_{i-1}, the latter being abelian. Subgroups of abelian groups are abelian, so H is solvable by definition. □

Note that the following lemma is *false* for *infinite* solvable groups:

Lemma 2.100.

Let G be a *finite* solvable group. Then there exists a chain of subgroups

$$1 = G_0 \lhd G_1 \lhd \cdots \lhd G_r = G.$$

such that each G_i/G_{i-1} is *cyclic*. We call groups G with this property ***polycyclic groups***.

Proof. For any finite abelian group H, we can find a chain $1 = H_0 \lhd H_1 \lhd \cdots \lhd H_s = H$ such that each H_i/H_{i-1} is cyclic. (e.g. $H = C_2 \oplus C_2$ with $1 \lhd C_2 \times \{0\} \lhd C_2 \oplus C_2$).

We can thus find a chain

$$G_{i-1} = G_{i-1}^0 \lhd G_{i-1}^1 \lhd \cdots \lhd G_{i-1}^{s(i)} = G_i$$

such that each G_i^j/G_i^{j-1} is cyclic (just as above on G_i/G_{i-1}, since we can find such chains in the quotient and then just pull them back). Add those to our chain. □

Next time we'll show that S_5 is not solvable, and the problem comes from the fact that there are no subgroups of A_5 since A_5 is a simple group.

Recall that a group G is solvable if it has a solvable series, that is, groups

$$1 = G_0 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_r = G$$

such that each G_i/G_{i-1} is abelian. We have seen several examples of solvable groups, so it is time we present a (very important) non-example:

Theorem 2.101.

S_n is not a solvable group for any $n \geq 5$.

Proof. It is enough to show that

1. The only $H \lhd S_n$ such that $H \neq S_n$ with S_n/H abelian is $H = A_n$.
2. There does not exist $H \lhd A_n$ with $H \neq A_n$ and A_n/H abelian.

For 1: Consider a homomorphism $\varphi : S_n \to \Gamma$ for some abelian group Γ. It is enough to show $A_n \subseteq \ker(\varphi)$ (since kernels are normal subgroups). (This is true for all $n \geq 2$.) To show $A_n \subseteq \ker(\varphi)$, it suffices to show that for all transpositions (i, j) and (k, ℓ) we have that

$$\varphi((i, j)(k, \ell)) = 0.$$

Pick $\sigma \in S_n$ such that $\sigma(i) = k$, $\sigma(j) = \ell$. Together with the fact that $\varphi((i, j)(k, \ell)) = \varphi((i, j)$, this implies the ability for the following calculation:

$$\begin{aligned}\sigma(i, j)\sigma^{-1} = (k, \ell) \implies \sigma(i, j)\sigma(i, j)\sigma^{-1} \\ &= \varphi((i, j)) + \varphi(\sigma) + \varphi((i, j)) - \varphi(\sigma) \quad \text{(additive notation since } \Gamma \text{ is abelian)} \\ &= 2\varphi((i, j) = \varphi((i, j)^2) = \varphi(\mathrm{id}) = 0.\end{aligned}$$

For 2: Consider a homomorphism $\psi : A_n \to \Gamma$ with Γ abelian. We must show $A_n \subseteq \ker(\psi)$, i.e. we need to show that for transpositions (i, j) and (k, ℓ) that$\psi((i, j)(k, \ell)) = 0$. Since $n \geq 5$, we can pick some $\sigma \in A_n$ such that $\sigma(i) = k$ and $\sigma(j) = \ell$. Then

$$\psi((i, j)(k, \ell)) = \psi((i, j)\sigma(i, j)\sigma^{-1})$$

The rest is an exercise. □

We now want to show that having a solvable field extension is equivalent to having a solvable Galois group.

Lemma 2.102.

If G is a solvable group and $f : G \twoheadrightarrow H$ is a surjective group homomorphism then H is solvable.

Proof. For a solvable series we have

$$1 = G_0 \lhd G_1 \lhd \cdots \lhd G_r = G,$$

the series

$$1 = f(G_0) \lhd f(G_1) \lhd \cdots f(G_r) = H$$

is a solvable series, completing the proof. □

Remark 2.103. The following theorem shows that there is no general formula for the roots of a quintic. Note that its converse is also true—but we won't prove that here.

Theorem 2.104.

If $\mathbb{Q} \subseteq L$ be a solvable field extension then $\operatorname{Gal}(L/\mathbb{Q})$ is a solvable group.

Proof. Set $G := \operatorname{Gal}(L/\mathbb{Q})$. By definition, $\mathbb{Q} \subseteq L$ is a Galois extension and

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_r = K$$

such that ther eexists $a_i \in K_i$ and $n_i \geq 2$ with

$$K_{i+1} = K_i[\sqrt[n_i]{a_i}].$$

[We can't immediately use Kummer theory since we need an nth root of unity, but there might not be roots of unity here. We need to somehow put the roots of unity in here so that we can use Kummer theory.]

Let $N = n_1 n_2 \cdots n_r$ and define

$$L' := L[\text{primitive } N\text{th root of unity}].$$

Claim 2.105. $\mathbb{Q} \subseteq L'$ is a Galois extension.

Proof. Let $\beta \in L$ be primitive, so $L = \mathbb{Q}[\beta]$. Let $f \in \mathbb{Q}[x]$ be the minimal polynomial of β. Then L is the splitting field for f and L' is the splitting field for $(x^N - 1)f$. Then since L' is a splitting field for some polynomial, it follows that $\mathbb{Q} \subseteq L'$ is a Galois extension. □

Let $G' := \operatorname{Gal}(L'/\mathbb{Q})$. Then $\mathbb{Q} \subseteq L \subseteq L'$ and $\mathbb{Q} \subseteq L$ is Galois. Thus by a corollary to the Galois correspondence, we have $\operatorname{Gal}(L'/L)$ is a normal subgroup of G' and

$$G = G' / \operatorname{Gal}(L'/L).$$

This implies that G is a surjective image of G', namely via the quotient map $\pi : G' \to G$ with $g \mapsto g \operatorname{Gal}(L'/L)$. It therefore follows from the lemma that G' is solvable, so we deduce that G is solvable. Now set

$$\mathbb{Q} = F_{-1} \subseteq F_0 \subseteq F_1 \subseteq \cdots \subseteq F_r = L',$$

where F_0 adjoins a primitive Nth root of unity to $E_1 = \mathbb{Q}$. Thus $E_1 \subseteq F_0$ is a cyclotomic extension, so $\operatorname{Gal}(F_0/F_{-1})$ is abelian (since we know that cyclotomic extensions have abelian Galois groups).

We now want to build up the rest of the field. We will follow the same procedure as before—for $i \geq 0$, we will take

$$F_{i+1} := F_i[\sqrt[n_i]{a_i}].$$

Since F_i contains a primitive Nth root of unity, it also contains a primitive n_ith root of unity.

Thus we can apply Kummer theory—Kummer theory thus implies that the extension $F_i \subseteq F_{i+1}$ is a Galois extension with cyclic Galois group $(\operatorname{Gal}(F_{i+1}/F_i))$. (In fact, it is isomorphic to C_m with $m \mid n_i$.)

The Galois extension then turns the chain of field extensions

$$\mathbb{Q} = F_{-1} \subseteq F_0 \subseteq F_1 \subseteq \cdots \subseteq F_r = L'$$

into a sequence of groups

$$1 = \operatorname{Gal}(L'/F_r) \subseteq \operatorname{Gal}(L'/F_{r-1}) \subseteq \operatorname{Gal}(L'/F_{r-2}) \subseteq \cdots \operatorname{Gal}(L'/F_{-1}) = \operatorname{Gal}(L'/\mathbb{Q}) = G'.$$

If we set $G_i := \operatorname{Gal}(L'/F_i)$ then we can rewrite the above as

$$1 = G_r \subseteq G_{r-1} \subseteq G_{r-2} \subseteq \cdots \subseteq G_{-1} = G'.$$

But by the above, each $F_{i-1} \subseteq F_i$ is a Galois extension with $\operatorname{Gal}(F_)i/F_{i-1})$ is abelian. Thus $G_i \lhd G_{i-1}$, and since

$$G_{i-1}/G_i \cong \operatorname{Gal}(F_i/F_{i-1}),$$

we have $G/_{i-1}/G_i$ is abelian. It follows that

$$1 = G_r \subseteq G_{r-1} \subseteq G_{r-2} \subseteq \cdots \subseteq G_{-1} = G'$$

is a solvable series. □

This proves that we cannot solve the quintic by taking iterated roots.

§3 Homeworks

§3.1 Algebra 4 Homework 5

Exercise 3.1 (Artin 15.2.1)**.** Let α be a complex root of the polynomial $x^3 - 3x + 4$. Find the inverse of $\alpha^2 + \alpha + 1$ in the form $a + b\alpha + c\alpha^2$, with a, b, c in $\mathbb{Q}$.

Proof. Note

$$(\alpha^2 + \alpha + 1)(a + b\alpha + c\alpha^2) = a\alpha^2 + b\alpha^3 + c\alpha^4 + a\alpha + b\alpha^2 + c\alpha^3 + a + b\alpha + c\alpha^2$$

$$= c\alpha^4 + (b+c)\alpha^3 + (a+b+c)\alpha^2 +)a + b)\alpha + a.$$

We're given $\alpha^3 = 3\alpha - 4$, so $\alpha^4 = \alpha\alpha^3 = 3\alpha^2 - 4\alpha$. Hence we can rewrite the above as

$$\begin{aligned} c(3\alpha^2 - 4\alpha) + &(b+c)(3\alpha - 4) + (a+b+c)\alpha^2 + (a+b)\alpha + a \\ &= 3c\alpha^3 - 4c\alpha + 3b\alpha - 4b + 3c\alpha - 4c + a\alpha^2 + b\alpha^2 + c\alpha^2 + a\alpha + b\alpha + a \\ &= (3c + a + b + c)\alpha^2 + (-4c + 3b + 3c + a + b)\alpha + (-4b - 4c + a) \\ &= (a + b + 4c)\alpha^3 +)a + 4b - c)\alpha + (a - 4b - 4c). \end{aligned}$$

We need this be 1, so we have the system

$$\begin{bmatrix} a + b + 4c = 0 \\ a + 4b - c = 0 \\ a - 4b - 4c = 1 \end{bmatrix},$$

and solving the system yields $\alpha^{-1} = \frac{17}{49} - \frac{5}{49}\alpha - \frac{3}{49}\alpha^2$. □

Exercise 3.2 (Artin 15.2.2)**.** Let $f(x) = x^n - a_{n-1}x^{n-1} + \cdots \pm a_0$ be an irreducible polynomial over F, and let α be a root of f in an extension field K. Determine the element α^{-1} explicitly in terms of α and of the coefficients a_i.

Proof. We assume $\alpha \neq 0$ since if $\alpha = 0$ then α^{-1} doesn't exist. We're given $\alpha^n = a_{n-1}\alpha^{n-1} - \cdots \mp a_0$, so multiplying through by α^{-1} and isolating $a_0\alpha^{-1}$ we get

$$a_0\alpha^{-1} = \alpha^{n-1} - a_{n-1}\alpha^{n-1} + \cdots \mp a_1.$$

$a_0 \neq 0$ since otherwise $f = xg$ for some $g \in F[x]$ of degree ≥ 1, contradicting f is irreducible. Then we can multiply through by a_0^{-1} to conclude

$$\alpha^{-1} = a_0^{-1}(\alpha^{n-1} - a_{n-1}\alpha^{n-2} + \cdots \mp a_1)$$

whenever f is irreducible. □

Exercise 3.3 (Artin 15.3.2)**.** Prove that the polynomial $x^4 + 3x + 3$ is irreducible over the field $\mathbb{Q}[\sqrt[3]{2}]$.

Proof. Let $f := x^4 + 3x + 3$ and set $K := \mathbb{Q}[\sqrt[3]{2}]$. Note that f is irreducible over $\mathbb{Q}$ since f is Eisenstein at $p = 3$. Let α be a root of f. Then since f is a monic irreducible over $\mathbb{Q}$ with α as a root, we have by uniqueness that f is the minimal polynomial for α over $\mathbb{Q}$. It follows from this that $[\mathbb{Q} : \mathbb{Q}[\alpha]] = \deg(f) = 4$.

It suffices to show that $[K : K[\alpha]] = 4$ so that the degree 4 polynomial f is also the minimal polynomial for α over K, which immediately gives that f is irreducible over K. We know that $[\mathbb{Q} : \mathbb{Q}[\alpha]] = 4$ since f is irreducible and we also know $[\mathbb{Q} : K] = 3$. We have the nested field extensions $\mathbb{Q} \subseteq K \subseteq K[\alpha]$, and by the multiplicative property of the degree we know $[\mathbb{Q} : K[\alpha]] = [\mathbb{Q} : \mathbb{Q}[\alpha]][\mathbb{Q}[\alpha] : K[\alpha]]$ and $[\mathbb{Q} : K[\alpha]] = [\mathbb{Q} : K][K : K[\alpha]]$. The first of these gives $[\mathbb{Q} : K[\alpha]] = 4[\mathbb{Q}[\alpha] : K[\alpha]]$ and the second gives $[\mathbb{Q} : K[\alpha]] = 3[K : K[\alpha]]$. But then

$$4[\mathbb{Q}[\alpha] : K[\alpha]] = 3[K : K[\alpha]]]. \tag{$*$}$$

But $\mathbb{Q} \subseteq K \subseteq K[\alpha]$, so by Corollary 15.3.8 we have $[\mathbb{Q}[\alpha] : K[\alpha]] \leq 3$ and $[K : K[\alpha]] \leq 4$, and the only positive integer solution to $(*)$ abiding by these conditions has $[K : K[\alpha]] = 4$ as desired. □

Exercise 3.4 (Artin 15.3.8)**.** Let α and β be complex numbers. Prove that if $\alpha + \beta$ and $\alpha\beta$ are algebraic numbers, then α and β are also algebraic numbers.

Proof. Let $\alpha, \beta \in \mathbb{C}$ be algebraic. We know that the sum and product of algebraic numbers are algebraic. We have $(\alpha - \beta)^2 = (\alpha + \beta)^2 - 4\alpha\beta$ is algebraic, so $\alpha - \beta$ is algebraic. This gives that $(\alpha + \beta) + (\alpha - \beta) = 2\alpha$ (resp. $(\alpha + \beta) - (\alpha - \beta) = 2\beta$) is algebraic, so α (resp. β) is algebraic. □

Exercise 3.5 (Artin 15.3.9)**.** Let α and β be complex roots of irreducible polynomials f and g in $\mathbb{Q}[x]$. Let $K = \mathbb{Q}[\alpha]$ and $L = \mathbb{Q}[\beta]$. Prove that $f(x)$ is irreducible in $L[x]$ if and only if $g(x)$ is irreducible in $K[x]$.

Proof. Denote by M the field $K[\beta] = L[\alpha] = \mathbb{Q}[\alpha, \beta]$. We then have the nested field extensions $\mathbb{Q} \subseteq K \subseteq M$ and $\mathbb{Q} \subseteq L \subseteq M$. By the multiplicative property of the degree we have

$$[\mathbb{Q} : K][K : M] = [\mathbb{Q} : M] = [\mathbb{Q} : L][L : M],$$

so

$$\frac{[K : M]}{[\mathbb{Q} : L]} = \frac{[L : M]}{[\mathbb{Q} : K]}$$

Using $M = K[\beta] = L[\alpha]$ this is rewritten as

$$\frac{[K : K[\beta]]}{[\mathbb{Q} : \mathbb{Q}[\beta]]} = \frac{[L : L[\alpha]]}{[\mathbb{Q} : \mathbb{Q}[\alpha]]}.$$

Note that f is irreducible over $\mathbb{Q}[\beta]$ if and only if $[\mathbb{Q}[\beta] : \mathbb{Q}[\alpha, \beta]] = [\mathbb{Q}[\alpha] : \mathbb{Q}] = \deg(f)$, which is equivalent to $[\mathbb{Q} : \mathbb{Q}[\alpha, \beta]] = [\mathbb{Q} : \mathbb{Q}[\alpha]][\mathbb{Q} : \mathbb{Q}[\beta]]$. Then we get the result because we know f is irreducible over $L[x]$ if and only if the the right side above is 1, or equivalently if the left side above is 1, which similarly holds if and only if g is irreducible in $K[x]$. This completes the proof. □

Exercise 3.6 (Artin 15.4.1)**.** Let $K = \mathbb{Q}[\alpha]$, where α is a root of $x^3 - x - 1$. Determine the irreducible polynomial for $\gamma = 1 + \alpha^2$ over $\mathbb{Q}$.

Proof. Set $f := x^3 - x - 1$. f is irreducible over $\mathbb{Q}$ since it is a monic irreducible in $\mathbb{F}_2[x]$. Hence, since α is a root of f, f is the minimal polynomial of α over $\mathbb{Q}$.

We claim $[\mathbb{Q}[\alpha] : \mathbb{Q}[\gamma]] = 1$. Indeed, clearly $\mathbb{Q}[\gamma] \subseteq \mathbb{Q}[\alpha]$, and conversely notice that

$$\gamma - 1 = \alpha^2 \Rightarrow \alpha(\gamma - 1) = \alpha + 1 \Rightarrow \alpha(\gamma - 2) = 1 \Rightarrow \alpha = \frac{1}{\gamma - 2},$$

so $\alpha \in \mathbb{Q}[\gamma]$, so it follows that $\mathbb{Q}[\alpha] = \mathbb{Q}[\gamma]$, giving the desired.

It then follows from the multiplicative property of the degree of the field extension that $[\mathbb{Q} : \mathbb{Q}[\gamma]] = 3$, so the minimal polynomial for γ is cubic. We're given $\gamma = \alpha^2 + 1$, and using that $\alpha^3 = \alpha + 1$ we compute $\gamma^2 = 3\alpha^2 + \alpha + 1$ and $\gamma^3 = 7\alpha^2 + 5\alpha + 2$. It follows that $\gamma^3 - 5\gamma^2 + 8\gamma - 5 = 0$, so the minimal polynomial for γ must be the cubic monic $x^3 - 5x^2 + 8x - 5$ by uniqueness. □

Exercise 3.7 (Artin 15.4.2)**.** Determine the irreducible polynomial for $\alpha = \sqrt{3} + \sqrt{5}$ over the following fields.

(a) $\mathbb{Q}$.

Proof. $\mathbb{Q}[\alpha]$ is a degree 4 extension since

$$\alpha^2 = 8 + 2\sqrt{15},$$
$$\alpha^3 = 18\sqrt{3} + 14\sqrt{5},$$

and $\alpha^4 = 124 + 32\sqrt{15} = 16(\alpha^2 - 8) + 124$ and hence $(1, \sqrt{3}, \sqrt{5}, \sqrt{15})$ form a basis for $\mathbb{Q}[\alpha]$ as a $\mathbb{Q}$-vector space. α is a root of the monic $x^4 - 16x^2 + 4$ has α as a root, so by uniqueness it is the minimal polynomial for x over $\mathbb{Q}$ (if it weren't then it could be factored, lowering its degree, contradicting the degree of the extension $\mathbb{Q} \subseteq \mathbb{Q}[\alpha]$ is 4). □

(b) $\mathbb{Q}[\sqrt{5}]$.

Proof. We know that $\mathbb{Q} \subseteq \mathbb{Q}[\alpha]$ is a degree 4 extension and that $\mathbb{Q}[\sqrt{5}]$ is a quadratic extension, so by the multiplicative property of the degree we know since $[\mathbb{Q} : \mathbb{Q}[\sqrt{5}]] = 2$ that $[\mathbb{Q}[\sqrt{5}] : \mathbb{Q}[\alpha]] \geq 2$, so it would suffice to find a quadratic irreducible over $\mathbb{Q}[\sqrt{5}]$ with root α. In fact, $\alpha^2 = 8 + 2\sqrt{15}$, so so $\alpha^2 - 2\alpha\sqrt{5} = 8 + 2\sqrt{15} - 2(5) - 2\sqrt{15} = -2$, so the monic irreducible $x^2 - 2\sqrt{5}x + 2$ is the minimal polynomial for α over $\mathbb{Q}[\sqrt{5}]$ by uniqueness. □

(c) $\mathbb{Q}[\sqrt{10}]$.

Proof. Set $K := \mathbb{Q}[\alpha]$. Note that $\sqrt{10} \notin \mathbb{Q}[\alpha]$. Indeed, if it were then $\sqrt{10} = a + b\sqrt{5}$ for some $a, b \in \mathbb{Q}$, meaning

$$10 = a^2 + 2ab\sqrt{5} + 5b^2,$$

so since $\sqrt{5}$ is irrational we must have $2ab = 0$, i.e. either a or $b = 0$. But then either $a^2 = 10$ or $5b^2 = 10$, both of which are impossible for $a, b \in \mathbb{Q}$, so we conclude $\sqrt{10} \notin \mathbb{Q}[\alpha]$ as claimed.

since. Since $\sqrt{10} \notin K$, we have that $K \subseteq K[\sqrt{10}]$ is a quadratic extension. But $\mathbb{Q} \subseteq K$ is a degree 4 extension, so the field extension $\mathbb{Q} \subseteq K[\sqrt{10}]$ has degree 8 by the multiplicative property of the index. But we also have the nested extensions $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{10}]$, so

$$[\mathbb{Q} : K[\alpha]] = [\mathbb{Q} : \mathbb{Q}[\sqrt{10}]][\mathbb{Q}[\sqrt{10}] : K[\sqrt{10}]],$$

that is, $8 = 2[\mathbb{Q}[\sqrt{10}] : K[\sqrt{10}]]$, so $\mathbb{Q}[\sqrt{10} \subseteq K[\alpha]$ is a degree 4 extension, meaning the minimal polynomial for α over $\mathbb{Q}[\sqrt{10}]$ is the polynomial from part (a), namely $x^4 - 16x^2 + 4$. □

(d) $\mathbb{Q}[\sqrt{15}]$.

Proof. We have $\alpha^2 = 8 + 2\sqrt{15}$, so $x^2 - (8 + 2\sqrt{15})$ is the minimal polynomial since $x - (\sqrt{3} + \sqrt{5})$ is not a polynomial over $\mathbb{Q}[\sqrt{15}]$. □

Exercise 3.8 (Artin 15.6.1)**.** Let F be a field of characteristic zero, f' the derivative of some polynomial in $F[x]$, and g an irreducible polynomial that is a common divisor of f and f'. Then g^2 divides f.

§3.2 Algebra 4 Homework 6

Proof. $g \mid f$ iff $f = ga$ for some $a \in F[x]$, so it suffices to show $g \mid a$. If $f = ga$ then $f' = g'a + ga'$. In particular this gives

$$g'a = f' - ga'. \tag{$*$}$$

Obviously $g \mid ga'$, so since we're also given $g \mid f'$ we get $g \mid f' - ga'$, so by $(*)$ we have $g \mid g'a$. g is irreducible over the UFD $F[x]$, so g is prime, and hence either $g \mid g'$ or $g \mid a$. $g \mid g'$ iff $g' = 0$, but the below shows this isn't the case: Recall that F perfect iff all irreducibles $g \in F[x]$ have $g' = 0$. $\operatorname{char} F = 0$ implies F is perfect, so since $g \in F[x]$ is irreducible we have $g' \neq 0$. Hence $g \mid a$, completing the proof per our initial remark. □

Exercise 3.9 (Artin 15.6.2)**.**

(a) Let F be a field of characteristic zero. Determine all square roots of elements of F that a quadratic extension of the form $F(\sqrt{a})$ contains.

(b) Classify quadratic extensions of $\mathbb{Q}$.

Proof. (a) Let $a \in F$. We have $F(\sqrt{a}) = F[t]/(t^2 - a)$, where $\sqrt{a}$ is the residue of t. We have the basis $\{1, a\}$, so each $z \in F(\sqrt{a})$ has $z = x + y\sqrt{a}$ for some $x, y \in F$. We have $z^2 = (x^2 + y^2) + 2xy\sqrt{a}$, and $x^2 + y^2 \in F$, so for z to be a root of something in F we need that $2xy\sqrt{a} = 0$. Since $\operatorname{char} F = 0$, we have either $x = 0$, $y = 0$, or $a = 0$. If $a = 0$ then $F(\sqrt{a}) \cong F[t]/(t^2)$, which has zero divisors and is hence not a field. Hence eiter $x = 0$ or $y = 0$, and in particular, either $z^2 = x^2$ or $z^2 = y^2 a$ for $x, y \in F$.

In the former case we have $z \in F$, generaing no new square roots. In the latter case, $z^2 = y^2 a$, so the square root $y\sqrt{a}$ is generated.

Therefore, all square roots of elements of F that a quadratic extension of the form $F(\sqrt{a})$ contains are square roots of $y^2 a$ for all $y \in F$, the roots of which take the form $\pm y\sqrt{a}$ for $y \in F$.

(b) Recall that if $\operatorname{char} F \neq 2$ then $F \subseteq K$ is a quadratic extension of F if and only if $K = F(\sqrt{a})$ for some $a \in F$ such that $\sqrt{a} \notin F$.

$\operatorname{char} \mathbb{Q} \neq 2$, so $\mathbb{Q} \subseteq K$ is a quadratic extension if and only if $K = \mathbb{Q}(\sqrt{a})$ for some $a = p/q \in \mathbb{Q}$ such that $\sqrt{a} = \sqrt{p/q} = \sqrt{p}/\sqrt{q} \notin \mathbb{Q}$. In particular this holds if and only if both $\sqrt{p}$ and $\sqrt{q}$ are not perfect squares. □

Exercise 3.10 (Artin 15.6.3)**.** Determine the quadratic number fields $\mathbb{Q}(\sqrt{d})$ that contain a primitive nth root of unity for some integer n.

Proof. Clearly any quadratic number field $\mathbb{Q}(\sqrt{d})$ contains the primitive first root of unity 1 and $\mathbb{Q}(\sqrt{-1})$ contains the primitive square root of unity i, so we'll consider $|d| \geq 2$.

$\mathbb{Q}(\sqrt{d})$ contains a primitive nth root of unity $\zeta = e^{2\pi i k/n}$ iff $\mathbb{Q}(\sqrt{d}) \cong \mathbb{Q}[x]/(\Phi_n)$, where Φ_n is the nth cyclotomic polynomial. Φ_n must have degree 2 so that $\mathbb{Q}(\sqrt{d})$ has degree 2 over $\mathbb{Q}$. Recall that the degree of the nth cyclotomic polynomial is $\phi(n)$, so we need n such that $\phi(n) = 2$. We observe from the Euler product formula $\phi(n) = n\prod_{p|n}(1 - 1/p)$ that $\phi(n) = 2$ iff $n \in \{3, 4, 6\}$, so only these could work. We now determine what d has $\mathbb{Q}(\sqrt{d}) \cong \mathbb{Q}[x]/(\Phi_3)$ or $\mathbb{Q}[x]/(\Phi_4)$ or $\mathbb{Q}[x]/(\Phi_6)$. d must be negative to contain $\zeta \in \mathbb{C} \setminus \mathbb{R}$.

- Case 1: $n = 3$, $\zeta = e^{2\pi i k/n} = e^{2\pi i k/3} = \cos\left(\frac{2\pi k}{3}\right) + i \sin\left(\frac{2\pi k}{3}\right)$ for k and 3 coprime. When $k = 1$ we have

$$\zeta = \cos\left(\frac{2\pi}{3}\right) + i\sin\left(\frac{2\pi}{3}\right) = -\frac{1}{2} + i\frac{\sqrt{3}}{2} = -\frac{1}{2} + \frac{\sqrt{-3}}{2} \in \mathbb{Q}(\sqrt{-3}).$$

- Case 2: $n = 4$, $\zeta = e^{2\pi ik/n} = e^{2\pi ik/4} = \cos\left(\frac{2\pi k}{4}\right) + i\sin\left(\frac{2\pi k}{6}\right) = \cos\left(\frac{\pi k}{2}\right) + i\sin\left(\frac{\pi k}{2}\right)$ for k and 4 coprime. When $k = 1$ we have
$$\zeta = \cos\left(\frac{\pi}{2}\right) + i\sin\left(\frac{\pi}{2}\right) = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2} = -\frac{1}{2} + \frac{\sqrt{-2}}{2} \in \mathbb{Q}(\sqrt{-2}).$$
- Case 3: $n = 6$, $\zeta = e^{2\pi ik/n} = e^{2\pi ik/6} = \cos\left(\frac{2\pi k}{6}\right) + i\sin\left(\frac{2\pi k}{6}\right) = \cos\left(\frac{\pi k}{3}\right) + i\sin\left(\frac{\pi k}{3}\right)$ for k and 6 coprime. When $k = 1$ we have
$$\zeta = \cos\left(\frac{\pi}{3}\right) + i\sin\left(\frac{\pi}{3}\right) = -\frac{1}{2} + i\frac{\sqrt{3}}{2} = \frac{1}{2} + \frac{\sqrt{-3}}{2} \in \mathbb{Q}(\sqrt{-3}\square$$

Exercise 3.11 (Artin 15.7.1)**.** Identify the group $(\mathbb{F}_4, +)$.

Proof. $\mathbb{F}_4 \cong \mathbb{F}_2[x]/(x^2 + x + 1)$, so letting α be the image of x under the canonical map we have $\mathbb{F}_4 = \{0, 1, \alpha, \alpha + 1\}$, with addition defined by $1 + 1 = 0$ and $\alpha^2 = \alpha + 1$.

$(\mathbb{F}_4, +)$ is abelian and we know from last semester there'e exactly two abelian groups of order 4 up to isomorphism, the cyclic group $C_4 \cong \mathbb{Z}/(4)$ and the Klein-4 group $J \cong \mathbb{Z}/(2) \oplus \mathbb{Z}/(2)$. $(\mathbb{F}_4, +) \ncong C_4$ because there are no elements of additive order 4, meaning $(\mathbb{F}_4, +) \cong J$, the Klein-4 group. □

Exercise 3.12 (Artin 15.7.7)**.** If K is a finite field then the product of the nonzero elements of K is -1.

Proof. Let $q = p^n$. Recall that the $q - 1$ nonzero elements of $\mathbb{F}_q$ are roots of $x^{q-1} - 1 = \prod_{\alpha \in \mathbb{F}_q^\times}(x - \alpha)$. The constant term on the LHS is -1, so -1 must also be the constant term on the RHS, $\prod_{\alpha \in \mathbb{F}_{p^n}^\times}(-1)^{|\mathbb{F}_q^\times|}\alpha = \prod_{\alpha \in \mathbb{F}_{p^n}^\times}(-1)^{q-1}\alpha$. When p is an odd prime we have q is odd, so $(-1)^{q-1} = 1$ and hence the result follows.

We now show the result holds in the case $p = 2$. If q is a power of 2 then elements of $\mathbb{F}_{2^n}$ are the 2^n different linear combinations of the vector space $\{1, \alpha, \alpha^2, \dots, \alpha^n\}$ over $\mathbb{F}_2$. Hence $+1 = -1$ in $\mathbb{F}_{2^n}$, so
$$\prod\nolimits_{\alpha \in \mathbb{F}_{2^n}^\times}(-1)^{2^n-1}\alpha = \prod\nolimits_{\alpha \in \mathbb{F}_{2^n}^\times}(+1)^{2^n-1}\alpha = \prod\nolimits_{\alpha \in \mathbb{F}_{2^n}^\times}\alpha,$$
so just as in the case of odd primes we get the result. □

Exercise 3.13 (Artin 15.7.8)**.** The polynomials $f := x^3 + x + 1$ and $g := x^3 + x^2 + 1$ are irreducible over $\mathbb{F}_2$. Let K be the field extension obtained by adjoining a root of f, and let L be the extension obtained by adjoining a root of g. Describe explicitly an isomorphism from K to L, and determine the number of such isomorphisms.

Proof. Let α be a root of f and let β be a root of g. The minimal polynomial of α (resp. β) is f (resp. g) since f and g are monic irreducibles and the minimal polynomial is unique. Notice $g(\alpha + 1) = 0$. Indeed, since $\alpha^3 + \alpha + 1 = 0$ we have that
$$(\alpha + 1)^3 = \alpha^3 + 3\alpha^2 + 3\alpha + 1 = (\alpha^3 + \alpha + 1) + 3\alpha^2 + 2\alpha = 3\alpha^2 + 2\alpha = \alpha^2$$

in $\mathbb{F}_2(\alpha)$, and

$$(\alpha+1)^2 = \alpha^2 + 2\alpha + 1 = \alpha^2 + 1,$$

and hence

$$(\alpha+1)^3 + (\alpha+1)^2 + 1 = 2\alpha^2 + 1 + 1 = 0$$

in $\mathbb{F}_2(\alpha)$. It follows that $\alpha+1$ is a root of the monic irreducible $g \in \mathbb{F}_2[x]$, so by uniqueness of the minimal polynomial we have g is the minimal polynomial for $\alpha+1$. It follows that $L = \mathbb{F}_2[x]/(g)$ with $\alpha+1$ the image of x under the canonical map $\mathbb{F}_2[x] \to \mathbb{F}_2[x]/(g)$. This gives a map $\sigma : L \to K$ given by $\beta \mapsto \alpha+1$ where we set $\sigma|\mathbb{F}_2 := \mathrm{id}_{\mathbb{F}_2}$. We now show this is an isomorphism of fields extensions over $\mathbb{F}_2$.

We now give an explicit isomorphism $\sigma : L \to K$ per the above observations. Note that $L = \mathbb{F}_2(\beta)$, which is $\mathbb{F}_2[\beta]$ (since β is algebraic over $\mathbb{F}_2$), so any $x \in L$ takes the form $c_0 + c_1\beta + c_2\beta^2$ for some $c_0, c_1, c_2 \in \mathbb{F}_2$ because β has degree 3 over $\mathbb{F}_2$. Then set

$$\sigma(c_0 + c_1\beta + c_2\beta^2) := c_0 + c_1(\alpha+1) + c_1(\alpha+1)^2.$$

σ is well-defined: If $x = c_0 + c_1\beta + c_2\beta^2, x' = c_0' + c_1'\beta + c_2'\beta^2 \in L$ are equal then necessarily $c_0 = c_0', c_1 = c_1', c_2 = c_2'$ since $\{1, \beta, \beta^2\}$ is linearly independent in L. Hence $\sigma(x) = \sigma(x')$, so σ is well-defined.

σ is a ring homomorphism: We have $\sigma(1) = 1$ since $0, 1 \in \mathbb{F}_2$ and if $x, x' \in L$ then

$$\begin{aligned} \sigma(x + x') &= \sigma((c_0 + c_1\beta + c_2\beta^2) + (c_0' + c_1'\beta + c_2'\beta^2)) \\ &= \sigma((c_0 + c_0') + (c_1 + c_1')\beta + (c_2 + c_2')\beta^2) \\ &= (c_0 + c_0') + (c_1 + c_1')(\alpha+1) + (c_2 + c_2')(\alpha+1)^2 \\ &= \sigma(x) + \sigma(x') \end{aligned}$$

and it is clear from how σ acts on $\{1, \beta, \beta^2\}$ that σ preserves field multiplication.

σ is bijective: it is an injection as the kernel is is clearly trivial, and a surjection because any $c_0 + c_1\alpha + c_2\alpha^2$ has $c_0 + c_1(\alpha-1) + c_2(\alpha-1)^2 = \alpha^2 c_2 + \alpha(c_1 - 2c_2) + c_0 - c_1 + c_2$, so choose the corresponding element in L to be $x = c_0 - c_1 + c_2 + (c_1 - 2c_2)\beta + c_2\beta^2$. This gives σ is a bijection.

Finally, σ is an isomorphism of field extensions because $\sigma|\mathbb{F}_2 = \mathrm{id}_{\mathbb{F}_2}$ follows from $\sigma(c_0) = c_0$ for any $c_0 \in \mathbb{F}_2$ by definition of σ.

We know $K \cong L$ are finite fields of order $2^{\deg(f)} = 2^{\deg(g)} = 8$, so since there is a unique field of order $q = p^n$ for each prime p and $n \geq 1$ we know that the number of such isomorphisms is the size of the automorphism group of $\mathbb{F}^8$.

Recall that if $\alpha \in K$ and $\beta \in L$ for field extensions $K, L \subseteq F$ then there is an isomorphism of field extensions $F(\alpha)$ and $F(\beta)$ of F that is the identity on F if and only if the irreducible polynomials for α and β over F coincide. We just showed this is the case, so this is indeed an isomorphism. In this case we know $K \cong L$, so it follows that so long as α and β are distinct roots of the irreducible $f = x^3 + x^2 + 1$ then there exists a field isomorphism from α to K. $\alpha = \beta^2$ and $\beta^2 + \beta$ are the two other (distinct) roots of f distinct from its third root β , so since f is the irreducible polynomial for all three we conclude that there are exactly three automorphisms for this field, and if there is another such isomorphism then it must be one of these. □

Exercise 3.14 (Artin 15.7.9)**.** Work this problem without appealing to Artin Theorem 15.7.3.

(a) Determine the number of monic irreducible polynomials of degree 2 in $\mathbb{F}_p[x]$.

(b) Let $f \in \mathbb{F}_p[x]$ be a quadratic irreducible polynomial. Prove that $K := \mathbb{F}_p[x]/(f)$ is a field of order p^2 and that its elements have the form $a + b\alpha$, where $a, b \in \mathbb{F}_p$ and α is a root of f in K. Moreover, every such element with $b \neq 0$ is the root of an irreducible quadratic polynomial in $\mathbb{F}_p[x]$.

(c) Show that every polynomial of degree 2 in $\mathbb{F}_p[x]$ has a root in K.

(d) Show that all the fields K constructed as above for a given prime p are isomorphic.

Proof. We prove each point.

(a) Let $f \in \mathbb{F}_2[x]$ be monic. f is reducible iff f splits completely as $(x - a)(x - b)$ for some $a, b \in \mathbb{F}_p$. There are $p(p-1)/2 + p$ unordered pairs $\{a, b\}$ for $a, b \in \mathbb{F}_p$, so the remaining $p^2 - (p(p-1)/2 + p) =$ must be irreducible, so there are $p^2 - (p(p-1)/2 + p) = p(p-1)/2$ monic irreducible $f \in \mathbb{F}_p[x]$ of degree 2.

(b) Let $f \in \mathbb{F}_2[x]$ be a quadratic irreducible and set $K := \mathbb{F}_p[x]/(f)$. Recall that the principal ideal (f) in a polynomial ring over a field is maximal if and only if f is irreducible, so we have that K, the quotient ring $\mathbb{F}_p[x]/(f)$, is a field. Where α is a root of f in K we have α is the residue of x mod (f), so since f is a quadratic irreducible the field extension $\mathbb{F}_2 \subseteq K$ is quadratic. Hence the elements of K take the form $a + b\alpha$, where $a, b \in \mathbb{F}_2$. K has order p^2 because there are p^2 distinct elements that may take this form.

Moreover, if $x = a + b\alpha \in K$ has $b \neq 0$ then x must be the root of an irreducible quadratic polynomial in $\mathbb{F}_2$ because any element of this form has degree 2 over $\mathbb{F}_2$ since $\alpha \notin \mathbb{F}_2[x] \Rightarrow b\alpha \notin \mathbb{F}_2$ for any nonzero $b \in \mathbb{F}_2$, so the minimal polynomial of x is quadratic, and hence x is a root of a quadratic irreducible.

(c) There are $p(p-1)/2$ monic quadratic irreducibles in $\mathbb{F}_p[x]$. If g is one of them then the remaining $p(p-1)/2 - 1$ have at most twice as many roots in K, namely $p(p-1) - 2$ of them The set $K \setminus F$ has cardinality $p(p-1)$, so it contains at least two elements that are not the root of any polynomial monic quadratic irreducibles in $F[x]$. By part (b) we know each of the $p(p-1)$ elements is the root of one of the $p(p-1)/2$ monic quadratic irreducibles in $\mathbb{F}_p[x]$ (since we can clear the leading coefficient to make it monic). Thus they are roots of g. This holds for all monic irreducible quadratic g and so so all quadratic polynomials that are irreducible in $F[x]$ have a root in K, and the reasoning gives that the same holds for those that are reducible, giving the result.

(d) Let $f, g \in \mathbb{F}_p[x]$ be irreducible quadratics and set $K := \mathbb{F}_p[x]/(f)$, $L := \mathbb{F}_p[x]/(g)$. By part (c) we know since f is a polynomial of degree 2 in $\mathbb{F}_p[x]$ that L contains a root of f, call it β. Then $L = \mathbb{F}_p(\beta)$ and $K = \mathbb{F}_p(\alpha)$. But f is the irreducible polynomial of both α and β since both are roots and f is irreducible over $\mathbb{F}_p[x]$. Hence $K = F(\alpha) \cong F(\beta) = L$, as desired.

□

Exercise 3.15 (Artin 15.M.4)**.**

(a) Let p be an odd prime. Prove that exactly half of the elements of $\mathbb{F}_p^\times$ are squares and that if α and β are nonsquares, then $\alpha\beta$ is a square.

(b) Prove the same assertion for any finite field of odd order.

(c) Prove that in a finite field of even order, every element is a square.

(d) Prove that the irreducible polynomial for $\gamma := \sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$ is reducible modulo p for every prime p.

Proof. We prove each point.

(a) Let p be an odd prime. We know $\mathbb{F}_p^\times$ is cyclic, say with generator α. First we show that $\mathbb{F}_p^\times = \{1, \alpha, \dots, \alpha^{p-1}\}$, $g = \alpha^j \in \mathbb{F}_p^\times$ a square if and only if j is even. Indeed, the reverse implication is immediate, while for the forward implication we note $g = \alpha^i a$ square iff there's α^i with $\alpha^i\alpha^2 = \alpha^{2i} = \alpha^j$ iff $2i = 2 + n|\mathbb{F}_p^\times| = j + nt$, where t is even since p is an odd prime, so t must be even. Since the set of possible $\alpha^j \in \mathbb{F}_p^\times$ with j even is half of them, we conclude exactly half of $\mathbb{F}_p^\times$ are squares.

From the above we conclude that if a, b are nonsquares then $a = \alpha^{\text{odd}}$ and $b = \alpha^{\text{odd}}$, so $ab = \alpha^{\text{odd}}b^{\text{odd}} = \alpha$, so $ab = \alpha^{\text{even}}$, a square.

(b) All finite fields of odd order have order $q = p^n$ for an odd prime p and $n \geq 1$. Then the same proof *verbatim* (other than replacing p with $q = p^n$) as in part (a) above works since we know $\mathbb{F}_q^\times$ is also cyclic.

(c) K is a finite field of even order iff $K = \mathbb{F}_{2^n}$, which again we recall is cyclic. Hence any $x \in K$ has $x = \alpha^j$ for some j. If j is even then $\alpha^{j/2} \in K$ is the square root of α^j, affirming the claim. If j is odd, say $2\ell + 1$ for some integer ℓ, then $(\alpha^t)^2 = \alpha^{2t}$ is the square root of $\alpha^{2\ell+1}$ iff $2t \equiv 2k + 1 \pmod{2^n - 1}$. Then $2t = 2\ell + 1 + k(2^n - 1)$ for some integer k, so $t = \ell + \frac{1}{2} + k2^{n-1} - \frac{k}{2}$, which is even when k is chosen to be odd.

(d) Recall the irreducible polynomial for γ over $\mathbb{Q}$ is $f := x^4 - 10x + 1$. f cannot have linear factors since none of $\pm(\sqrt{2}+\sqrt{3})$ or $\pm(\sqrt{2}-\sqrt{3})$ are in $\mathbb{F}_p$. Hence f must split into quadratic factors. Hence it suffices to show that any combination of $f = (x-\sqrt{2}+\sqrt{3})(x-\sqrt{2}-\sqrt{3})(x+\sqrt{2}+\sqrt{3})(x-\sqrt{2}+\sqrt{3})$ into a product of quadratic polynomials is a valid factorization of f over $\mathbb{F}_p[x]$. The three such combinations are $(x^2-1-2\sqrt{2})(x^2-1+2\sqrt{2})$, $(x^2+1-2\sqrt{3})(x^2+1+2\sqrt{3})$, and $(x^2-5-2\sqrt{6})(x^2-5+2\sqrt{6})$. At least one of these works since at least one of $\sqrt{2}$, $\sqrt{3}$, or $\sqrt{6}$ is in $\mathbb{F}_p$ since the product of two non-squares is a square when p is odd, completing the proof. □

§3.3 Algebra 4 Homework 7

Exercise 3.16 (Artin 15.8.2)**.** Determine all primitive elements for the extension $K = \mathbb{Q}(\sqrt{2},\sqrt{3})$ of $\mathbb{Q}$.

Proof. We show that $\gamma = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ is primitive if and only if at least two elements of $\{b, c, d\}$ are nonzero.

We first show the forward direction. $[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 4$, so if $\gamma = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ is primitive for K over $\mathbb{Q}$ then its minimal polynomial has degree 4. If γ is primitive then so is $\gamma + q$ for any $q \in \mathbb{Q}$, so it suffices to characterize primitive elements for K of the form $\gamma = b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$. The minimal polynomial of γ must have degree 4, so at least two elements of $\{b, c, d\}$ must be nonzero (since otherwise $K = \mathbb{Q}(\gamma) = \mathbb{Q}(b\sqrt{2})$ or $\mathbb{Q}(c\sqrt{3})$ or $\mathbb{Q}(d\sqrt{6})$ which are either degree 1 or degree 2 extensions depending on b, c, d.

For the reverse direction, let at least two of b, c, d be nonzero. We may assume $a = 0$ as before, so it suffices to show $\gamma = \sqrt{x}+s\sqrt{y}+t\sqrt{z}$ for $s, t \in \mathbb{Q}$ and distinct $x, y, z \in \{2, 3, 6\}$.

In the case s (or instead t) is zero, we recall from lecture that all but finitely many t (or, respectively, s) is primitive, and in particular such t must be such that at least two of $\pm x \pm t\sqrt{z}$ (resp. $\pm x \pm s\sqrt{y}$) coincide, which is impossible given that x, y, z are distinct.

If all three coefficients are nonzero then we can reduce to the case above for exactly two nonzero coefficients by noticing that, where $\gamma = \sqrt{x} + s\sqrt{y} + t\sqrt{z}$ for $s, t \in \mathbb{Q}$ and distinct $x, y, z \in \{2, 3, 6\}$ as above, we have when $K \in \mathbb{Q}$ that

$$\gamma^2 - K\gamma = \sqrt{x}\big(-K + 2s\sqrt{y} + 2t\sqrt{z}\big) + \sqrt{y}\big(2st\sqrt{z} - Ks\big) - Kt\sqrt{z} + s^2y + t^2z + x$$

and an appropriate choice makes one of $\sqrt{x}$, $\sqrt{y}$, or $\sqrt{z}$ vanish, reducing us to the above case. This completes the proof.

□

Exercise 3.17 (Artin 15.10.1)**.** Prove that the subset of $\mathbb{C}$ consisting of the algebraic numbers is algebraically closed.

Proof. Let $A \subseteq \mathbb{C}$ be the algebraic numbers over $\mathbb{Q}$. A is algebraically closed if all nonconstant $f \in A[x]$ have a root in A. Suppose for a contradiction $f \in A[x]$ is nonconstant without any roots in A. Then f has an irreducible factor of degree ≥ 2, so we can assume without loss of generality that f is that irreducible. Then $A \subseteq A[x]/(f) = A(\tau)$ is a field extension of A of degree $\deg f \geq 2$. But τ is transcendental since $\tau \notin A$ (since otherwise $f(\tau) = 0$, contradicting f has no roots in A), whereas $f(\tau) = 0$ over $(A(\tau))[x]$, and so τ is algebraic over A. Hence meaning $[A(\tau) : A] < +\infty$, so τ is algebraic over A. But then there's some polynomial $g \in A[x]$ with $g = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$, where $a_i \in A$, such that $g(\tau) = 0$. It follows that τ is algebraic over $\mathbb{Q}(a_1, \ldots, a_n)$, so $[\mathbb{Q}(\tau) : \mathbb{Q}(a_0, \ldots, a_n)] < +\infty$. But each a_i being algebraic means that $[\mathbb{Q}(a_0, \ldots, a_{i+1}) : \mathbb{Q}(a_i)] < +\infty$ for each $0 \leq i \leq n-1$, so by the multiplicative property of the degree we have

$$[\mathbb{Q}(\tau) : \mathbb{Q}] = [\mathbb{Q}(\tau) : \mathbb{Q}(a_0, \ldots, a_n)][\mathbb{Q}(a_0, \ldots, a_n) : \mathbb{Q}(a_0, \ldots, a_{n-1})] \cdots [\mathbb{Q}(a_0) : \mathbb{Q}]$$

is finite, contradicting $[\mathbb{Q}(\tau) : \mathbb{Q}] = +\infty$ since τ is transcendental. □

Exercise 3.18 (Artin 15.M.1)**.** Let $F(\tau)$ be a field extension generated by a transcendental element τ and let β be an element of $F(\tau)$ that is not in F. Prove that τ is algebraic over $F(\beta)$.

Proof. Recall if τ is transcendental then $F(\tau) \overset{\cong}{\to} F(x)$, with x the image of τ. $\beta \in F(\tau)$, so there's $f, g \in F[x]$ with $\beta = f(\tau)/g(\tau)$, where g is nonzero. Then $\beta g(\tau) = f(\tau)$, so $\beta g(\tau) - f(\tau) = 0$. We claim $h := \beta g - f \in F(\beta)[x]$, since then $h(\tau) = 0$ and hence τ is algebraic over $F(\beta)$ as desired. For this it suffices to show that h is not constant. Indeed, $g \neq 0$ means that β has a term ax^k for some nonzero $k \geq 1$, and $\beta \notin F$ means $\beta a \notin F$, meaning $\beta g - f$ has nonzero coefficient on x^k, as desired. □

Exercise 3.19 (4)**.** Let K be a field and $f \in K[x]$ be monic of degree n. Let $K \subseteq L$ be a splitting field for f. Prove that $[L : K]$ divides $n!$.

Proof. We induct on the degree of $f \in K[x]$.

Base case ($n = 1$ or $n = 2$): f is monic of degree n, so since L is a splitting field for f we have

$$K \subseteq K_1 \subseteq \cdots \subseteq K_\ell = L,$$

where $\ell \leq n$. This is clear, as we can construct such K_i by starting with K, adjoining a root of f, $\alpha \notin K$, to get $f = (x - \alpha)^d q$, where d is the multiplicity of α and $q \in F[x]$ is some degree $n - d$ polynomial. If $\deg q = 1$ then we're done since $d = n$ implies $K_1 = L = K(\alpha)$ is a degree n extension over K, which divides $n!$. Otherwise we proceed by adjoining a root of q. Such a root β has an irreducible factor of q as its minimal polynomial by uniqueness and hence has degree $\leq \deg(q) = n - d$.

Hence the field extension $K_1 \subseteq K_2 = K(\alpha, \beta)$ is a degree $n - d$ extension, so $K \subseteq (K_1 \subseteq K_2 =)L$ is a degree $n(n-d)$ extension, which divides $n!$.

Case 1: f is reducible:

Suppose the claim holds for some $1 \leq k \leq n$. If f is reducible then $f = f_1 f_2$, with $f_1, f_2 \in K[x]$ nonconstant polynomials. If $\deg(f_1) = b$ and L' is the splitting field over K of f_1, L is the splitting field of f_2 over L' then, by the induction hypothesis, we have $[L' : K]$ divides $b!$ and $[L : L']$ divides $(n-b)!$. Thus by the multiplicative property of the index we know $[L : K]$ divides $b!(n-b)!$, which divides $n!$ (as the denominator of definition of $\binom{n}{b}$, which are integers).

Case 2: f is irreducible:

Where α is a root of p, we have $[K(\alpha) : K] = k$. Then we have $f = (x - \alpha)q$ over $K(\alpha)$, where $\deg(q) \leq n - 1$. Taking L to be the splitting field of q over $K(\alpha)$, we have by our induction hypothesis that $[L : K(\alpha)]$ divides $(n-1)!$. Thus the degree $[L : K] = [L : K(\alpha)][K(\alpha) : K]$ divides $(n-1)!n = n!$, completing the proof. □

Exercise 3.20 (5)**.** Let F be a field of characteristic p and let $F \subseteq K$ be a finite field extensions such that p does not divide $[K : F]$. Prove that $F \subseteq K$ is a separable field extension.

Proof. If $\operatorname{char} F = p$ and $F \subseteq K$ has finite degree then K is separable iff the minimal polynomial f for α is separable for each $\alpha \in K$, which holds iff $f' \neq 0$ for each such f. If $\alpha \in K \setminus F$ then $2 \leq \deg \alpha \leq [K : F]$. We have $\deg \alpha = \deg f = [F(\alpha) : F]$, so since $p \nmid [K : F(\alpha)] = [K : F(\alpha)][F(\alpha) : F] = [K : F(\alpha)] \deg \alpha$, we have fore each $n \in \mathbb{N}$ that $[K : F(\alpha)] \deg \alpha \neq pn$ implies $\deg \alpha \nmid p$, so since $\deg \alpha \geq 2$ and $\deg \alpha \nmid p$ we have f'_α has nonzero coefficient for $x^{\deg \alpha - 1}$ modulo p, i.e. $f' \neq 0$, meaning f is separable, proving the claim. □

Exercise 3.21 (6)**.** Let $f : \mathbb{R} \to \mathbb{R}$ be a field automorphism.

(a) Prove that $f(q) = q$ for all $q \in \mathbb{Q}$.

(b) Prove that if $x > 0$ then $f(x) > 0$, and prove that this implies f is increasing.

(c) Prove that if $|x - y| < 1/n$ for some $n \geq 1$ then $|f(x) - f(y)| < 1/n$. Then prove this implies f is continuous.

(d) Prove that $f(x) = x$ for all $x \in \mathbb{R}$. In other words, the group of field automorphisms of $\mathbb{R}$ is the trivial group.

Proof. (a) For a field automorphism $\mathbb{R} \overset{\cong}{\to} \mathbb{R}$ we require $f(1/n)f(n) = 1 = f(1)$ and hence $f(1/n) = f(1)/f(n)$, so $m/n = \sum_1^m f(1/n) = f(\sum_1^m 1/n) = f(m/n)$, so $f(m/n) = m/n$ as desired.

(b) Note $x > 0$ iff there's nonzero $\alpha \in \mathbb{R}$ with $\alpha^2 = x$, so $f(x) = f(\alpha)f(\alpha) = f(\alpha)^2 > 0$ since $f(\alpha) \in \mathbb{R} \setminus \{0\}$ means its square is positive, and indeed $f(\alpha) \neq 0$ because f must be injective and hence have trivial kernel. This implies f is increasing because $x > y$ implies $x - y > 0$ and so $f(x - y) > 0$, so $f(x) > f(y)$.

(c) First note $|f(x) - f(y)| = |f(x - y)|$. $|f(x - y)| \leq f(|x - y|)$ since if $|x - y| < 1/n$ then $-1/n < x - y < 1/n$ then $f(-1/n) < f(x - y) < f(1/n)$ since f is increasing, and so $-1/n < f(x - y) < 1/n$ by part (a) ,so $|f(x - y)| < 1/n$. Hence for $\varepsilon > 0$ choose $\delta = 1/n$ for some n such that $1/n < \varepsilon$.

(d) Continuous functions are uniquely determined by their values at rational points, so by (a) and (c) we're done by the limit characterization of continuity which gives $f = \mathrm{id}$. □

§3.4 Algebra 4 Exam 2

Lemma 3.22: A.

Let R be a ring and $a \in R$. Then the translation map $\tau_a : R[x] \to R[x]$ via $f = f(x) \mapsto \tau_a f := f(x - a)$ is a ring homomorphism.

Proof. τ_a is well-defined since if $f := a_n x^n + \cdots + a_0 \in R[x]$ is arbitrary then $\tau_a f \in R[x]$. τ_a is a ring homomorphism—we have $\tau_a(1) = 1$ is immediate, that for $g = b_m x^m + \cdots + b_0 \in R[x]$ then $\tau_a(f + g) = (f + g)(x - a) = f(x - a) + g(x - a) = \tau_a f + \tau_a g$, and $\tau_a(fg) = (fg)(x - a) = f(x - a)g(x - a) = (\tau_a f)(\tau_a g)$, giving the result. □

Lemma 3.23: B.

Let R be a ring and $a \in R$, and $f := a_n x^n + \cdots + a_0 \in R[x]$ for a_n nonzero. Then $f(x + a)$ is an irreducible element of $R[x]$ if and only if f is an irreducible element of $R[x]$.

Proof. We prove the contrapositive, that if f is reducible, then $f(x - a)$ is reducible. Suppose that $f = gh$ for some $g, h \in R[x]$ is a proper factorization of f in $R[x]$. Since the factorization in $R[x]$ is proper, both g and h have positive degree and $\deg(f) = \deg(g) + \deg(h)$.

The translation map $f \mapsto \tau_a f$ is a ring homomorphism by Lemma A above, so since $f = gh$ we have $\tau_a f = (\tau_a g)(\tau_a h)$. $\deg(\tau_a f) = \deg(\tau_a g)\deg(\tau_a h)$.

We now show that for any $p \in R[x]$, $\deg(\tau_a p) \leq \deg(p)$. Indeed, each term of $f(x - a)$ is of the form

$$a_k(x - a)^k = a_k \sum_{j=0}^{k} \binom{k}{j} (-1)^j x^j a^{k-j}, \qquad \text{(since R is a commutative ring)}$$

which can have terms of degree at most $k \leq n$, so

$$\begin{aligned}(\tau_a f) &= \deg\left(\sum_{k=0}^{n} a_k(x-a)^k\right) \\ &\leq \max\{\deg(a_0), \deg(a_1(x-k)), \dots, \deg((a_n(x-a)^n)\} \\ &\leq \max\{0, 1, \dots, n\} && \text{(per the above observation)} \\ &= n = \deg(f),\end{aligned}$$

as claimed. Our assumption that $a_n \neq 0$ gives that $\deg \tau_a f = \deg f$. This forces $\deg(\tau_a g) = \deg g$ and $\deg(\tau_a h) = \deg h$, since if one has strict inequality then the other must increase to compensate, which again is not possible by the above argument. Therefore the factorization $\tau_a f = (\tau_a g)(\tau_a h)$ is proper, meaning $\tau_a f$ is irreducible as claimed. Hence, by the contrapositive, if $\tau_a f$ is an irreducible element of $R[x]$ then so is f.

The reverse implication comes from applying the result established just above, and then considering $\tau_{-a}\tau_a f$ (since $-a \in R$ whenever $a \in R$). □

Exercise 3.24 (1)**.** For a field extension $K \subseteq L$, define $\mathrm{Gal}(L/K)$ to be the group of all field isomorphisms $\phi : L \to L$ such that $\phi|_K = \mathrm{id}_K$. Fix a square-free integer $d \geq 2$, so elements of $\mathbb{Q}[\sqrt{d}]$ can be uniquely written as $a + b\sqrt{d}$ for $a, b \in \mathbb{Q}$. Define a set map $\phi : \mathbb{Q}[\sqrt{d}] \to \mathbb{Q}[\sqrt{d}]$ via the formula

$$\phi(a + b\sqrt{d}) = a - b\sqrt{d}$$

Do the following:

(a) (5 points) Prove that ϕ is an element of $\mathrm{Gal}(\mathbb{Q}[\sqrt{d}]/\mathbb{Q})$. [Hint: the most important thing to prove is that ϕ is actually a homomorphism of fields!]

Proof. Let $a + b\sqrt{d}$ and $r + s\sqrt{d}$ be arbitrary elements of $\mathbb{Q}[\sqrt{d}]$. ϕ is well-defined because $a+b\sqrt{d} = r+s\sqrt{d}$ implies $a-b\sqrt{s} = r-s\sqrt{d}$. We also observe that $\phi|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$ because d being a square-free integer implies $\sqrt{d} \notin \mathbb{Q}$ and so $a + b\sqrt{d} \in \mathbb{Q}$ iff $b = 0$ (since $\left\{1, \sqrt{d}\right\}$ are linearly independent in the $\mathbb{Q}$-vector space $\mathbb{Q}[\sqrt{d}]$, whereas $b = 0$ gives $\phi(a + b\sqrt{d}) = \phi(a) = a$ so that $\phi = \mathrm{id}$ when $a + b\sqrt{d} \in \mathbb{Q}$). We now show ϕ is a ring homomorphism.

- We have $\phi(1) = \phi(1 + 0\sqrt{d}) = 1 - 0\sqrt{d} = 1$, so ϕ preserves the identity.
- We have

$$\begin{aligned}\phi(a + b\sqrt{d}) + \phi(r + s\sqrt{d}) &= a - b\sqrt{d} + r - s\sqrt{d} \\ &= \phi((a + r) + (b + s)\sqrt{d}),\end{aligned}$$

  so ϕ preserves addition.
- We have

$$\phi(a + b\sqrt{d})\phi(r + s\sqrt{d}) = (a - b\sqrt{d})(r - s\sqrt{d})$$

$$\begin{aligned}&= ar - as\sqrt{d} - br\sqrt{d} + bsd\\ &= (ar+bsd) - (as+br)\sqrt{d}\\ &= \phi((ar+bsd) + (as+br)\sqrt{d})\\ &= \phi((a-b\sqrt{d})(r-s\sqrt{d})),\end{aligned}$$

so ϕ preserves multiplication.

Hence ϕ is a ring homomorphism. Lastly we observe that ϕ is an involution, i.e. $\phi^{-1} = \phi\circ\phi$ since $\phi\circ\phi(a+b\sqrt{d}) = \phi(a-b\sqrt{d}) = \phi(a)+\phi(-b)\phi(\sqrt{d}) = a+b\sqrt{d}$. Hence ϕ is a bijection, as we have exhibited an explicit inverse. We have now shown that ϕ is a field isomorphism with $\phi|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$, so in particular ϕ is a field automorphism relative to K. We therefore conclude $\phi \in \mathrm{Gal}(\mathbb{Q}[\sqrt{d}]/\mathbb{Q})$. □

(b) (5 points) Prove that the only elements of $\mathrm{Gal}(\mathbb{Q}[\sqrt{d}]/\mathbb{Q})$ are ϕ and id.
[Hint: think about where an element of $\mathrm{Gal}(\mathbb{Q}[\sqrt{d}]/\mathbb{Q})$ must send $\sqrt{d}$.]

Proof. Let $\psi \in \mathrm{Gal}(\mathbb{Q}[\sqrt{d}]\mathbb{Q})$. Then ψ is a field automorphism relative to $\mathbb{Q}$, so $\psi(\sqrt{d})^2 = \psi(d) = d$ since $d \in \mathbb{Q}$. Hence $\psi(\sqrt{d}) = \pm\sqrt{d}$. Thus we're done if we show $\psi(\sqrt{d}) = +\sqrt{d}$ (resp. $\psi(\sqrt{d}) = -\sqrt{d}$) then $\psi = \mathrm{id}$ (resp. $\psi = \phi$). Indeed, $\psi(\sqrt{d}) = +\sqrt{d}$ implies that for any $r, s \in \mathbb{Q}$ we have $\psi(r+s\sqrt{d}) = \psi(r)+\psi(s)\psi(r\sqrt{d}) = r+s\sqrt{d}$ (resp. $\psi(r+s\sqrt{d}) = \psi(r)+\psi(s)\psi(\sqrt{d}) = r-s\sqrt{d}$), so $\psi = \mathrm{id}$ (resp. $\psi = \phi$) as claimed. We thus conclude $\mathrm{Gal}(\mathbb{Q}[\sqrt{d}]/\mathbb{Q})$ is the group $\{\mathrm{id}, \phi\}$ (and hence $\mathrm{Gal}(\mathbb{Q}[\sqrt{d}/\mathbb{Q}) \cong C_2$, the cyclic group of order 2). □

Exercise 3.25 (2)**.** (10 points) Let $K \subseteq L$ be an algebraic field extension and let T be such that $K \subseteq T \subseteq L$ and such that T is closed under addition and multiplication (so T is a ring). Prove that T is a field.

[Hint: you have to prove that for $t \in T$ nonzero we have $1/t \in T$. How can you use the fact that elements of L are algebraic over K to prove this?]

Proof. $K \subseteq T$ and K is a field means its identity is inherited by T. This together with the closure of T under addition and multiplication along with the distributivity/associativity by virtue of these operations in K, L gives that T is a ring. T is not the zero ring since $K \subseteq T$ and $K \neq \{0\}$ since K is a field. Let $t \in T$ be nonzero. $t \in T \subseteq L$ implies $t \in L$, so t is algebraic over K since L is an algebraic extension of K. Let $f = x^n - a_{n-1}x^{n-1} + \cdots \pm a_0 \in K[x]$ be the minimal polynomial for $t \in L$ over K. Working in the algebraic field extension $K \subseteq L$, we showed in Artin Exercise 15.2.2 (from Homework 5)[3] that $L \ni t^{-1} = a_0^{-1}(t^{n-1} - a_{n-1}t^{n-1} + \cdots \mp a_1)$ (where we know $a_0 \neq 0$ since f is irreducible—if $a_0 = 0$ then we f would reduce as $f = xq$ for some $q \in F[x]$ of smaller

[3] (Artin 15.2.2). Let $f(x) = x^n - a_{n-1}x^{n-1} + \cdots \pm a_0$ be an irreducible polynomial over F, and let α be a root of f in an extension field K. Determine the element α^{-1} explicitly in terms of α and of the coefficients a_i.

degree than f). Hence each scalar here is in T since it is inherited from K (including a_0^{-1} since $a_0 \neq 0$ is in K and K is a field), so we have since T is closed under addition and multiplication that $t^{-1} = pa_0^{-1}(t^{n-1} - a_{n-1}t^{n-2} + \cdots \mp a_1)$ is also in T. Hence T is a ring with all nonzero $t \in T$ units, and thus T is a field as claimed. □

Exercise 3.26 (3)**.** Do the following:

(a) (5 points) Let $K \subseteq L$ be a field extension such that $[L : K]$ is prime. Prove that there are no fields F with $K \subsetneq F \subsetneq L$.

Proof. If $[L : K] = p$ is prime and there were some proper intermediate field F such that $K \subsetneq F \subsetneq L$ are nested field extensions then $[L : F] \geq 2$ (resp. $[F : K] \geq 2$) since $F = L$ iff $[L : F] = 1$ (resp. $K = F$ iff $[F : K] = 1$). By the multiplicative property of the degree we have

$$p = [L : K] = [L : F][F : K],$$

so since p is prime the only possibilities are (i) $[L : F] = p$ and $[F : K] = 1$ or (ii) $[L : F] = 1$ and $[F : K] = p$, but both cases contradicting the assumptions that $K \neq F$ and $F \neq L$. □

(b) (5 points) Let $K \subseteq L$ be a field extension and let $u \in L$ be an element that is algebraic over K and such that the minimal polynomial $f \in K[x]$ for u has odd degree. Prove that $K[u] = K[u^2]$.

Proof. Set $F := K[u^2]$. We have $K \subseteq F \subseteq K[u]$ and $[K[u] : K]$, which we know is the degree of the minimal polynomial f for u over K, is given to be odd. We have

$$[K[u] : K] = [K[u] : F]\ [F : K]$$

by the multiplicative property of the degree, so since the product $[K[u] : K]$ is odd we know both factors $[K[u] : F]$ and $[F : K]$ must be odd.
$F \subseteq K[u]$ and $u^2 \in F$, so we have that the extension $F \subseteq F[u]$ is at most a quadratic extension: indeed, the minimal polynomial g for u over F divides $h := x^2 - u$ because $h(u^2) = 0$, and hence g has degree ≤ 2. $[K[u] : F] \neq 2$ since we know by the above that $[K[u] : F]$ is odd, so $[K[u] : F] = 1$, giving $K[u] = F = K[u^2]$ as desired. □

Exercise 3.27 (4)**.** Compute the minimal polynomials over $\mathbb{Q}$ of the following algebraic numbers:

(a) (2 points) $1 + \sqrt{2}$

Proof. Let $\alpha = 1 + \sqrt{2}$. Note $\alpha(\alpha - 2) - 1 = \alpha^2 - 2\alpha - 1 = 0$, leading us to claim $f := x^2 - 2x - 1 = 0$ is the minimal polynomial for α over $\mathbb{Q}$. If f were reducible then it must split into two linear factors in $\mathbb{Q}[x]$, one of which must be $(x - (1 + \sqrt{2}))$. But $1 + \sqrt{2} \notin \mathbb{Q}$, so f is a monic irreducible with root α. Thus by uniqueness of such a polynomial we conclude f is the minimal polynomial for α over $\mathbb{Q}$. □

(b) (3 points) $\sqrt{1+\sqrt{2}}$

Proof. In the above notation, we claim the minimal polynomial for $\sqrt{1+\sqrt{2}} = \sqrt{\alpha}$ over $\mathbb{Q}$ is $g := f(x^2) = x^4 - 2x^2 - 1$, where f and α are as above. $g(\sqrt{\alpha}) = f(\alpha) = 0$, so since the minimal polynomial divides all elements of $\mathbb{Q}[x]$ with β as a root, the minimal polynomial has degree at most four.

If we show the quartic g is irreducible then it follows that g is a monic irreducible with $\sqrt{\alpha}$ as a root, so as before we are done by uniqueness as such a polynomial. By Lemma B from the first page it suffices to show $g(x-1)$ is an irreducible element of $\mathbb{Q}[x]$. Noting that $g(x-1) = x^4 - 4x^3 + 4x^2 - 2$, if $p = 2$ then $a_4 = 1$ doesn't divide p but p divides the remaining coefficients, and p^2 doesn't divide the constant term. Thus $g(x-1)$ is irreducible by Eisenstein's criterion, and consequently g is an irreducible element in $\mathbb{Q}[x]$, so per our previous remarks we conclude g is the minimal polynomial for $\sqrt{a}$ over $\mathbb{Q}$. □

Exercise 3.28 (5)**.** Consider the polynomials $f(x) = x^2 + 1$ and $g(x) = x^2 + 2x - 1$ in $\mathbb{F}_3[x]$.

(a) (3 points) Prove that $f(x)$ and $g(x)$ are irreducible.

Proof. f is quadratic, so if f were reducible then it would split into two linear terms in $\mathbb{F}_3[x]$, meaning f must have a root in $\mathbb{F}_3$. But $f(0) = 1$, $f(1) = 2$, and $f(2) = 2$, so no such root exists, so f is irreducible Similarly, quadratic g has $g(0) = 2$, $g(1) = 2$, and $g(2) = 1$, so g is irreducible by the same argument. □

(b) (7 points) Let K be obtained by adjoining a root α of $f(x)$ to $\mathbb{F}_3$, and let L be obtained by adjoining a root β of $g(x)$ to $\mathbb{F}_3$. In other words, $K = \mathbb{F}_3[\alpha]$ and $L = \mathbb{F}_3[\beta]$, and

$$f(\alpha) = \alpha^2 + 1 = 0 \quad \text{and} \quad g(\beta) = \beta^2 + 2\beta - 1 = 0$$

Give an explicit isomorphism $\phi : \mathbb{F}_3[\alpha] \to \mathbb{F}_3[\beta]$.

[Hint: the most important thing to decide is what $\phi(\alpha) \in L$ should be - make this explicit and easy to find in your solution, and make sure you explain what you check to make sure that your choice works!.]

Proof. f (resp. g) is a monic polynomial with root α (resp. β) that is irreducible by part (a), so α (resp. β) has minimal polynomial f (resp. g) by uniqueness of such a polynomial. Note that

$$f(\beta+1) = (\beta+1)^2 + 1 = \beta^2 + 2\beta + 2 = (\beta^2 + 2\beta - 1) + 3,$$

and since we're given $\beta^2 - 2\beta - 1 = 0$ and we know $3 = 0$ in $\mathbb{F}_3$, it follows that $f(\beta+1) = 0$, i.e. $\beta+1$ is a root of f. Thus, again invoking uniqueness of the minimal polynomial, we have since f is a monic irreducible that $\beta+1$ has minimal polynomial f as well. This leads us to claim

$$\phi : \mathbb{F}_3[\alpha] \to \mathbb{F}_3[\beta]$$

$$\phi(c_0 + c_1\alpha) := c_0 + c_1(\beta + 1) \tag{$*$}$$

is an isomorphism of fields. To show this, consider arbitrary $x := c_0 + c_1\alpha$ and $x' := c_0' + c_1'\alpha$ (that is, arbitrary elements of $\mathbb{F}_3[\alpha]$, since $[\mathbb{F}_3[\alpha] : \mathbb{F}_3] = \deg f = 2$, the degree of the minimal polynomial of α over $\mathbb{F}_3$, meaning $\{1, \alpha\}$ is a basis for the $\mathbb{F}_3$-vector space $\mathbb{F}_3[\alpha]$, so any element of $\mathbb{F}_3[\alpha]$ is written in this way).
We first note ϕ is well-defined, since if $x = x'$ then necessarily $c_0 = c_0'$ and $c_1 = c_1'$ since $\{1, \alpha\}$ is linearly independent in K so that $\phi(x) = \phi(x')$ by $(*)$ above, as needed.
We now show ϕ is a homomorphism of fields:

- We have $\phi(1) = \phi(1 + 0\alpha) = 1 + 0(\beta + 1) = 1$, so ϕ preserves the identity.
- We have

$$\begin{aligned}\phi(x + x') &= \phi((c_0 + c_0') + (c_1 + c_1')\alpha)\\ &= (c_0 + c_0') + (c_1 + c_1')(\beta + 1)\\ &= \phi(x) + \phi(x'),\end{aligned}$$

  so ϕ preserves addition.
- First note that

$$\begin{aligned}xx' &= (c_0 + c_1\alpha)(c_0' + c_1'\alpha)\\ &= c_0c_0' + c_0c_1'\alpha + c_1c_0'\alpha + c_1c_1'\alpha^2\\ &= (c_0c_0' - c_1c_1') + (c_0c_1' + c_1c_0')\alpha,\end{aligned}$$

  where we used that $\alpha^2 = -1$ in K. Hence $\phi(xx') = (c_0c_0' - c_1c_1') + (c_0c_1' + c_1c_0')(\beta + 1)$. On the other hand, we have

$$\begin{aligned}\phi(x)\phi(x') &= (c_0 + c_1(\beta + 1))(c_0' + c_1'(\beta + 1))\\ &= c_0c_0' + c_0c_1'(\beta + 1) + c_1c_0'(\beta + 1) + c_1c_1'(\beta + 1)^2\\ &= c_0c_0' + c_0c_1' + c_1c_0' + c_1c_1' + c_0c_1'\beta + c_1c_0'\beta + c_1c_1'\beta^2 + 2c_1c_1'\beta\\ &= (c_0c_0' + c_0c_1' + c_1c_0' + c_1c_1') + \beta(c_0c_1' + c_1c_0' + c_1c_1'\beta + 2c_1c_1')\\ &= \beta(c_1c_0' + c_0c_1') + c_0c_0' + c_1c_0' + c_0c_1' + 2c_1c_1'\\ &= (c_0c_1' + c_1c_0')(\beta + 1) + (c_0c_0' - c_1c_1'),\end{aligned}$$

  where we used that $2 = -1$ in $\mathbb{F}_3$ and $\beta^2 = 1 - 2\beta$. This coincides with the above, so we have shown $\phi(xx') = \phi(x)\phi(x')$, and hence ϕ preserves multiplication.

We now show ϕ is bijective. ϕ is injective because $\phi(x) = 0$ iff $c_0 = c_1 = 0$, so ϕ has trivial kernel. ϕ is surjective because the observation that $\phi(a + b\alpha) = a + b\beta + b = a + b + b\beta$ implies by the definition of ϕ in $(*)$ that each $c_0 + c_1\beta \in L$ is the image of $(c_0 - c_1) + c_1\alpha \in K$. We therefore conclude $\mathbb{F}_3[\alpha] \cong \mathbb{F}_3[\beta]$ as witnessed by the isomorphism of fields ϕ.
(We make an additional observation that in fact $\phi|_{\mathbb{F}_3} = \mathrm{id}_{\mathbb{F}_3}$: Indeed, if $x \in \mathbb{F}_3$ then $x = c_0 + 0\alpha$, so $\phi(x) = c_0 + 0(\beta + 1) = c_0$, meaning $\phi|\mathbb{F}_3 = \mathrm{id}_{\mathbb{F}_3}$ since $x \in \mathbb{F}_3$ is

arbitrary. Since $\deg(\alpha) = 2$ and $\mathbb{F}_9 = \mathbb{F}_3[\alpha] \cong \mathbb{F}_3[x]/(f)$, we have by uniqueness of finite fields of order $\mathbb{F}_q$ for $q = p^k$ that in fact $\phi \in \mathsf{Gal}(\mathbb{F}_9/\mathbb{F}_3)$.) □

Exercise 3.29 (6)**.** (5 points) Construct a primitive element for the extension $\mathbb{Q}[\sqrt{2}, \sqrt[3]{2}]$ over $\mathbb{Q}$. Make sure to justify your answer!

Proof. Let $L := \mathbb{Q}[\sqrt{2}, \sqrt[3]{2}]$. We have nested field extensions $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{2}] \subseteq L$ and $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt[3]{2}] \subseteq L$. $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$ and $[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = 3$, so by Artin's Corollary 15.3.8 we have that both 2 and 3 are divisors of and have product at most than $N := [\mathbb{Q}[\sqrt{2}, \sqrt[3]{2}] : \mathbb{Q}]$, meaning $N = 6$.

We claim $\gamma := \sqrt{2} + \sqrt[3]{2}$ is a primitive element for the field extension $\mathbb{Q} \subseteq L$. $\gamma \in L$, so it suffices to show the degree of its minimal polynomial is six (that is, $[\mathbb{Q}[\gamma] : \mathbb{Q}] = 6$), since then this forces $\mathbb{Q}[\gamma] = L$. We have by the multiplicative property of the degree that

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

so it only remains to show $[\mathbb{Q}[\gamma] : \mathbb{Q}[\sqrt{2}]] = 3$. Notice that $(\gamma - \sqrt{2})^3 = 2$, leading us to claim $f := (x - \sqrt{2})^3 - 2$ is the minimal polynomial for γ over $\mathbb{Q}[\sqrt{2}]$.

By Lemma B from the first page it suffices to show $\tau_{-\sqrt{2}} f = ((x+\sqrt{2})-\sqrt{2})^3 - 2 = x^3 - 2$ is irreducible over $\mathbb{Q}[\sqrt{2}]$. Indeed, if $\tau_{-\sqrt{2}} f$ were reducible then it would have a linear factor $(x - (r + s\sqrt{2}))$ for some $r, s \in \mathbb{Q}$ satisfying

$$\begin{aligned} 2 = (r + s\sqrt{2})^3 &= r^3 + 3\sqrt{2}r^2 s + 6rs^2 + 2\sqrt{2}s^3 \\ &= r^3 + 6rs^2 + (3r^2 s + 2s^3)\sqrt{2} \\ &= r(r^2 + 6s^2) + s(3r^2 + s^3)\sqrt{2}, \end{aligned}$$

so since $\{1, \sqrt{2}\}$ is linearly independent in the $\mathbb{Q}[\sqrt{2}]$-vector space $\mathbb{Q}[\sqrt{2}, \sqrt[3]{2}]$ we have the following system of equations:

$$\begin{bmatrix} r(r^2 + 6s^2) = 2 \\ s(3r^2 + s^2) = 0 \end{bmatrix}.$$

The bottom equation forces either $s = 0$ or $3r^2 + s^2 = 0$, so $s = 0$ in any case. Then the top equation gives $r^3 = 2$, but no such $r \in \mathbb{Q}$ exists. It follows that the cubic polynomial $\tau_{-\sqrt{2}} f$ has no linear factors, so per our prior remarks we conclude that the monic polynomial f is irreducible, and since it has γ as a root we conclude by uniqueness of the minimal polynomial that γ is the minimal polynomial for γ over $\mathbb{Q}[\sqrt{2}]$, so by our previous remarks we have γ is a primitive element for the field extension $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{2}, \sqrt[3]{2}]$. □

§3.5 Algebra 4 Homework 8

Exercise 3.30 (Artin 16.1.1)**.** 1.1. Determine the orbit of the polynomial below. If the polynomial is symmetric, write it in terms of the elementary symmetric functions.

(a) $u_1^2u_2 + u_2^2u_3 + u_3^2u_1 \quad (n = 3)$,
(b) $(u_1 + u_2)(u_2 + u_3)(u_1 + u_3) \quad (n = 3)$,
(c) $(u_1 - u_2)(u_2 - u_3)(u_1 - u_3) \quad (n = 3)$,
(d) $u_1^3u_2 + u_2^3u_3 + u_3^3u_1 - u_1u_2^3 - u_2u_3^3 - u_3u_1^3 \quad (n = 3)$,
(e) $u_1^3 + u_2^3 + \cdots + u_n^3$.

Proof. Given each part, let f be its given polynomial, and take $\tau, \sigma \in S_3$ denote $\tau = (12)$ and $\sigma = (123)$.

(a) Observe $(12).f = u_2^2u_1 + u_1^2u_3 + u_3^2u_1 \neq f$, so since similar reasoning holds for arbitrary transpose $\tau \in S_3$ we have that f is not symmetric since it has nontrivial orbit. Any 3-cycle σ has $\sigma f = f$, so a transpose τ is the only permutation in S_3 which generates nontrivial orbit, so we have found the orbit of f in all cases to be order 2 as given.

(b) This is symmetric. Per lecture, we have

$$f = (s_1 - u_1)(s_1 - u_2)(s_1 - u_3) = s_1^3 - s_1s_1^2 + s_2s_1 - s_3 = s_1s_2 - s_3.$$

(c) This is similar (a), the orbits being of order 2 and $(f, \tau.f)$ for a transpose $\tau \in S_3$. Notice that $f = \Delta((x - u_1)(x - u_2)(x - u_3))$ so f is again fixed by A_3. τ just changes the sign of f, so the orbit $S_3f = \{\pm f\}$.

(d) This is essentially previous part, as $\sigma f = f$ and $\tau f = -f$ so the orbit is $S_3f = \{\pm f\}$.

(e) f is symmetric and so has trivial orbit. Clearly we only need s_1, s_2, s_3 in our linear combination in terms of the elementary symmetric polynomials, and we observe that for each i we have $u_i^3 = s_1u_i^2 - s_2u_i + s_3$, so $\sum u_i^3 = s_1 \sum u_i^2 - s_2 \sum u_i + \sum s_3 = s_1(s_1^2 - 2s_2) - s_1s_2 + ns_3$. □

Exercise 3.31 (2)**.** Let K be a field and let $f(x) \in K[x]$ be a monic degree n polynomial. Assume that $K \subseteq L$ is a field extension such that L contains all the roots $\alpha_1, \dots, \alpha_n$ of f, counted with multiplicity. Prove that the discriminant of $f(x)$ satisfies the identity

$$\Delta(f) = (-1)^{\binom{n}{2}} \prod_{i=1}^{n} f'(\alpha_i)$$

Proof. Where $f = \prod_{k=1}^{n}(x - \alpha_k) \in K[x]$, we apply the product rule for n factors to get that

$$f'(x) = \frac{d}{dx}\left(\prod_{k=1}^{n}(x - \alpha_k)\right) = \sum_{k=1}^{n} \prod_{\substack{1 \le j \le n \\ j \neq k}} (x - \alpha_j).$$

Thus $f'(\alpha_i) = \sum_{k=1}^{n}(\alpha_i - \alpha_k) \prod_{\substack{1 \le j \le n \\ j \neq k}}(\alpha_i - \alpha_j)$. The product above is zero if $k \neq i$, leaving only the $k = i$ term in the sum. Thus,

$$\begin{aligned}
\prod_{i=1}^{n} f'(\alpha_i) &= \prod_{i=1}^{n} \prod_{\substack{1 \le j \le n \\ j \neq i}} (\alpha_i - \alpha_j) \\
&= \prod_{i=1}^{n}\left(\left(\prod_{1 \le j < i}(\alpha_i - \alpha_j)\right)\left(\prod_{i < j \le n}(\alpha_i - \alpha_j)\right)\right) \\
&= \prod_{i=1}^{n}\left((-1)^{i-1}\left(\prod_{1 \le j < i}(\alpha_j - \alpha_i)\right)\left(\prod_{i < j \le n}(\alpha_i - \alpha_j)\right)\right) \\
&= (-1)^{\binom{n}{2}} \prod_{i=1}^{n}\left(\left(\prod_{1 \le j < i}(\alpha_j - \alpha_i)\right)\left(\prod_{i < j \le n}(\alpha_i - \alpha_j)\right)\right) \\
&= (-1)^{\binom{n}{2}}\left(\prod_{i=1}^{n}\prod_{1 \le j < i}(\alpha_j - \alpha_i)\right)\left(\prod_{i=1}^{n}\prod_{i < j \le n}(\alpha_i - \alpha_j)\right) \quad \text{(index flip)} \\
&= (-1)^{\binom{n}{2}}\left(\prod_{j=1}^{n}\prod_{1 \le i < j}(\alpha_i - \alpha_j)\right)\left(\prod_{i=1}^{n}\prod_{i < j \le n}(\alpha_i - \alpha_j)\right) \quad \text{(index flip)} \\
&= (-1)^{\binom{n}{2}}\left(\prod_{1 \le i < j \le n}(\alpha_i - \alpha_j)\right)\left(\prod_{1 \le i < j \le n}(\alpha_i - \alpha_j)\right) \\
&= (-1)^{\binom{n}{2}} \prod_{1 \le i < j \le n}(\alpha_i - \alpha_j)^2 = (-1)^{\binom{n}{2}}\Delta(f),
\end{aligned}$$

and multiplying through by $(-1)^{\binom{n}{2}}$ gives the result. □

Exercise 3.32 (3)**.** Let $f(x) = x^5 + px + q$, with p, q elements of a field K. Prove that the discriminant of f satisfies $\Delta(f) = 5^5q^4 + 4^4p^5$.

Proof. First consider the case 0 is a root of f. Then $q = 0$, so $f(\alpha_i) = 0$ implies $\alpha_i^5 + p\alpha_i = 0$, so $\alpha_i = 0$ or $\alpha_i^4 = -p$. Then the previous exercise gives

$$\Delta(f) = (-1)^{\binom{5}{2}} \prod\nolimits_{i=1}^{5} f'(\alpha_i) = (-1)^{10} \prod\nolimits_{i=1}^{n} (5\alpha_i^4 + p) = p \prod\nolimits_{i=1}^{5} (-4p) = 4^5p^5 + 5^5q^4,$$

affirming the claim. Now suppose f has nonzero roots. Then $q \neq 0$, so if α_i is a root then $f(\alpha_i) = \alpha_i^5 + p\alpha_i = -q$, so $5\alpha_i^5 + 5p\alpha_i = -5q$, so $\alpha_i(5\alpha_i^4 + p) = -4p\alpha_i - q$, which gives that $5\alpha_i^4 + p = -4p - q\alpha_i^{-1} = \frac{-q-4p\alpha_i}{\alpha_i} = \frac{1}{\alpha_i}(4p)(-\frac{q}{4p} - \alpha_i)$. Thus

$$\begin{aligned}\Delta(f) &= (-1)^{\binom{5}{2}} \prod\nolimits_{i=1}^{5} f'(\alpha_i) = \frac{4^5p^5}{\prod_{i=1}^{5} \alpha_i} \prod\nolimits_{i=1}^{5} (-\frac{q}{4p} - \alpha_i) \\ &= \frac{4^5p^5}{(-1)^5 q} f(-q/4p) = 5^5q^4 + 4^4p^5,\end{aligned}$$

as desired. □

Exercise 3.33 (4)**.** Say that a field extension $K \subseteq L$ is a ***normal extension*** if all irreducible polynomials $f(x) \in K[x]$ which have a root in L split into linear factors in L. If $K \subseteq L$ is finite, we proved in class that this holds if and only if $K \subseteq L$ is the splitting field of some polynomial. Let $\alpha \in \mathbb{R}$ satisfy $\alpha^4 = 5$.

Are the following extensions normal or not?

(a) $\mathbb{Q} \subseteq \mathbb{Q}(i\alpha^2)$

(b) $\mathbb{Q}(i\alpha^2) \subseteq \mathbb{Q}(\alpha + i\alpha)$. You should also justify that this is indeed a field extension.

(c) $\mathbb{Q} \subseteq \mathbb{Q}(\alpha + i\alpha)$.

Proof. (a) $f := x^2 + 5$ splits completely over $\mathbb{Q}(i\alpha^2)$ and any field in which f does so must contain $i\alpha^2$, so by the characterization we conclude this is a normal extension.

(b) First notice $\alpha \in \mathbb{R}$, so $\alpha^2 \in \mathbb{R}$, and since $\alpha^2 > 0$ and α^2 squares to 5, we conclude $\alpha^2 = \sqrt{5}$. Thus $\mathbb{Q}(i\alpha^2) = \mathbb{Q}(\sqrt{-5})$. Now, $\mathbb{Q}(\sqrt{-5}) \subseteq \mathbb{Q}(\alpha + i\alpha)$ is a field extension because $(\alpha + i\alpha)^2 = 2\sqrt{-5} \in \mathbb{Q}(\sqrt{-5})$.

This is a normal extension since the minimal polynomial for $\alpha + i\alpha$ over $\mathbb{Q}(\sqrt{-5})$ is $g := x^2\sqrt{-5} + 10$ since $g(\alpha + i\alpha) = \sqrt{-5}(\alpha^2)(1+i)^2 + 10 = 0$, and g is irreducible over $\mathbb{Q}(\sqrt{5})$. Clearly $-\alpha - i\alpha$ is also a root and is in the extension, so g splits completely, and that it is a splitting field is obvious since the field is $\mathbb{Q}(\alpha + i\alpha)$ and we are concerned with the minimal polynomial of $\alpha + i\alpha$, so the extension is normal.

(c) We claim this is not a normal extension. Since $i \notin \mathbb{R}$ and $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$ thanks to $\alpha \in \mathbb{R}$, we know that $\mathbb{Q}[\alpha]$ is a splitting field for $f := x^4 - 5 \in \mathbb{Q}[x]$ (which is irreducible by Eisenstein), and hence $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4]$, so $[\mathbb{Q}(\alpha, i) : \mathbb{Q}] = 8$. Now, it suffices to show that $\gamma := \alpha(1+i)$ has minimal polynomial g over $\mathbb{Q}$ which does not split completely in $\mathbb{Q}(\gamma)$.

First note $\gamma^4 = -20$ and so $x^4 + 20 \in \mathbb{Q}[x]$ has γ as a root. Thus $[\mathbb{Q}(\gamma) : \mathbb{Q}] \leq 4$. But $\mathbb{Q}(\alpha, i) = \mathbb{Q}(\alpha(1+i), i) = \mathbb{Q}(\gamma)(i)$, whereas $x^2 + 1 \in \mathbb{Q}(\gamma)[x]$. Hence $8 = [\mathbb{Q}(\alpha, i) : \mathbb{Q}] = [\mathbb{Q}(\gamma)(i) : \mathbb{Q}(\gamma)] = 2$ and $[\mathbb{Q}(\gamma) : \mathbb{Q}] = 4$, whereas $i \notin \mathbb{Q}(\gamma)$, but $g(i\gamma) = 0$, meaning g does not split completely over $\mathbb{Q}$.

□

Exercise 3.34 (Artin 16.3.2)**.** Determine the degrees of the splitting fields of the following polynomials over $\mathbb{Q}$:
(a) $x^3 - 2$, (b) $x^4 - 1$, (c) $x^4 + 1$.

Proof. (a) Note $\sqrt[3]{2}$ is a root of $f := x^3 - 2$, but $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$ so that the complex roots of f are not in this extension, so the degree of the splitting field is strictly greater than $\deg(f) = 3$. Recall that we showed on the last homework that if $f \in K[x]$ is a monic of degree n and $K \subseteq L$ is a splitting field for f then $[L : K]$ divides $n!$. so the degree of the splitting field divides $3! = 6$, forcing the degree of the splitting field to be six.

(b) Note $f := x^4 - 1 = (x^2 + 1)(x^2 - 1)$ has roots $\pm i, \pm 1$, so the extension is at most quadratic since these sit in $\mathbb{Q}(i)$, a degree 2 extension. It can't be a degree 1 extension since $i \notin \mathbb{Q}$, so we conclude the degree is 2.

(c) Where ω is a primitive eighth root of unity, notice that $\omega, \omega^3, \omega^5, \omega^7$ are distinct roots of $x^4 + 1$. Any field $L \supseteq \mathbb{Q}$ containing one, therefore, contains the other three; therefore—hence $\mathbb{Q}[\omega]$ is a splitting field for $x^4 + 1$. We conclude that the extension is degree 4 since we know the minimal polynomial for ω has degree 4 over $\mathbb{Q}$. □

Exercise 3.35 (Artin 16.4.1)**.** (a) Determine all automorphisms of the field $\mathbb{Q}(\sqrt[3]{2})$, and of the field $\mathbb{Q}(\sqrt[3]{2}, \omega)$, where $\omega = e^{2\pi i/3}$.

(b) Let K be the splitting field over $\mathbb{Q}$ of $f := (x^2 - 2x - 1)(x^2 - 2x - 7)$. Determine all automorphisms of K.

Proof. (a) $\mathbb{Q}(\sqrt[3]{2})$: Where $f := x^3 - 2$, we know since $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}]$ is a real extension and $\sqrt[3]{2}$ is the only real root of f that since any such automorphism σ maps roots to roots it then must map $\sqrt[3]{2}$ to itself. hence $\sigma = \text{id}$.

$\mathbb{Q}(\sqrt[3]{2}, \omega)$: $\omega^3 = 1$, so $x^3 - 1 = (x-1)(x^2 + x + 1)$ has ω as a root. Any automorphism σ maps roots to roots, so since σ is determined by the image of $\sqrt[3]{2}$ and ω, there are six possibilities (since $\sigma(\sqrt[3]{2})$ is either $\sqrt[3]{2}$ or one of the two complex roots of $x^3 - 2$ and $\sigma(\omega) = \pm\omega$.

We have the nested field extensions $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt[3]{2}, \omega)$. If $\sigma \in \text{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}(\sqrt[3]{2})$ then $\sqrt[3]{2} \to \sqrt[3]{2}$ is forced and either $\omega \mapsto \omega$ or $\omega \mapsto \omega^2$, so the Galois group of this extension is isomorphic to the subgroup $\{1, \tau\}$ of S_3, where $\tau \in S_3$ is a transposition.

Also note that $\mathbb{Q}(\omega)$ is an intermediate field extension, i.e. $\mathbb{Q} \subseteq \mathbb{Q}(\omega) \subseteq \mathbb{Q}(\sqrt[3]{2}, \omega)$, so the automorphisms in $\text{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}(\omega))$ all have $\omega \mapsto \omega$ and there are three choices of the image of $\sqrt[3]{2}$, each corresponding to the roots of $x^3 - 2$, so this Galois group is isomorphic to the subgroup $\{1, \sigma, \sigma^2\}$, where $\sigma \in S_3$ is a (the) cyclic permutation. It follows that (3)(2) divides the order of $\text{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q})$, and since $|S_3| = 6$ we conclude it must be six, and hence isomorphic to S_3, i.e. for $\tau \in S_3$ and $\sigma \in S_3$ as given we have $\text{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}) \cong \{1, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\} = S_3$.

(b) Note f splits completely in $\mathbb{Q}[\sqrt{2}]$ since f has roots $1 \pm \sqrt{2}$ and $1 \pm 2\sqrt{2}$ which are in $\mathbb{Q}[\sqrt{2}]$, and any field containing these roots must contain $\sqrt{2}$, so this is indeed the splitting field. 2 is a square-free element of $\mathbb{Q}$, so we recall from the first midterm that $\text{Gal}(\mathbb{Q}[\sqrt{2}]/\mathbb{Q}) = \{\text{id}, \phi\}$, where ϕ is the conjugation map $a + b\sqrt{2} \mapsto a - b\sqrt{2}$, so these are the only two such automorphisms. □

§3.6 Algebra 4 Homework 9

Exercise 3.36 (Artin 16.6.1)**.** Let α be a complex root of the polynomial $x^3 + x + 1$ over $\mathbb{Q}$, and let K be a splitting field of this polynomial over $\mathbb{Q}$. Is $\sqrt{-31}$ in $\mathbb{Q}(\alpha)$? Is it in K?

Proof. $f := x^3 + x + 1$ is irreducible over $\mathbb{Q}$ since its projection into $\mathbb{F}_2[x]$ is irreducible is irreducible $\mathbb{F}_2[x]$, so the minimal polynomial of α over $\mathbb{Q}$ is f. Thus $|\mathbb{Q}(\alpha) : \mathbb{Q}| = \deg(f) = 3$, whereas for $\beta := \sqrt{-31}$ we have $|\mathbb{Q}(\beta) : \mathbb{Q}| = 2$. Then by the multiplicative property of the degree we have

$$|\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)| = \frac{|\mathbb{Q}(\alpha, \beta) : \mathbb{Q}|}{|\mathbb{Q}(\alpha) : \mathbb{Q}|} \text{ and } |\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\beta)| = \frac{|\mathbb{Q}(\alpha, \beta) : \mathbb{Q}|}{|\mathbb{Q}(\beta) : \mathbb{Q}|},$$

so

$$|\mathbb{Q}(\alpha,\beta) : \mathbb{Q}(\alpha)| = \frac{|\mathbb{Q}(\alpha,\beta) : \mathbb{Q}|}{2} \neq \frac{|\mathbb{Q}(\alpha,\beta) : \mathbb{Q}|}{3} = |\mathbb{Q}(\alpha,\beta) : \mathbb{Q}(\beta)|.$$

Thus $|\mathbb{Q}(\alpha,\beta) : \mathbb{Q}(\alpha)| \neq |\mathbb{Q}(\alpha,\beta) : \mathbb{Q}(\beta)|$, so $\beta \notin \mathbb{Q}(\alpha)$.

On the other hand, $\Delta(f) = -4(1)^3 - 27(1) = -31$ and the square root of the discriminant is a product of differences of elements in K (since f splits completely over K), so $\sqrt{-31} = \sqrt{\Delta(f)} \in K$. □

Lemma 3.37.

If K is perfect and $L = K(\sqrt{d_1}, \ldots, \sqrt{d_n})$ for pairwise coprime square-free $d_i \in K$ then L/K is a Galois extension of degree 2^n and

$$\mathrm{Gal}(L/K) = \langle \sigma_1, \cdots, \sigma_n \rangle \cong \bigoplus_{i=1}^{n} C_2,$$

where $\sigma_i : L \to L$ the field automorphism determined by $\sigma(\sqrt{d_i}) := -\sqrt{d_i}$.

Proof. We first show L is a splitting field over K. If $f := (x^2 - d_1) \cdots (x^2 - d_n)$ then f splits completely in L, so it suffices to show any intermediate field in which f splits completely is a subfield of L. If F were such a subfield then $\sqrt{d_1}, \ldots, \sqrt{d_n} \in F$, so since $K \subseteq F$ implies $L = K(\sqrt{d_1}, \ldots, \sqrt{d_n}) \subseteq F(\sqrt{d_1}, \ldots, \sqrt{d_n})$. Then $F \subseteq L$ and $L \subseteq F$, $F = L$, so L is a splitting field over K per our initial remark. Since K is perfect the extension is Galois.

We now show $|L : K| = 2^n$ and $\mathrm{Gal}(L/K) \cong \bigoplus_{i=1}^{n} C_2$ by induction on $n \geq 1$. We first show the base case $n = 1$. We already know $K \subseteq K(\sqrt{d_1})$ for square-free $d_1 \in K$ is a quadratic extension, so $|L : K| = 2$. The extension L/K is Galois by the above argument, so $|G| = |L : K| = 2$, forcing $G \cong C_2$. We know that the Galois group of a quadratic extension $K \subseteq K(\sqrt{d_1})$ is $\{\mathrm{id}, \sigma_1\}$, so the base case holds.

For the induction step we begin by setting $K' := K(\sqrt{d_1}, \ldots, \sqrt{d_{n-1}})$. Because the $\sqrt{d_i}$ are pairwise we know $K' \subseteq K'(\sqrt{d_n}) = L$ is a proper quadratic extension. Then by the multiplicative property of the degree and the induction hypothesis we have

$$|L : K| = |L : K'||K' : K| = 2(2^{n-1}) = 2^n \tag{$*$}$$

and $\mathrm{Gal}(K'/K) = \langle \sigma_1, \cdots, \sigma_{n-1} \rangle \cong \bigoplus_{i=1}^{n-1} C_2$. We note that $\mathrm{Gal}(K'/K) < G$ with $|G : \mathrm{Gal}(K'/K)| = |L : K'| = 2$. For each $\sigma \in \mathrm{Gal}(K'/K)$ we have that both $\sigma, \sigma\sigma_n \in G$. This gives us 2^n automorpshims in G, and hence is all of G since $|G| = |L : K| = 2^n$ (by $(*)$). From this and the fact that $\mathrm{Gal}(K'/K) = \langle \sigma_1, \ldots, \sigma_{n-1} \rangle$ by the induction hypothesis, we have $G = \langle \sigma, \sigma_n : \sigma \in \mathrm{Gal}(K'/K) \rangle = \langle \sigma_1, \ldots, \sigma_n \rangle$. The σ_i act nontrivially on the disjoint subfields $K(\sqrt{d_i})$ of L, and hence the σ_i commute. Hence $G = \langle \sigma_1, \ldots, \sigma_n \rangle = \langle \sigma_1, \ldots, \sigma_{n-1} \rangle \oplus \langle \sigma_{n-1} \rangle$, where the direct sum is understood as each $\sigma \in G$ takes the form $\sigma = ab$ for some $a \in \langle \sigma_1, \ldots, \sigma_n \rangle \cong \bigoplus_{i=1}^{n-1} C_2$ and $b \in \langle \sigma_n \rangle \cong C_2$. It follows that $G \cong \bigoplus_{i=1}^{n-1} C_2 \oplus C_2 = \bigoplus_{i=1}^{n} C_2$. This completes the proof of the lemma. □

Exercise 3.38 (Artin 16.6.2)**.** Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$. Determine $|K : \mathbb{Q}|$, prove that K is a Galois extension of $\mathbb{Q}$, and determine its Galois group.

Proof. As an immediate application of the above lemma, K is a Galois extension of $\mathbb{Q}$ with $|K : \mathbb{Q}| = 2^3 = 8$ and $\mathrm{Gal}(K/\mathbb{Q}) \cong C_2 \oplus C_2 \oplus C_2$. □

Exercise 3.39 (Artin 16.7.2)**.** Let K/F be a Galois extension such that $\mathrm{Gal}(K/F) \cong C_2 \oplus C_{12}$. How many intermediate fields

$$F \subseteq L \subseteq K$$

are there in the following cases?

(a) $|L : F| = 4$.

Proof. Set $G := \mathrm{Gal}(K/F)$. An intermediate field $F \subseteq L \subseteq K$ corresponding to a subgroup $H < G$ satisfies $|L : F| = |G : H|$, so $|G : H| = 4$, so $4|H| = |G|$, giving $|H| = 6$. There are exactly three such subgroups of G, namely $\{0\} \oplus C_6$, $C_2 \oplus C_3$, and $\langle (1, 2)\rangle = \{(0, 0),(1, 2),(0, 4),(1, 6),(0, 8),(1, 10)\}$. Hence there are exactly three intermediate fields $F \subseteq L \subseteq K$ with $|L : F| = 4$. □

(b) $|L : F| = 9$.

Proof. Set $G := \mathrm{Gal}(K/F)$. An intermediate field $F \subseteq L \subseteq K$ corresponding to a subgroup $H < G$ satisfies $|L : F| = |G : H|$, so $|G : H| = 9$, so $9|H| = |G| = 24$. Thus H is not a group, meaning there are no such intermediate fields. □

(c) $\mathrm{Gal}(K/L) \cong C_4$.

Proof. Set $G := \mathrm{Gal}(K/F)$. If $K/L/F$ and L corresponds to the subgroup H of G then $H \cong \mathrm{Gal}(K/L) \cong C_4$, so it suffices to determine how many subgroups of $\mathrm{Gal}(K/F) \cong C_2 \oplus C_{12}$ are isomorphic to C_4. There are exactly two such subgroups, namely $\langle(0, 3)\rangle$ and $\langle(1, 3)\rangle$. Hence exactly two intermediate fields $F \subseteq L \subseteq K$ with $\mathrm{Gal}(K/L) \cong C_4$ exist. □

Exercise 3.40 (Artin 16.7.4)**.** Let $F = \mathbb{Q}$ and $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$. Determine all intermediate fields $F \subseteq L \subseteq K$.

Proof. $\sqrt{2}, \sqrt{3}, \sqrt{5} \in \mathbb{Q}$ are coprime and square-free, so in the notation of and by the lemma we have $G := \mathrm{Gal}(K/F) = \langle \sigma_1, \sigma_2, \sigma_3 \rangle \cong C_2 \oplus C_2 \oplus C_2$.

- The trivial subgroup of G corresponds to K whereas G itself corresponds to F.
- G has exactly seven subgroups H of order 2, namely $\langle \sigma_i \rangle$ $(1 \leq i \leq 3)$, $\langle \sigma_i \sigma_j \rangle$ $(1 \leq i < j \leq 3)$, and $\langle \sigma_1 \sigma_2 \sigma_3 \rangle$. It follows that there are exactly seven fields L with $F \subseteq L \subseteq K$ and $|K : L| = |G : H| = 4$.
- G has exactly seven subgroups H of order 4, namely $\langle \sigma_i, \sigma_j \rangle$ $(1 \leq i \neq j \leq 3)$, $\langle \sigma_i, \sigma_j \sigma_k \rangle$ $(1 \leq i \neq j \neq k \leq 3)$, and $\langle \sigma_1 \sigma_2, \sigma_1 \sigma_3 \rangle$. It follows that there are exactly seven fields L with $F \subseteq L \subseteq K$ and $|K : L| = |G : H| = 4$.

Since the intermediate in the below table have the given degrees $|K : L|$ and contain the correct number fields per the above argument, it follows that the table gives all intermediate fields $F \subseteq L \subseteq K$. □

$\lvert K : L \rvert = 1$	$\lvert K : L \rvert = 2$	$\lvert K : L \rvert = 4$	$\lvert K : L \rvert = 8$
L	$\mathbb{Q}(\sqrt{2})$	$\mathbb{Q}(\sqrt{2}, \sqrt{3})$	F
	$\mathbb{Q}(\sqrt{3})$	$\mathbb{Q}(\sqrt{2}, \sqrt{5})$	
	$\mathbb{Q}(\sqrt{5})$	$\mathbb{Q}(\sqrt{2}, \sqrt{15})$	
	$\mathbb{Q}(\sqrt{6})$	$\mathbb{Q}(\sqrt{3}, \sqrt{5})$	
	$\mathbb{Q}(\sqrt{10})$	$\mathbb{Q}(\sqrt{3}, \sqrt{10})$	
	$\mathbb{Q}(\sqrt{15})$	$\mathbb{Q}(\sqrt{5}, \sqrt{6})$	
	$\mathbb{Q}(\sqrt{30})$	$\mathbb{Q}(\sqrt{6}, \sqrt{10})$	

Table 1: Intermediate Fields of $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$

Exercise 3.41 (Artin 16.7.7)**.**

(a) Determine the minimal polynomial for $i + \sqrt{2}$ over $\mathbb{Q}$.

Proof. Note $(i+\sqrt{2})^4 - 2(i+\sqrt{2})^2 + 9 = 0$, so we claim the monic $f := x^4 - 2x^2 + 9$ is the minimal polynomial for $(i+\sqrt{2})$. $(i+\sqrt{2})^2 = 1 + 2i\sqrt{2}$ and $(i+\sqrt{2})^3 = 5i - \sqrt{2}$, so f is not a root of any polynomial in $\mathbb{Q}[x]$ of degree ≤ 3. It then only remains to show f is irreducible. $f \in K$

We now show f is irreducible over $\mathbb{Q}$. Note $f = (x^2)^2 - 2(x^2) + 9$, so if $g := x^2 - 2x + 9$ then $\Delta(g) = 4 - 4(9) < 0$, meaning g (and hence $f = g(x^2)$) has no real roots. Thus f must split into quadratic factors, say as $f = (x^2 + ax + b)(x^2 + cx + d)$ for $a, b, c, d \in \mathbb{Q}$. Then $f = x^4 + x^3(a+c) + x^2(ac+b+d) + x(ad+bc) + bd = x^4 - 2x^2 + 9$, so $a = -c$, $ac + b + d = -2$, $ad = -bc$, and $bd = 9$, which easily leads to a contradiction. □

(b) Prove that the set $(1, i, \sqrt{2}, i\sqrt{2})$ is a basis for $\mathbb{Q}(i, \sqrt{2})$ over $\mathbb{Q}$.

Proof. $\mathbb{Q} \subseteq \mathbb{Q}(i)$ and $\mathbb{Q}(i) \subseteq \mathbb{Q}(i, \sqrt{2})$ are quadratic extensions, so it follows that $|\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}| = 4$. Since $(1, i, \sqrt{2}, i\sqrt{2})$ spans $\mathbb{Q}(i, \sqrt{2})$ as a $\mathbb{Q}$-vector space and has four elements, it is a basis. □

Exercise 3.42 (Artin 16.7.11)**.** Let $\alpha = \sqrt[3]{2}$, $\beta = \sqrt{2}$, and $\gamma = \alpha + \beta$. Let $L := \mathbb{Q}(\alpha, \beta)$, and let K be the splitting field of the polynomial $g := (x^3 - 2)(x^2 - 3)$ over $\mathbb{Q}$.

(a) Determine the minimal polynomial for γ over $\mathbb{Q}$, and its roots in $\mathbb{C}$.

Proof. Since $2 = \alpha^3 = (\gamma - \beta)^3$, we have that $2 = \gamma^3 - 3\gamma^2\beta + 3\gamma\beta^2 - \beta^3 = \gamma^3 - 3\gamma^2\beta + 6\gamma - 2\beta$, and so solving for β we find $\beta = (\gamma^3 + 9\gamma - 2)/(3\gamma^2 + 3)$, so $\gamma \in \mathbb{Q}(\alpha, \beta)$, meaning $\mathbb{Q}(\gamma) = \mathbb{Q}(\alpha, \beta)$, so γ has degree six over $\mathbb{Q}$. If we consider $f := ((x - \beta)^3 - 2)((x + \beta)^3 - 2) = x^6 - 9x^4 - 4x^3 + 27x^2 - 36x - 23$. It must be the minimal polynomial for γ since we know it has degree 6 and $f(\gamma) = (\alpha^3 - 2)((\alpha + 2\beta)^3 - 2) = 0$, f is monic, and it must be irreducible since otherwise the degree of γ over $\mathbb{Q}$ must be less than six. In summary, $f \in \mathbb{Q}[x]$ given by

$$f := x^6 - 9x^4 - 4x^3 + 27x^2 - 36x - 23$$

is the minimal polynomial for γ over $\mathbb{Q}$, and since $f = ((x - \beta)^3 - 2)((x + \beta)^3 - 2)$ we see f has roots $\omega^j\alpha \pm \beta$ over $\mathbb{C}$ for $\omega = e^{2\pi i/3}$. □

(b) Determine the Galois group of $K/\mathbb{Q}$.

Proof. We first show $L = K(i)$. Observe that $L(i)$ contains α, β and the roots of g are $\omega, \omega^2, \sqrt[3]{2}$, and $\pm\sqrt{3}$ for and $\omega = e^{2\pi i/3} = \cos(2\pi/3) + i \sin(2\pi/3) = -1/2 + i\sqrt{3}/2 \in K = \mathbb{Q}(\omega, \sqrt[3]{2}, \sqrt{3})$, so $L \subsetneq K \subseteq L(i)$, and $|L(i) : L| = 2$ forces $K = L(i)$. Set $G := \mathrm{Gal}(K/\mathbb{Q})$. We now show $|G| = 12$. $K/\mathbb{Q}$ is a Galois extension since K is by definition a splitting field over $\mathbb{Q}$, so $|G| = |K : \mathbb{Q}|$. By the above we know $|K : L| = 2$ and we already know $|L : \mathbb{Q}| = 6$, so $|G| = |K : \mathbb{Q}| = |K : L||L : \mathbb{Q}| = 12$. Recall that there are exactly five groups of order 12 up to isomorphism, namely C_{12}, $C_6 \oplus C_2$, $S_3 \oplus C_2$, A_4, or $\mathrm{Dic}_3 = \langle a, x : a^6 = 1,\ x^2 = a^3, x^{-1}ax = a^{-1}\rangle$. We now study the subgroups of G.

- The intermediate field $L = \mathbb{Q}(\alpha, \beta)$ has degree 6 over $\mathbb{Q}$ as argued in part (a), so its corresponding subgroup H^* has index $|G : H^*| = 6$ and hence order 2. The extension $L/\mathbb{Q}$ is not a splitting field since $\mathbb{Q} \subseteq L$ is a real extension whereas the minimal polynomial of $\alpha = \sqrt[3]{2}$ must have the complex ω as a root, so $L/\mathbb{Q}$ is not a Galois extension. Therefore, the subgroup H corresponding to L is not normal in G.
- The intermediate field $\mathbb{Q}(\beta)$ has degree 2 over $\mathbb{Q}$, so its corresponding subgroup $H := \mathrm{Gal}(K/\mathbb{Q}(\beta))$ has index $|G : H| = |\mathbb{Q}(\beta) : \mathbb{Q}| = 2$. Hence H is a normal subgroup of G that has order 6.
- The intermediate field $\mathbb{Q}(\alpha)$ has degree 3 over $\mathbb{Q}$, so its corresponding subgroup $H' := \mathrm{Gal}(K/\mathbb{Q}(\beta))$ has index $|G : H'| = |\mathbb{Q}(\alpha) : \mathbb{Q}| = 3$, so H' is a subgroup

of G with order 4. $\mathbb{Q}(\alpha)/\mathbb{Q}$ is not a Galois extension since it is not a splitting field over $\mathbb{Q}$—indeed, if it were then by the fundamental theorem of splitting fields we have that the irreducible $x^3 - 2 \in \mathbb{Q}[x]$ which has root α in $\mathbb{Q}(\alpha)$ splits completely in $\mathbb{Q}(\alpha)$, contradicting that $\mathbb{Q} \subseteq \mathbb{Q}(\alpha)$ is a real extension and hence does not contain the complex roots ω, ω^2 ($\omega = e^{2\pi i/3} \notin \mathbb{R}$). It follows that the subgroup $H'' := \mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ is a non-normal subgroup of order 6 in G.

- The intermediate field $\mathbb{Q}(\alpha, \omega)$, the splitting field of $x^3 - 2$, has degree 6 over $\mathbb{Q}$—indeed, $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\alpha)(\omega) = \mathbb{Q}(\alpha, \omega)$ is a quadratic extension since ω has minimal polynomial $x^2 + x + 1$ over $\mathbb{Q}$, which gives us that $|\mathbb{Q}(\alpha, \omega) : \mathbb{Q}| = |\mathbb{Q}(\alpha, \omega) : \mathbb{Q}(\alpha)||\mathbb{Q}(\alpha) : \mathbb{Q}| = (2)(3) = 6$ by the multiplicative property of the degree. The subgroup corresponding to $\mathbb{Q}(\alpha, \omega)$, $H^{**} := \mathrm{Gal}(\mathbb{Q}(\alpha, \omega)/\mathbb{Q})$, then has index $|G : H^{**}| = 6$ and hence order 2. $\mathbb{Q}(\alpha, \omega)$ is distinct from the other intermediate fields since it is the only one which is a splitting field for $x^3 - 2$, and in particular this gives us that the fixed field of H^{**} is distinct from the fixed fields of the subgroups H, H', H^*, G, and the trivial subgroup.

G can't be abelian since by the third point above we know H'' is not a normal subgroup of G (since all subgroups of abelian groups must be normal). It follows that $G \ncong C_{12}$ and $G \ncong C_3 \oplus C_2 \oplus C_2$, leaving only A_4, $S_3 \oplus C_2$, and Dic_3 as possibilities (where $\mathrm{Dic}_n \cong \langle a, x : a^{2n} = 1,\ x^2 = a^n,\ x^{-1}ax = a^{-1}\rangle$). By the second point we know G has a subgroup of order 6, ruling out A_4 which has no such subgroup.

We showed in the first and last points above that H and H^{**} are distinct subgroups of G of order 2, so since Dic_3 only has one subgroup of order two it follows that it follows that $G \cong S_3 \oplus C_2$. □

§3.7 Algebra IV Final

Exercise 3.43 (1)**.** Let $L = \mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}]$.

(a) (5 points) Prove that $\mathbb{Q} \subseteq L$ is a Galois extension and calculate its Galois group G.

Proof. Notice that 2 is square-free in $\mathbb{Q}$, 3 is square-free in $\mathbb{Q}(\sqrt{2})$, and 5 is square-free in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Thus, $\mathbb{Q} \subsetneq \mathbb{Q}(\sqrt{2}) \subsetneq \mathbb{Q}(\sqrt{2}, \sqrt{3}) \subsetneq \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) = L$ is a chain of quadratic extensions. Then by the multiplicative property of the degree,

$$|L : \mathbb{Q}| = |L : \mathbb{Q}(\sqrt{2}, \sqrt{3})||\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})||\mathbb{Q}(\sqrt{2}) : \mathbb{Q}| = 2^3. \qquad (*)$$

Thus $\mathbb{Q} \subseteq L$ is a finite extension over $\mathbb{Q}$, a field of characteristic zero, and hence a perfect field. It is then enough to show that L is a splitting field over $\mathbb{Q}$, from which it will follow that $\mathbb{Q} \subseteq L$ is a Galois extension by the splitting field characterization. Notice that $f := (x^2 - 2)(x^2 - 3)(x^2 - 5) \in \mathbb{Q}[x]$ splits completely over L. On the other hand, suppose f splits completely over an extension $\mathbb{Q} \subseteq K$. Then K contains

$\sqrt{2}, \sqrt{3}, \sqrt{5}$, so $L = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) \subseteq K(\sqrt{2}, \sqrt{3}, \sqrt{5}) = K$. Thus K contains L as a subfield, so L is a splitting field for f over $\mathbb{Q}$. Thus $\mathbb{Q} \subseteq L$ is a Galois extension.

Let $G := \mathrm{Gal}(L/\mathbb{Q})$. $\mathbb{Q} \subseteq L$ is a Galois extension, so by the degree characterization and $(*)$ we know $|G| = |L : \mathbb{Q}| = 8$, so $|G| = p^3$ for $p = 2$ prime. It follows that there exists a chain of normal subgroups

$$1 \lhd G_1 \lhd G_2 \lhd G$$

such that $G/G_2 \cong G_2/G_1 \cong G_1/1 \cong C_2$, which uniquely determines the group as $G \cong C_2 \oplus C_2 \oplus C_2$, corresponding to the three commuting generators $\sigma_2, \sigma_3, \sigma_5 \in G$ of order 2, determined by $\sigma_2(\sqrt{2}) := -\sqrt{2}$, $\sigma_3(\sqrt{3}) := -\sqrt{3}$, $\sigma_5(\sqrt{5}) := -\sqrt{5}$. □

(b) (5 points) For each of the following subfields of L, give the subgroup of G corresponding to it under the Galois correspondence:

$$K_1 = \mathbb{Q}[\sqrt{10}], \quad K_2 = \mathbb{Q}[\sqrt{6}, \sqrt{15}], \quad K_3 = \mathbb{Q}[\sqrt{2} + \sqrt{3}], \quad K_4 = \mathbb{Q}[\sqrt{30}]$$

Proof. The Galois correspondence reverses inclusions, so the trivial subgroup corresponds with L itself, whereas $G \cong C_2 \oplus C_2 \oplus C_2$ corresponds with $\mathbb{Q}$. We now determine the nontrivial proper subgroups of G in order to determine the correspondences for the intermediate fields K_1, K_2, K_3, K_4:

- $G \cong C_2 \oplus C_2 \oplus C_2$ has exactly seven subgroups of order 2, each of which are isomorphic to C_2 (since there is only one group of order 2 up to isomorphism):

  $$\langle \sigma_2 \rangle, \ \langle \sigma_3 \rangle, \ \langle \sigma_5 \rangle, \ \langle \sigma_2\sigma_3 \rangle, \ \langle \sigma_2\sigma_5 \rangle, \ \langle \sigma_3\sigma_5 \rangle, \ \langle \sigma_2\sigma_3\sigma_5 \rangle.$$

  It follows that there are exactly seven fields $L \supseteq K \supseteq \mathbb{Q}$ with $|K : L| = |G : H| = 4$
- $G \cong C_2 \oplus C_2 \oplus C_2$ has exactly seven subgroups H of order 4:

  $$\langle \sigma_2, \sigma_5 \rangle, \ \langle \sigma_3, \sigma_5 \rangle, \ \langle \sigma_3, \sigma_5 \rangle, \ \langle \sigma_2, \sigma_3\sigma_5 \rangle, \ \langle \sigma_3, \sigma_2\sigma_5 \rangle, \ \langle \sigma_5, \sigma_2\sigma_3 \rangle, \ \langle \sigma_2\sigma_3, \sigma_2\sigma_5 \rangle.$$

  No subgroup is isomorphic to C_4 since this would imply that a single generator has degree 4, and we know the generators only have degree 2. Since the only other group of order 4 (up to isomorphism) is the Klein-4 group $V \cong C_2 \oplus C_2$, we conclude each of the above subgroups is isomorphic to V. It follows that there are exactly seven fields $L \supseteq K \supseteq \mathbb{Q}$ with $|L : K| = |G : H| = 2$.

By the Galois correspondence we know that each subgroup H of $\mathrm{Gal}(L/K)$ corresponds to the intermediate field L^H, the field fixed by its elements. We can immediately rule out the trivial group and G for the correspondences for each of K_1, K_2, K_3, K_4, since all have degree either 2 or 4 over $\mathbb{Q}$ (and not 1 or 8, which would be necessary for this by the Galois correspondence). By accounting for the images of the generators, we can now determine the K_i and corresponding subgroup for each $i = 1, 2, 3, 4$:

- $K_1 = \mathbb{Q}(\sqrt{10})$: $\sqrt{3} \notin K_1$, so σ_3 fixes K_1. Also, $\sigma_2\sigma_5(\sqrt{10}) = \sigma_2\sigma_5\sqrt{5}\sqrt{2} = (-\sqrt{2})(-\sqrt{5}) = \sqrt{10}$, so K_1 corresponds with $\langle \sigma_3, \sigma_2\sigma_5 \rangle \cong C_2 \oplus C_2$, the Klein-4 group.
- $K_2 = \mathbb{Q}(\sqrt{6}, \sqrt{15})$: First note $K_2 = \mathbb{Q}(\sqrt{6}, \sqrt{10})$; indeed, $\mathbb{Q}(\sqrt{6}, \sqrt{10}) \subseteq K_2$ because $(\sqrt{6}+\sqrt{15})^2 = 21+6\sqrt{10}$, and $K_2 \subseteq \mathbb{Q}(\sqrt{6}, \sqrt{10})$ since $(\sqrt{6}+\sqrt{10})^2 = 16+4\sqrt{15}$. Note that $\sqrt{6} = \sqrt{2}\sqrt{3}$, Then since $\sigma_2\sigma_3$ fixes $\sqrt{6}$ and σ_5 fixes $\sqrt{6}$, we have $\sigma_2\sigma_3\sigma_5$ fixes $\sqrt{6}$. Also, $\sqrt{10} = \sqrt{2}\sqrt{5}$ and $\sqrt{10}$, so $\sigma_2\sigma_5$ fixes $\sqrt{10}$ and σ_3 fixes $\sqrt{10}$, so (again using that G is abelian) it follows that $\sigma_2\sigma_3\sigma_5$ fixes $\sqrt{10}$. Hence K_2 is fixed by $\langle \sigma_2\sigma_3\sigma_5 \rangle$, so again by the Galois correspondence we have that K_2 corresponds with the subgroup $\langle \sigma_2\sigma_3\sigma_5 \rangle \cong C_2$.
- $K_3 = \mathbb{Q}(\sqrt{2}+\sqrt{3})$: Recall we have shown before that $K_3 = \mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Then no subgroups of G containing σ_2 or σ_3 fix K_3, so since $\sqrt{5} \notin K_3$ we conclude K_3 corresponds with $\langle \sigma_5 \rangle \cong C_2$.
- $K_4 = \mathbb{Q}(\sqrt{30})$: Since $\sqrt{30} = \sqrt{2}\sqrt{3}\sqrt{5}$, any combination of $\sigma_2\sigma_3$, $\sigma_2\sigma_5$, or $\sigma_3\sigma_5$ is the identity on $\sqrt{30}$ since it maps exactly two of its three factors $\sqrt{2}$, $\sqrt{3}$, or $\sqrt{5}$ to -1, which then cancel, preserving the original sign. Since $C_2 \oplus C_2 \oplus C_2$ is abelian, we can write $\sigma_3\sigma_5$ as $\sigma_3\sigma_5 = (\sigma_2\sigma_2)\sigma_3\sigma_5 = (\sigma_2\sigma_3)(\sigma_2\sigma_5)$, so the subgroup corresponding to K_4 is $\langle \sigma_2\sigma_3, \sigma_2\sigma_5 \rangle \cong C_2 \oplus C_2$, the Klein-4 group.

□

Exercise 3.44 (2)**.** Let K be a perfect field of characteristic $p > 0$ and let $a \in K$ be such that $f(x) = x^p - x - a$ is irreducible. Let $K \subseteq L$ be an extension of K such that there exists some $\lambda \in L$ with $f(\lambda) = 0$.

(a) (5 points) Prove that $\lambda + m$ is a root of $f(x)$ for all $m \in \mathbb{F}_p$.

Proof. K has prime characteristic (fields either have zero or prime characteristic), so we may invoke the "freshman's dream," that $(x + y)^p = x^p + y^p$ for all $x, y \in K$. Suppose m is in the prime field $\mathbb{F}_p$ (all fields contain their prime fields). Then $\lambda + m \in L$. If $m = 0$ then the assertion immediately follows since $f(\lambda + m) = f(\lambda + 0) = 0$, so we may assume $m \neq 0$. Then if λ is a root of f, we have

$$\begin{aligned} f(\lambda + m) &= (\lambda + m)^p - (\lambda + m) - a \\ &= \lambda^p + m^p - \lambda - m - a && \text{(freshman's dream)} \\ &= f(\lambda) + f(m) + a = f(m) + a, \end{aligned}$$

so it suffices to show $f(m) = -a$, that is, that $m^p - m = 0$. $m \neq 0$, so $m \in \mathbb{F}_p^\times$. But $\mathbb{F}_p^\times$ is a cyclic group of order $p - 1$, so $m^p = mm^{p-1} = m(1) = m$, as claimed. This completes the proof. □

(b) (3 points) Prove that $K(\lambda)$ is a splitting field for f, so $K \subseteq K(\lambda)$ is a Galois extension.

Proof. We know from part (a) that f has a root at $\lambda + m$ for the p-many $m \in \mathbb{F}_p$, so f splits completely over $K(\lambda)$ as $(x - \lambda)(x - (\lambda + 1)) \cdots (x - \lambda + (p - 1))$. It follows that $K(\lambda)$ is a splitting field for f. But f is a monic irreducible with λ as a root, so f is the minimal polynomial for λ over K by uniqueness. It follows that $|K(\lambda) : K| = \deg(f) = p$, so $K \subseteq K(\lambda)$ is a finite extension, so since K is given to be perfect we conclude by the splitting field characterization that $K \subseteq K(\lambda)$ is a Galois extension. □

(c) (2 points) Prove that $\mathrm{Gal}(K(\lambda)/K)$ is cyclic of order p.

Proof. Let $G_f := \mathrm{Gal}(K(\lambda)/K)$. $K \subseteq K(\lambda)$ is a (finite) Galois extension by part (b) and K is a perfect field, so by the degree characterization we have $|G_f| = |K(\lambda) : K| = |K(\lambda) : K| = \deg(f) = p$. p is prime and the unique group of order p up to isomorphism is C_p, so G_f is cyclic of order p. □

Exercise 3.45 (3)**.** Fix a field K of characteristic zero, and let $s_1, \dots, s_n$ be the elementary symmetric functions in $K[x_1, \dots, x_n]$. Let $K(x_1, \dots, x_n)$ be the field of rational functions in the x_i and let $K(s_1, \dots, s_n)$ be the field of rational functions in the s_i.

(a) (3 points) Show $K(x_1, \dots, x_n)$ is a Galois extension of $K(s_1, \dots, s_n)$ with Galois group S_n.

Proof. Let $F := K(s_1, \dots, s_n)$ and $L := K(x_1, \dots, x_n)$. We need to show $F \subseteq L$ is a Galois extension and $\mathrm{Gal}(L/F) \cong S_n$.

We first show that $F \subseteq L$ is a finite extension—indeed, recall that the elementary symmetric functions are the coefficients of the polynomial with roots $x_1, \dots, x_n$, namely the polynomial $x^n - s_1 x^{n-1} + s_2 x^{n-2} - \cdots \pm s_n$. We then have a finite chain of field extensions made by adjoining elements x_i, each algebraic over F:

$$F \subseteq F(x_1) \subseteq (F(x_1))(x_2) \subseteq \cdots \subseteq (F(x_1, \dots, x_{n-1}))(x_n) = L.$$

Then each extension is of finite degree, so it follows by the multiplicative property of the degree gives that $F \subseteq K$ is a finite extension.

Since $\mathrm{char}(K) = 0$ implies $\mathrm{char}(F) = 0$, we know F is perfect. It follows that in order to show $F \subseteq L$ is a Galois extension with Galois group S_n, it suffices to show $F = L^{S_n}$ by the fixed field characterization.

We claim F is the field fixed by all automorphisms of S_n, where S_n acts on L in the natural way by permuting the indices of the variables $x_1, \dots, x_n$. We first observe that each element of L takes the form fg^{-1} for some coprime $f, g \in K[x_1, \dots, x_n]$ with $g \neq 0$.

- ($L^{S_n} \subseteq F$): Let $\sigma \in S_n$ fix all of L, i.e. suppose $\sigma(fg^{-1}) = fg^{-1}$ for all of L. $1 \in L$, so setting $g = 1$ gives for arbitrary $f \in K[x_1, \dots, x_n]$ that that $\sigma(f) = f$. $f \in K[x_1, \dots, x_n]$ was arbitrary, so $f \in K[s_1, \dots, s_n]$ since by Gauss we know $K[x_1, \dots, x_n]^{S_n} = K[s_1, \dots, s_n]$. If we set $f = 1$ and let $g \in K[x_1, \dots, x_n]$, $g \neq 0$ be arbitrary, then we conclude by the same argument that $g \in K[s_1, \dots, s_n]$. It follows that $fg^{-1} \in K(s_1, \dots, s_n) = F$, as desired.
- ($F \subseteq L^{S_n}$): If $fg^{-1} \in K(s_1, \dots, s_n) = F$ then $g \neq 0$ and $f, g \in K[x_1, \dots, x_n]$, so σ fixes fg^{-1} since then $\sigma(fg^{-1}) = \sigma(f)\sigma(g^{-1}) = \sigma(f)(\sigma(g))^{-1} = fg^{-1}$.

It follows that $F = L^{S_n}$, concluding the proof per our prior remarks. □

(b) (3 points) Suppose that $n = 5$, and let $w = x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1$. Calculate the Galois group of the extension $K(x_1, \dots, x_5) \supseteq K(s_1, \dots, s_5, w)$.

Proof. Let $F := K(s_1, \dots, s_5)$ and $L := K(x_1, \dots, x_5)$, so that $K(s_1, \dots, s_5, w) = F(w)$ and $F(w) \subseteq L$ (the latter holds since $w \in L$). First note that $K, F, F(w), L$

are again perfect for the same reasons as in part (a). Recall that if $F \subseteq L$ is a Galois extension and $F \subseteq K \subseteq L$, then $K \subseteq L$ is a Galois extension. Since $F \subseteq L$ is a Galois extension by part (a), it follows that $F(w) \subseteq L$ is a Galois extension.

Set $G := \mathrm{Gal}(L/F)$. By part (a) we know $G \cong S_5$, so we will identify G with the action of its elements on the indices of the variables x_i. By the Galois correspondence, $F(w)$ corresponds to the subgroup of S_n fixing $F(w)$. Note that it suffices to determine the group of automorphisms fixing w, since we found in part (a) that the elements of F are invariant under any $\sigma \in S_5$. We claim $G \cong D_5$, the dihedral group of order 10.[4]

- The cycle (12345) and reflection (52)(43) fix w, so all 10 elements of $\langle(12345), (52)(43)\rangle$ fix w as well.
- These are the *only* ten; indeed, suppose $\sigma(x_1) = x_j$ for some $j = 1, \ldots, 5$. If w is to remain fixed under σ, then x_j must share exactly one term with x_{j+1} and exactly one term with x_{j-1} (where $j + 1$ is to be understood as $j \pmod 5 + 1$ to account for the indices cycling and starting at 1), giving two further choices. But this completely determines $\sigma(w)$, so we conclude that there are no more than ten possibilities for $\sigma(x_i)$.

It follows that $\mathrm{Gal}(L/F) = \langle\sigma, \tau\rangle$, where σ and τ act on the indices of the x_i as the permutations (12345) and (52)(43), respectively. Then $\sigma^5 = \tau^2 = 1$, and $\tau\sigma\tau = (15432) = s^{-1}$, which characterizes D_5, so $G \cong D_5 = \langle s, r : s^5 = r^2 = 1, rsr = s^{-1}\rangle$, the dihedral group of order 10. □

(c) (4 points) Let G be a finite group. Prove that there exists a Galois extension $F_1 \subseteq F_2$ of fields with Galois group G. [Hint: by Cayley's theorem, all finite groups can be embedded into S_n for some n.]

Proof. Let G be any finite group and $F := K(s_1, \ldots, s_n)$. G is a finite group, so by Cayley's theorem there exists an embedding $G \hookrightarrow S_n$ for some n. Let $F_1 := F(x_1, \ldots, x_n)^G$ and $F_2 := F(x_1, \ldots, x_n)$, so that F_1 is the subfield of F_2 fixed by G and hence $F_1 \subseteq F_2$ is a finite extension, where here we are identifying G with its embedding in S_n (which acts on the variables $x_1, \ldots, x_n$ as described in part (a) above). Then, since K is a field of characteristic zero and hence perfect, we conclude that G is the Galois group of the extension $F_1 \subseteq F_2$. Hence, for any finite group G, there exists a Galois extension $F_1 \subseteq F_2$ of fields with Galois group G. □

[4] One could also show this by noting that we can represent w as a labelled cyclic graph with five nodes labeled $1, \ldots, 5$. The task is then to determine what actions on the polygon preserves the structure of the graph, which we know is exactly the group D_5, the group of symmetries of a regular pentagon.

Lemma 3.46.

If L is a subfield of $\mathbb{C}$ and $\mathbb{Q} \subseteq L$ is a Galois extension, then L is closed under complex conjugation.

Proof. Let $z \in L$. If $\overline{z} \in \mathbb{Q}$ then $\overline{\overline{z}} = z \in \mathbb{Q}$, in which case the claim follows (since then both $z, \overline{z} \in L$, as claimed). Thus we may assume that both $z, \overline{z} \notin \mathbb{Q}$.

We first show z and $\overline{z}$ has the same minimal polynomial over $\mathbb{Q}$. Where $z = a + bi$, observe that $z - a = bi$, so $a^2 - 2az + z^2 = -b^2$. Thus if $z \notin L \setminus \mathbb{Q}$ then $g := x^2 - 2ax + a^2 + b^2 = 0$ is the minimal polynomial for f, by uniqueness of such a polynomial. By the quadratic formula g has roots $a \pm bi$, i.e. z and $\overline{z}$, so if $\overline{z} \notin L$ then $\overline{z}$ has minimal polynomial f as well.

$\mathbb{Q} \subseteq L$ is a Galois extension, so L is a splitting field over $\mathbb{Q}$ (there is no issue, since $\mathbb{Q}$ is perfect). Since z and $\overline{z}$ have the same minimal polynomial g over $\mathbb{Q}$. As the minimal polynomial for z, we know that g is a monic irreducible with a root z in L. Then, by the fundamental theorem of splitting fields, we conclude g splits completely over L, so $\overline{z} \in L$. $z \in L$ was arbitrary, so we conclude L is closed under complex conjugation. □

Exercise 3.47 (4)**.** Let L be a subfield of $\mathbb{C}$ such that $\mathbb{Q} \subseteq L$ is a Galois extension with Galois group $\mathbb{Z}/(5)$. Let α be any element of L that does not lie in $\mathbb{Q}$ and let $f(x) \in \mathbb{Q}[x]$ be the minimal polynomial of α.

(a) (5 points) Prove that α is a primitive element of $\mathbb{Q} \subseteq L$ and that $f(x)$ splits completely in L.

Proof. Let $\alpha \in L \setminus \mathbb{Q}$ have minimal polynomial $f \in \mathbb{Q}[x]$ over $\mathbb{Q}$.

We first show that α is a primitive element for $\mathbb{Q} \subseteq L$. We know $\alpha \notin \mathbb{Q}$, so $\mathbb{Q} \subsetneq \mathbb{Q}(\alpha)$. We are given that $\mathbb{Q} \subseteq L$ is a Galois extension, so $5 = |\operatorname{Gal}(L/\mathbb{Q})| = |L : \mathbb{Q}|$. But on a previous midterm we showed for extensions $K \subseteq L$ of prime degree that there are no fields F such that $K \subsetneq F \subsetneq L$, so since $\mathbb{Q} \subsetneq \mathbb{Q}(\alpha) \subseteq L$, we conclude $L = \mathbb{Q}(\alpha)$. Thus α is a primitive element of $\mathbb{Q} \subseteq L$.

We now show f splits completely over L. We're given $\mathbb{Q} \subseteq L$ is a Galois extension, so L is a splitting field for some polynomial over $\mathbb{Q}$ ($\mathbb{Q}$ is perfect so this goes through without issue). f is a minimal polynomial for $\alpha \in L$, so f is a monic irreducible with a root in L. Then, by the fundamental theorem of splitting fields, f splits completely over L. □

(b) (5 points) Prove that all the roots of $f(x)$ in L lie in $\mathbb{R}$.

Proof. $\mathbb{Q} \subseteq L$ is a Galois extension, so by the lemma we know L is closed under complex conjugation. In particular, where $\tau : \mathbb{C} \to \mathbb{C}$ is the complex conjugation map $z \mapsto \overline{z}$, the restriction $\tau|_L : L \to L$ is well-defined. Preservation of field operations under $\tau|_L$ is then inherited at once from τ. Thus $\tau|_L$ is a field automorphism of L relative to $\mathbb{Q}$, that is, $\tau|_L \in \mathrm{Gal}(L/\mathbb{Q})$.

Suppose for a contradiction $f(z) = 0$ for some $z \in \mathbb{C} \setminus \mathbb{R}$. Then $\tau|_L \neq \mathrm{id}_L$, so the orbit $\langle \tau|_L \rangle$ is a subgroup of $\mathrm{Gal}(L/\mathbb{Q})$ order 2 in $\mathrm{Gal}(L/\mathbb{Q})$ (since $\overline{\overline{z}} = z$). But $\mathrm{Gal}(L/\mathbb{Q}) \cong C_5$ is a cyclic group of prime order, which has no nontrivial proper subgroups, a contradiction. It follows that all roots of f (in L) lie in $\mathbb{R}$. □

Lemma 3.48.

$f := x^4 - x^2 - 1 \in \mathbb{Q}[x]$ is irreducible over $\mathbb{Q}$.

Proof. We show f is irreducible over $\mathbb{F}_3$. $f(0) = -1$, $f(1) = -1$, $f(2) = -1$, so f has no monic linear factors, and consequently no monic irreducible cubic factors. Thus f splits into two monic irreducible quadratic factors. But we know (cf. Artin p. 373) that the only monic irreducible polynomials of degree 2 over $\mathbb{F}_3$ are $a := x^2 + 1$, $b := x^2 + x - 1$, and $c := x^2 - x - 1$. But multiplying these over $\mathbb{F}_3$ gives $ab = -1 + x + x^3 + x^4, ac = -1 - x - x^3 + x^4, bc = 1 + x^4$, none of which are f. Thus f has no monic irreducible quadratic factors over $\mathbb{F}_3$. It follows that f is irreducible over $\mathbb{F}_3$, and hence over $\mathbb{Q}$, as claimed. □

Exercise 3.49 (5)**.** (5 points) Let K be the splitting field of $f(x) = x^4 - x^2 - 1$ over $\mathbb{Q}$. Prove that $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to the dihedral group of order 8. [Hint: figure out the roots of $f(x)$, and think about how the Galois group can permute them.]

Proof. Note $f = g(x^2)$ for $g = x^2 - x - 1 \in \mathbb{Q}[x]$, so by the quadratic formula g has roots $\alpha^2 = \frac{1}{2}(1 \pm \sqrt{5})$. Then, where $\varphi := \sqrt{\frac{1}{2}(1 + \sqrt{5})}$, it follows that f has roots $\pm\varphi$, $\pm i\varphi^{-1} \in K$.

We now show $K = \mathbb{Q}(\varphi, i)$. $\pm\varphi, \pm i\varphi^{-1} \in \mathbb{Q}(\varphi, i)$. We need to show that any field containing $\pm\varphi, \pm i\varphi^{-1}$ contains $\mathbb{Q}(\varphi, i)$. Indeed, $\mathbb{Q}(\varphi)$ is the smallest extension containing φ, but $i \notin \mathbb{Q}(\varphi)$ since $\mathbb{Q} \subseteq \mathbb{Q}(\varphi) \subseteq \mathbb{R}$ and $i \notin \mathbb{R}$. It follows that $\mathbb{Q}(\varphi, i)$ is contained in any extension with $\pm\varphi, \pm i\varphi^{-1}$ as elements, so we conclude that $K = \mathbb{Q}(\varphi, i)$ is the splitting field for f over $\mathbb{Q}$.

Set $G_f := \mathrm{Gal}(K/\mathbb{Q})$. We have $i \notin \mathbb{Q}(\varphi)$ since $\mathbb{Q} \subseteq \mathbb{Q}(\varphi)$ is a real extension, so $|K : \mathbb{Q}| = |K : \mathbb{Q}(\varphi)||\mathbb{Q}(\varphi) : \mathbb{Q}| = (2)(4) = 8$ by the multiplicative property of the degree. Then $\mathbb{Q} \subseteq K$ is a finite extension, so since K is a splitting field over $\mathbb{Q}$, a perfect field since $\mathrm{char}(\mathbb{Q}) = 0$, we conclude that the extension is Galois. Hence $|G_f| = |K : \mathbb{Q}| = 8$ by the degree characterization.

Each $\sigma \in G_f$ is determined by the image of the generators of the splitting field $\mathbb{Q}(\varphi, i)$ in which generators φ and i are linearly independent, so it follows that $\sigma \in G_f$ is determined by the images $\sigma(\varphi)$ and $\sigma(i)$. Recall that σ permutes the roots of irreducible polynomials over $\mathbb{Q}$. Then, since $\pm i$ are the roots of the irreducible polynomial $x^2 + 1$ over $\mathbb{Q}$ and as a field automorphism σ maps roots to roots, $\sigma(i) \in \{\pm i\}$. f itself is irreducible by the lemma, so $\sigma(\varphi)$ has all four roots as possible images, that is, $\sigma(\varphi) \in \{\pm\varphi, \pm i/\varphi\}$.

We now have identified 8 possibilities for σ. Since $|G_f| = 8$, so these must be all of them. In particular, there is a $\tau \in G_f$ such with $\tau(\varphi) = \varphi$ and $\tau(i) = -i$ and a $\sigma \in G_f$ such that $\sigma(\varphi) = i\varphi$ and $\sigma(i) = i$. We claim that $G_f = \langle \sigma, \tau : \sigma^4 = \tau^2 = \mathrm{id}, \tau\sigma\tau = \sigma^{-1} \rangle$, which characterizes the dihedral group of order 8. We can show this by listing the eight elements of G_f and checking that each relation is satisfied.

$\mathrm{id} : \varphi \mapsto \varphi,\, i \mapsto i$	$\tau : \varphi \mapsto \varphi,\, i \mapsto -i$
$\sigma : \varphi \mapsto i\varphi,\, i \mapsto i$	$\sigma\tau : \varphi \mapsto i\varphi,\, i \mapsto -i$
$\sigma^2 : \varphi \mapsto -\varphi,\, i \mapsto i$	$\sigma^2\tau : \varphi \mapsto -\varphi,\, i \mapsto -i$
$\sigma^3 : \varphi \mapsto -i\varphi,\, i \mapsto i$	$\sigma^3\tau : \varphi \mapsto -i\varphi,\, i \mapsto -i$

It now only remains to check that $\sigma^4 = \tau^2 = \mathrm{id}$ and $\tau\sigma\tau = \sigma^{-1}$:

- $\tau\sigma\tau = \tau(\sigma\tau)$ maps $\varphi \mapsto -\varphi \mapsto -\varphi$, $i \mapsto -i \mapsto i$, which is exactly the action of σ^3, so $\tau\sigma\tau = \sigma^3 = \sigma^{-1}$.
- $\sigma^4 = \sigma(\sigma^3)$ maps $\varphi \mapsto -i\varphi \mapsto -i^2\varphi = \varphi$, $i \mapsto i \mapsto i$, so $\sigma^4 = \mathrm{id}$.
- τ^2 maps $\varphi \mapsto \varphi \mapsto \varphi$, $i \mapsto -i \mapsto i$, so $\tau^2 = \mathrm{id}$.

Thus $G_f = \langle \sigma, \tau : \sigma^4 = \tau^2 = \mathrm{id}, \tau\sigma\tau = \sigma^{-1} \rangle$, so $G_f \cong D_4$, the dihedral group of order 8. □

Alphabetical Index