Solutions: Galois Theory by Tom Leinster

Hassaan Naeem

November 16, 2022

Chapter 1. Overview of Galois Theory

Exercise 1.1.3

Both proofs of 'if' contain little gaps: 'It follows by induction' in the first proof, and 'it's easy to see' in the second. Fill them.

Solution: We show both both parts (i) and (ii) seperately

(i) Follows from induction that for any polynomial p over $\mathbb{R}$, $\overline{p(w)} = p(\overline{w})$:

Let $p(w) = c_0 + c_1w^1 + c_2w^2 + ... + c_nw^n$ where $w^n \in \mathbb{C}$ and $c_n \in \mathbb{C}$.

$$\begin{aligned}
\overline{p(w)} &= \overline{c_0 + c_1w^1 + c_2w^2 + ... + c_nw^n} \\
&= \overline{c_0} + \overline{c_1w^1} + \overline{c_2w^2} + ... + \overline{c_nw^n} \\
&= c_0 + c_1\overline{w^1} + c_2\overline{w^2} + ... + c_n\overline{w^n} \\
&= p(\overline{w})
\end{aligned}$$

(ii) Checking that r is the zero polynomial:

Lemma. If $r(x) = a_0 + a_1x^1 + ... + a_nx^n$ and $r(x) = 0, \forall x \neq 0$, then $a_0 = 0$. Since $\mathbb{Q}$ is a field, and must contain a zero.

By this lemma we have that $\forall x$, $r(x) = 0$ and therefore $r(x) = 0 = x(a_1 + a_2x + ... + a_nx^{n-1}) = a_1 + a_2x + ... + a_nx^{n-1}$ and $\forall x \neq 0$ $a_1 = 0$. Hence, we repeat the Lemma and show that all $a_1, ..., a_n = 0$. Therefore $r(x)$ is the zero polynomial.

Exercise 1.1.6

Let $z \in \mathbb{Q}$. Show that z is not conjugate to z' for any complex number $z' \neq z$.

Solution:

Exercise 1.1.10

Suppose that $(z_1, ..., z_k)$ and $(z'_1, ..., z'_k)$ are conjugate. Show that z_i and z'_i are conjugate, for each $i \in \{1, ..., k\}$

Solution: By **Definition 1.1.9** have that:

$$p(z_1, ..., z_k) = 0 \Longleftrightarrow p(z'_1, ..., z'_k) = 0$$

When $k = 1$ we have that:

$$p(z_1) = 0 \Longleftrightarrow p(z'_1) = 0 \implies z_1 \text{ and } z'_1 \text{ are conjugate}$$

Similarly, for any k:

$$p(z_i) = 0 \Longleftrightarrow p(z'_i) = 0 \implies z_i \text{ and } z'_i \text{ are conjugate}$$

Exercise 1.2.2

Show that $Gal(f)$ is a subgroup of S_k.

Chapter 2. Group actions, rings and fields

Exercise 2.1.3

Check that $\bar{g}$ is a bijection for each $g \in G$. Also check that Σ is a homomorphism.

Solution: We show injectivity (i), surjectivity (ii) and homomorphism (iii) :

(i) Injectivity:

Let $x, y \in X$ and $\bar{g}$ be our bijection
If we have $\bar{g}(x) = \bar{g}(y)$

$\rightsquigarrow gx = gy \rightsquigarrow g^{-1}(gx) = g^{-1}(gy) \rightsquigarrow (g^{-1}g)x = (g^{-1}g)y \rightsquigarrow ex = ey \rightsquigarrow x = y \quad \square$

(ii) Surjectivity:

We know that $f : X \to Y$ is surjective iff $\forall y \in Y \ \exists x \in X : f(x) = y$
We let $x \in X$ and e be the identity in G then,
$x = ex = (gg^{-1})x = g(g^{-1}x) = gy = \bar{g}(y)$ where $y = g^{-1}x \in X \quad \square$

Therefore $\bar{g}$ is both injective and surjective, hence bijective.

(i) Σ is Homomorphism:

We have the map:

$$\Sigma : G \to Sym(X)$$
$$g \mapsto \bar{g}$$

We know that $\bar{g}$ is well defined
Then we take $g, h \in G, x \in X$, then by **Definition 2.1.1**.

$$\begin{aligned}\Sigma(gh)(x) &= gh(x) = g(hx) \\ &= \Sigma(g)(\Sigma(h)(x)) = \Sigma(g) \circ \Sigma(h)\ (x) \quad \square\end{aligned}$$

Exercise 2.1.10

Example **2.1.9(iii)** shows that the action of the isometry cube G of the cube on the set X of long diagonals is not faithful. By **Lemma 2.1.8**, there must be some non-identity isometry of the cube that fixes all four long diagonals. In fact, there is exactly one. What is it?

Solution: We show both both parts (i) and (ii) seperately

Exercise 2.2.6

Prove that the only subring of a ring R that is also an ideal is R itself.

Solution: We know that I is an ideal of R if:

$$\begin{aligned}&(I, +) \leq (R, +) \quad \text{[I is additive subgroup of R]} \\ &\& \ \forall r \in R, x \in I : \\ &(1)\ r \cdot x \in I \\ &(2)\ x \cdot r \in I\end{aligned}$$

We know that a subring S of R is a subset $S \subseteq R$ containing 0 and 1.

Therefore if we take S to be an ideal aswell then:

$$\begin{aligned}&(S, +) \leq (R, +) \\ &\& \ \forall r \in R, s \in S : \\ &(1)\ r \cdot s \in S \\ &(2)\ s \cdot r \in S\end{aligned}$$

But we know that $1 \in S$. Therefore, $\forall r \in R$, (1) $1 \cdot r = r \in S$ and (2) $r \cdot 1 = r \in S$
Therefore $\forall r \in R, r \in S \implies S = R \quad \square$

Exercise 2.2.8

The trivial ring or zero ring is the one-element set with its only possible ring structure. Show that the only ring in which $0 = 1$ is the trivial ring.

Solution: Let $(R, +, \cdot)$ be our commutative, unital ring.
If $1 = 0$ in R, then $\forall r \in R$ we have $r = 1r = 0r = 0 \quad \square$

Exercise 2.2.8

Fill in the details of Example 2.2.13.

Solution: We suppose that $I \subseteq \mathbb{Z}$ is an ideal and we take $n \in I$ to be the least positive integer in I. We have obviously that $\langle n \rangle \subseteq I$. Then we assume that that $m \in I$, by the division algorithm we know that:

$$\begin{aligned} m &= qn + r && (0 \leq r < n) \\ r &= m - qn && \in I \end{aligned}$$

Therefore $r = 0 \rightsquigarrow m = qn$. Therefore $m \in \langle n \rangle$ and we have that $I \subseteq \langle n \rangle$. Hence we have equality, $I = \langle n \rangle \quad \square$

Exercise 2.2.15

Let r and s be elements of an integral domain.
Show that $r|s|r \iff \langle r \rangle = \langle s \rangle \iff s = ur$ for some unit u.

Solution: If we have that $r|s|r$ then $\exists\ a \in R : s = ar$ and $\exists\ b \in R : r = bs$ then:

$$\begin{aligned} &\frac{s}{a} = bs \\ &b = \frac{1}{a} \rightsquigarrow ab = 1 \rightsquigarrow b = a^{-1} \end{aligned}$$

Then we have that $s = ar$, and we have just shown that a is a unit, hence $s = ur$. Therefore $r|s|r \implies s = ur$

If we have $\langle r \rangle = \langle s \rangle$, then $r = s$. Hence,

$$\begin{aligned} &r = 1s \quad \& \quad s = 1r \\ &r = as \quad \& \quad s = ar \quad (\text{where } a = 1) \\ &\implies s|r \ \& \quad r|s \end{aligned}$$

Therefore $\langle r \rangle = \langle s \rangle \implies r|s|r$

If we have that $s = ur$ for some unit u, then also we have that

$$\begin{aligned}
&u^{-1}s = u^{-1}ur \rightsquigarrow r = u^{-1}s \\
&\text{Therefore } s \in \langle r \rangle \;\&\; r \in \langle s \rangle, \langle s \rangle \subseteq \langle r \rangle \;\&\; \langle r \rangle \subseteq \langle s \rangle \\
&\implies \langle r \rangle = \langle s \rangle
\end{aligned}$$

Therefore $s = ur \implies \langle r \rangle = \langle s \rangle$

Exercise 2.3.1

Write down all the examples of fields that you know.

Solution: $\mathbb{C}, \mathbb{R}, \mathbb{Q}$

Exercise 2.3.5

Let $\phi : K \to L$ be a homomorphism of fields and let $0 \neq a \in K$. Prove that $\phi(a^{-1}) = \phi(a)^{-1}$. Why is $\phi(a)^{-1}$ defined?

Solution: Since K is a field, and the fact that $0 \neq a \in K$, we have that a is a unit, $aa^{-1} = 1$, and $a^{-1} \in K$. By **Lemma 2.3.3**, we have that $\phi : K \to L$ is injective. Hence, $\phi(a)\phi(a^{-1}) = \phi(a \circ a^{-1}) = \phi(1) = 1$, and $\phi(a^{-1})\phi(a) = \phi(a^{-1} \circ a) = \phi(1) = 1$. Therefore we have that $\phi(a^{-1})$ is both a left and right inverse of a and hence it is the only inverse of a. Therefore, by injectivity $\phi(a^{-1}) = \phi(a)^{-1}$.

Exercise 2.3.13

This proof of Lemma 2.3.12 is quite abstract. Find a more concrete proof, taking equation (2.2) as your definition of characteristic. (You will still need the fact that ϕ is injective.)

Solution: By (2.2) we have:

$$char R = \begin{cases} \text{least } n > 0 : n * 1_R = 0_R & \text{, if such an n exists} \\ 0 & \text{, otherwise} \end{cases}$$

We know that $\phi(1_K) = 1_L$ and $\phi(0_K) = 0_L$, since ϕ is injective, then also $\phi(n \cdot 1_K) = n \cdot 1_L$ $\forall n \in \mathbb{N}$. We have two possible cases for the characteristic c of K ($char K$), $c = 0$ or $c > 0$.

If $c = 0$, then $\phi(0_K) = 0_L = 0$. Therefore $char L = c = char K$.
If $c > 0$, then $\phi(c \cdot 1_K) = c \cdot 1_L = 0$. Therefore $char L = c = char K$.

Exercise 2.3.15

What is the prime subfield of $\mathbb{R}$? Of $\mathbb{C}$?

Solution: For $\mathbb{R}$ it is $\mathbb{Q}$. For $\mathbb{C}$ it is also $\mathbb{Q}$. See **Lemma 2.3.16**.

Exercise 2.3.25

What are the irreducible elements of a field?

Solution: We know thar for a ring R, r is irreducible if r is not 0 or a unit and if for $a, b \in R$, then $r = ab \implies a$ or b is a unit. However, we know that every element of a field K is a either a unit or 0. Therefore, there are no irreducible elements in a field.

Chapter 3. Polynomials

Exercise 3.1.4

Show that whenever R is a finite nontrivial ring, it is possible to find distinct polynomials over R that induce the same function $R \to R$. (Hint: are there finitely or infinitely many polynomials over R? Functions $R \to R$?)l

Solution:

Exercise 3.1.8

What happens to everything in the previous paragraph if we substitute $t = u^2+c$ instead?

Solution:

Exercise 3.1.13

Let p be a prime and consider the field $\mathbb{F}_p(t)$ of rational expressions over $\mathbb{F}_p$. Show that t has no pth root in $\mathbb{F}_p(t)$. (Hint: consider degrees of polynomials.)

Solution: A rational expression over K is $\frac{f(t)}{g(t)}$ where $f(t), g(t) \in K[t]$ with $g \neq 0$. For any $\frac{f(t)}{g(t)} \in \mathbb{F}_p(t)$ where $f(t), g(t) \in \mathbb{F}_p[t]$, suppose we have have that $\left(\frac{f(t)}{g(t)}\right)^p = t$. We then have that $f^p = tg^p$. Then $deg(f^p) = np$ where $n = deg(f)$ and $deg(tg^p) = deg(t) + deg(g^p) = 1 + mp$ where $m = deg(g)$, hence we have $np = mp + 1 \rightsquigarrow p = \frac{1}{n-m}$. But this is impossible since p is prime, hence a contradiction, hence t has no pth root in $\mathbb{F}_p(t)$.

Exercise 3.2.4

Prove that the ideals in Warning 3.2.3 are indeed not principal.

Solution:

Exercise 3.3.5

If I gave you a quadratic over $\mathbb{Q}$, how would you decide whether it was reducible or irreducible?

Solution: By **Lemma 3.3.1 (ii)**, if the quadratic has a root in $\mathbb{Q}$, then it is reducible. By the same lemma **(iii)**, if the quadratic has no root in $\mathbb{Q}$, then it is irreducible.

Exercise 3.3.13

The last step in (3.9) was $'deg(\bar{h}) \leq deg(h)'$. Why is that true? And when does equality hold?

Solution: $\bar{h} = hmodp$. Therefore if $p|a_{n_h}$ then $a_{n_{\bar{h}}} = 0$ and $deg(\bar{h}) < deg(h)$. If $p \nmid a_{n_h}$ then $a_{n_h} = a_{n_{\bar{h}}}$ and $deg(\bar{h}) = deg(h)$. Therefore $deg(\bar{h}) \leq deg(h)$. Equality holds on the preceding condition.

Exercise 3.3.15

Use Eisenstein's criterion to show that for every $n \geq 1$, there is an irreducible polynomial over $\mathbb{Q}$ of degree n.

Solution: Let $f(t) = a_0 + ... + a_n t^n \in \mathbb{Q}[t]$ with $n \geq 1$. For $n \geq 1$, we can always choose an $f \in \mathbb{Q}[t]$ such that $f(t) = a_n t^n + a_0$, and we can further always choose an a_n, a_0 and p such that $p \nmid a_n,\ p|a_0,\ p^2 \nmid a_0$. Hence, we have $f(t) = a_n t^n + a_0$ fulfilling the Eisenstein criterion, and hence $f(t)$ is irreducible over $\mathbb{Q}$. As an example, we can always choose $f(t) = t^n + 2$ and $p = 2$.

Chapter 4. Field extensions

Exercise 4.1.3

Find two examples of fields K such that $Q \subsetneqq K \subsetneqq \mathbb{Q}(\sqrt{2}, i)$

Solution: $K = \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ and
$K = \mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$

Exercise 4.1.5

Check the truth of all the statements in the previous paragraph.

Solution: Follow trivially from definitions of interesection and subfields. See **Lemma 2.2.3** for showing interesection of subfields still remains a subfield.

Exercise 4.1.7

What is the subfield of $\mathbb{C}$ generated by $\{7/8\}$? By $\{2+3i\}$? By $\mathbb{R} \cup \{i\}$?

Solution: Since $\mathbb{C}$ is of characteristic 0, by **Lemma 2.3.16** the prime subfield of $\mathbb{C}$ is $\mathbb{Q}$. Since $\mathbb{Q}$ contains $\{7/8\}$ and by definition of prime subfield, it is the intersection of all the subfields of $\mathbb{C}$ containing $\{7/8\}$, hence $\mathbb{Q}$ is generated by $\{7/8\}$.

Let L be the subfield of $\mathbb{C}$ generated by $\{2+3i\}$. Then $L = \{2a+3bi : a, b \in \mathbb{Q}\}$ by similar argument as **Example 4.1.6 (ii)**.

Similarly, let L be the subfield of $\mathbb{C}$ generated by $\mathbb{R} \cup \{i\}$. Then
$L = \mathbb{R} \cup \{a+bi : a, b \in \mathbb{Q}\} \stackrel{?}{=} \{a+bi : a \in \mathbb{R}, b \in \mathbb{Q}\}$.

Exercise 4.1.11

Let $M : K$ be a field extension. Show that $K(Y \cup Z) = (K(Y))(Z)$ whenever $Y, Z \subseteq M$.

Solution:

Exercise 4.2.2

Show that every element of K is algebraic over K.

Solution: Since K is a field, $\forall k \in K : \exists -k \in K : k + (-k) = (-k) + k = 0$. Therefore, $\forall k \in K$, we can choose $f(t) = t - k \in K[t]$. Hence we have that $f \neq 0$ and $f(k) = k - k = 0$. Therefore $\forall k \in K, k$ is algebraic over K.

Exercise 4.2.9

What is the minimal polynomial of an element of K?

Solution: We can refer back to **Exercise 4.2.2**. If we let $m(t) = t - k$, then we see that it is indeed monic and unique $\forall k \in K$ satisfying condition (4.2).

Exercise 4.3.5

Let $M : K$ and $L : K$ be field extensions, and let $\phi : M \to L$ be a homomorphism over K. Show that if $\alpha \in M$ has minimal polynomial m over K then $\phi(\alpha) \in L$ also has minimal polynomial m over K.

Solution:

Exercise 4.3.9

Fill in the details of the last paragraph of that proof.

Solution: We show that there is at most one homomorphism $\phi : K(t) \to L$ over K such that $\phi(t) = \beta$. We let ϕ and ϕ' be two such homomorphisms. Then we have that $\phi(t) = \beta = \phi'(t)$. By **Lemma 4.3.1 (ii)** we have that t generates $K(t)$ over K, and hence by **Lemma 4.3.6** $\phi = \phi'$ $\square$

Exercise 4.3.15

Prove that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

Solution: We know that $\sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ and hence $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Now we show the inclusion the other way. We use the hint and get that $(\sqrt{2} + \sqrt{3})^3 = 11\sqrt{2} + 9\sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Then we have that:
$11\sqrt{2}+9\sqrt{3}-9(\sqrt{2}+\sqrt{3}) = 2\sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$, hence $\sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$. Similarly, we get that $\sqrt{3} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$. Therefore, $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}+\sqrt{3})$ $\square$

Exercise 4.3.18

How many elements does the field $\mathbb{F}_3(\sqrt{2})$ have? What about $\mathbb{F}_2(\alpha)$, where α is a root of $1 + t + t^2$?

Solution: We know that $\mathbb{F}_3(\sqrt{2})$ can be constructed as $\mathbb{F}_3[t]/\langle t^2 - 2\rangle$. Hence, any element of the field has the form $a_0 + a_1 t + \langle t^2 - 2\rangle$ with $a_i \in \mathbb{F}_3$. Hence, there are $3^2 = 9$ elements.

In a similar manner, we know that $\mathbb{F}_2(\alpha)$ can be constructed as $\mathbb{F}_2[t]/\langle t^2+t+1\rangle$. Hence any element of the field has the form $a_0 + a_1 t + \langle t^2 + t + 1\rangle$ with $a_i \in \mathbb{F}_2$. Hence there are $2^2 = 4$ elements.

Chapter 5. Degree

Exercise 5.1.9

Write out the addition and multiplication tables of $\mathbb{F}_2(\alpha)$.

Solution: The tables are straightforward, using modulo arithmetic and the irreducible polynomial evaluated at α.

$+$	0	1	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

$\times$	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

Exercise 5.1.13

Give an example of to show that the inequalityin Corollary 5.1.12 can be strict. Your example can be as trivial as you like.

Solution: We choose our fields and hence extensions to be $\mathbb{C} : \mathbb{R} : \mathbb{Q}$. We also choose $\beta = \sqrt{2} \in \mathbb{C}$. The minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $m = t^2 - 2$, then $\deg_{\mathbb{Q}}(\beta) = [\mathbb{Q}(\beta) : \mathbb{Q}] = 2$.

Similarly, the minimal polynomial of $\sqrt{2}$ over $\mathbb{R}$ is $m = t - \sqrt{2}$, then $\deg_{\mathbb{R}}(\beta) = [\mathbb{R}(\beta) : \mathbb{R}] = 1$.

Hence we have that $[\mathbb{R}(\beta) : \mathbb{R}] < [\mathbb{Q}(\beta) : \mathbb{Q}]$ $\square$

Exercise 5.1.16

Let $M : K$ be a field extension and α a transcendental element of M. Can every element of $K(\alpha)$ be represented as a polynomial in α over K?

Solution: We have that $K(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} : f, g \in F[t] \right\}$, which is just $K(t)$, the field rational expressions. Therefore it is not polynomial is α over K.

Exercise 5.1.20

Show that a field extension whose degree is a prime number must be simple.

Solution: Let $M : K(\alpha) : K$ be field extensions where M and K are arbitrary fields, $\alpha \in M$, and $[M : K] = p$, where p is prime. By **Theorem 5.1.17 (iii)** we have $[M : K] = [M : K(\alpha)][K(\alpha) : K]$. Hence, we must have that $[K(\alpha) : K] = 1$ or p, however, we also know that $K(\alpha) \neq K$, hence $[K(\alpha) : K] = p$, and therefore, $[M : K(\alpha)] = 1$, which by **Example 5.1.3** tells us $M = K(\alpha)$. Hence $M : K$ is a simple.

Exercise 5.1.23

Generalize Example 5.1.22. In other words, what general result does the argument of Example 5.1.22 prove, not involving the particular numbers chosen there?

Solution: Let $M : K$ be a field extension and $\alpha_1, ..., \alpha_n \in M$. If $gcd(deg_K(\alpha_1)$ $, ..., deg_K(\alpha_n)) = 1$ (i.e., coprime), then we have that, $[K(\alpha_1, ..., \alpha_n) : K] = [K(\alpha_1) : K]...[K(\alpha_n) : K]$

Exercise 5.2.5

Let $M : K$ be a field extension and $K \subseteq L \subseteq M$. In the proof of Proposition 5.2.4, I said that if L is a subfield of M then L is a K-linear subspace of M. Why is that true? And is the converse also true? Give proof or a counterexample.

Solution: We know that M acts as a vector space over K. If L is a subfield of M, then we can similarly conclude that L acts as a vector space over K. Since we have that L is a subset of M (a subfield) we can conclude that L is a linear (K-linear) subspace of M (by definition of a linear subspace).

The converse is not true.

Exercise 5.2.8

Let $M : K$ be a field extension and write L for the set of elements of M algebraic over K. By imitating the proof of Proposition 5.2.7, prove that L is a subfield of M.

Solution: We have that $L = \{\alpha \in M : [K(\alpha) : K] < \infty\}$.
Then $\forall \alpha, \beta \in L,\ [K(\alpha, \beta) : K] \leq [K(\alpha) : K][K(\beta) : K] < \infty$
Now $\alpha + \beta \in K(\alpha, \beta)$, so $K(\alpha + \beta) \subseteq K(\alpha, \beta)$, hence
$[K(\alpha + \beta) : K] \leq [K(\alpha, \beta) : K] < \infty$, giving $\alpha + \beta \in L$. Similarly, $\alpha \cdot \beta \in L$.
Then $\forall \alpha \in L,\ [K(-\alpha) : K] = [K(\alpha) : K] < \infty$, giving $-\alpha \in L$. Similarly, $1/\alpha \in L$ (if $\alpha \neq 0$), and clearly $0, 1 \in L$ $\quad \square$

Exercise 5.3.7

Find an example of Lemma 5.3.6 where $[LL' : L] = 2$, and another where $[LL' : L] = 1$.

Solution: If we let $L = \mathbb{Q}(\sqrt{2})$ and $L' = \mathbb{Q}(\sqrt{3})$, we then get $LL' = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Then $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{3})] = 2$.

If we let $L = \mathbb{Q}(\sqrt{4})$ and $L' = \mathbb{Q}(\sqrt{3})$, we then get $LL' = \mathbb{Q}(\sqrt{4}, \sqrt{3})$. Then $[\mathbb{Q}(\sqrt{4}, \sqrt{3}) : \mathbb{Q}(\sqrt{3})] = 1$.

Chapter 6. Splitting fields

Exercise 6.1.5

Show that if a ring homomorphism ψ is injective then so is ψ_*, and if ψ is an isomorphism then so is ψ_*.

Solution: We have that $\psi : R \to S$ and $\psi_* : R[t] \to S[t]$. Since ψ is injective we that $\forall x, y \in R$ if $\psi(x) = \psi(y) \implies x = y$. Then we choose $f, f' \in R[t]$ and assume that $\psi_* f = \psi_* f'$. From **Definition 3.1.7** we then have that:

$$\begin{aligned}
\psi_* f &= \psi_* f' \\
\psi_* \left(\sum_i a_i t^i \right) &= \psi_* \left(\sum_i b_i t^i \right) \\
\sum_i \psi(a_i) t^i &= \sum_i \psi(b_i) t^i \\
\psi(a_i) &= \psi(b_i) \\
\implies a_i &= b_i
\end{aligned}$$

Hence we have that $f = \sum_i a_i t^i = f'$. Hence ψ_* is injective.

If ψ is an isomorphism then ψ is both surjective and injective. We have just shown that ψ_* is injective, so we show that it is also surjective to prove it is an isomorphism. We know that ϕ_* is surjective $\iff \forall s \in S[t]\ \exists r \in R[t] : \psi_* r = s$.

We choose $s \in S[t]$ and let e be the identity homomorphism. Then we have:

$$\begin{aligned} s &= es \\ &= (\psi_* \psi_*^{-1})s \\ &= \psi_*(\psi_*^{-1} s) \\ &= \psi_* \left(\psi_*^{-1} \left(\sum_i a_i t^i \right) \right) \\ &= \psi_* \left(\sum_i \psi^{-1}(a_i) t^i \right) \\ &= \psi_* r \end{aligned}$$

where $\psi^{-1}(a_i) \in R$ exists since ψ is an isomorphism, and $r = \sum_i \psi^{-1}(a_i)t^i \in R[t]$. Hence ψ_* is also surjective, hence it is an isomorphism.

Exercise 6.2.7

Show that (ii) can equivalently be replaced by: 'if L is a subfield of M containing K, and f splits in L, then $L = M$'.

Solution: We first show ($\implies$). We have that $M = K(\alpha_1, ..., \alpha_n)$ and so $M : K$ is well defined. We then take a basis $\alpha_1, ..., \alpha_n$ of M over K. Then we have that every subfield L of M containing K is a K-linear subspace of M. So if $\alpha_1, ..., \alpha_n \in L$, which would mean that f splits in L, then $L = M$.

We then show ($\Longleftarrow$). We have that $K \subseteq L = M$, and $f(t) = \beta(t-\alpha_1) \cdots (t-\alpha_n)$ for some $n \geq 0$ and $\beta, \alpha_1, ..., \alpha_n \in L = M$. Then the result follows trivially from **Proposition 5.2.4**.

Exercise 6.2.9

In Example 6.2.8(iii), I said that $\mathbb{Q}(\xi, \omega\xi, \omega^2\xi) = \mathbb{Q}(\xi, \omega)$. Why is that true?

Solution: $\omega = e^{2\pi i/3} = \frac{-1+i\sqrt{3}}{2}$, and hence $\omega^2 = \frac{-1-i\sqrt{3}}{2}$. and hence we see that ω^2 is a rational multiple of ω, hence $\mathbb{Q}(\xi, \omega\xi, \omega^2\xi) = \mathbb{Q}(\xi, \omega)$.

As an aside, we know that $\mathbb{Q}(\xi) = \left\{a + b\xi + c\xi^2 : a, b, c \in \mathbb{Q}\right\}$, and hence $\{1, \xi, \xi^2\}$ forms a basis for $\mathbb{Q}(\xi) : \mathbb{Q}$. Similarly, $\{1, \omega\}$ forms a basis for $\mathbb{Q}(\xi, \omega) : \mathbb{Q}(\xi)$. By **Theorem 5.1.17 (Tower Law)(i)** we then have that $\{1, \xi, \xi^2, \omega, \xi\omega, \xi^2\omega\}$ forms a basis for $\mathbb{Q}(\xi, \omega) : \mathbb{Q}$.

Exercise 6.2.12

Why does the proof of **Proposition 6.2.11** not show that there are *exactly* $[M : K]$ isomorphisms ϕ extending ψ? How could you strengthen the hypothesis in order to obtain that conclusion?

Solution: It can be strengthened by ...

Exercise 6.3.2

Check that this really does define a group.

Solution: Firstly we have that $Gal(M : K) = Aut(M : K)$. By definition we have $Aut(M : K) = \{f : M : K \to M : K \mid f \text{ is an isomorphism of } M : K\}$ and $\circ : M : K \times M : K \to M : K$. We show that the pair $(Aut(M : K), \circ)$ is a group.

Firstly, for $f, g \in Aut(M : K)$ and $\forall a, b \in M : K$, we have that:

$$\begin{aligned}(g \circ f)(ab) &= g(f(ab)) \\ &= g(f(a)f(b)) \\ &= g(f(a))g(f(b)) \\ &= (g \circ f)(a)(g \circ f)(b)\end{aligned}$$

Since f, g are bijective by defintion, $g \circ f$ is bijective, and by above is a homomorphism, hence it is an automporhism.

We now show associativity. $\forall f, g, h \in Aut(M : K)$ and $a \in M : K$ we have:

$$\begin{aligned}((h \circ g) \circ f)(a) &= h(g(f(a))) \\ &= h(g \circ f(a)) \\ &= h \circ (g \circ f(a)) \\ &= (h \circ (g \circ f))(a) \quad \Box\end{aligned}$$

Next, we check for an identity. $\forall f \in Aut(M : K)$ and $e_{M:K} : (M : K) \to (M : K)\ : a \mapsto a$ we have, $f \circ e_{M:K} = e_{M:K} \circ f = f$. Hence $e_{M:K}$ is the identity element.

Finally, we check for the inverse. $\forall f \in Aut(M : K)$, we have that $f \circ f^{-1} = e_{M:K} = f^{-1} \circ f$. This follows by definition since f is an isomorphism.

Exercise 6.3.4

Prove that $Gal(\mathbb{Q}(e^{2\pi i/3}) : \mathbb{Q}) = \{id, \kappa\}$, where $\kappa(z) = \bar{z}$.

Solution: We know that the identity is an automorphism of $\mathbb{Q}(e^{2\pi i/3})$ over $\mathbb{Q}$. By **Lemma 1.1.2**, since $\mathbb{Q} \subset \mathbb{R}$ we have that κ is also an automorphism of $\mathbb{Q}(e^{2\pi i/3})$ over $\mathbb{Q}$.

Hence we have that $\{id, \kappa\} \subseteq Gal(\mathbb{Q}(e^{2\pi i/3}) : \mathbb{Q})$. We also know that $\mathbb{Q}(e^{2\pi i/3}) : \mathbb{Q} = \mathbb{Q}(\frac{-1+i\sqrt{3}}{2}) : \mathbb{Q} = \mathbb{Q}(i\sqrt{3}) : \mathbb{Q}$

We let $\theta \in Gal(\mathbb{Q}(e^{2\pi i/3}) : \mathbb{Q})$. Since θ is a homomorphism we have that:

$$\begin{aligned}(\theta(i\sqrt{3}))^2 &= \theta((i\sqrt{3})^2) \\ &= \theta(-3) \\ &= -\theta(3) \\ &= -3\end{aligned}$$

Hence $\theta(i\sqrt{3}) = \pm i\sqrt{3}$. If $\theta(i\sqrt{3}) = i\sqrt{3}$ then $\theta = id$, and if $\theta(i\sqrt{3}) = -i\sqrt{3}$ then $\theta = \kappa$. Hence $Gal(\mathbb{Q}(e^{2\pi i/3}) : \mathbb{Q}) = \{id, \kappa\}$.

Exercise 6.3.11

I skipped two small bits in that proof: 'θ is surjective because σ is a permutation' (why?), and 'You can check that θ is a homomorphism of fields'. Fill in the gaps.

Solution: This follows by definition of permutation. A permutation is a bijective map from a set to itself, hence it is surjective. θ is a homomorphism of fields.

Secondly, by **Definition 6.3.5** $Gal_K(f)$ is $Gal(SF_K(f) : K)$. Then by **Definition 6.3.1** we know that an element of $Gal(M : K)$ is an isomorphism $\theta : M \to M$, hence by defintion we have that $\theta \in Gal_K(f)$ is a homomorphism of fields.

Chapter 7. Preparation for the fundamental theorem

Exercise 7.1.4

What happens if you drop the word 'irreducible' from Lemma 7.1.2? Is it still true?

Solution:

Exercise 7.1.4

What happens if you drop the word 'irreducible' from Lemma 7.1.2? Is it still true?

Solution:

Exercise 7.2.1

Try to find an example of an irreducible polynomial of degree d with fewer than d distinct roots in its splitting field.

Solution: An irreducible polynomial over a field of characteristic 0 has distinct roots in its splitting field. Therefore we must consider field of characteristic $p > 0$, where p is prime. Hence if we have the field extension $\mathbb{F}_p(t) : \mathbb{F}_p(t^p)$, and we consdier $t \in \mathbb{F}_p(t)$ its minimal polynomial over $\mathbb{F}_p(t^p)$ is $X^p - t^p = (X - t)^p$. We get to the last step from the Frobenius automorphism.

Exercise 7.2.8

Check one or two of the properties in Lemma 7.2.7.

Solution: We check the additive property.

We let $f(t) = \sum_{i=0}^n a_i t^i \in K[t]$ and $g(t) = \sum_{i=0}^n b_i t^i \in K[t]$. Then we have that $f(t) + g(t) = \sum_{i=0}^n (a_i + b_i)t^i = \sum_{i=0}^n c_i t^i \in K[t]$, where $c_i = (a_i + b_i)$. Then by **Definition 7.2.6** we have that $D(f + g)(t) = \sum_{i=1}^n ic_i t^{i-1} = \sum_{i=1}^n i(a_i + b_i)t^{i-1} = \sum_{i=1}^n ia_i t^{i-1} + \sum_{i=1}^n ib_i t^{i-1} = Df + Dg \in K[t]$

Exercise 7.2.15

Let $M : L : K$ be field extensions. Show that if $M : K$ is algebraic then so are $M : L$ and $L : K$.

Solution: By definition of an algebraic extension, we have that if $M : K$ is algebraic then $\forall \alpha \in M\ \exists f \neq 0 \in K[t] : f(\alpha) = 0$. Since we have that M is a field extension of L it must contain all of L, therefore we have that $\forall \alpha \in L\ \exists f \neq 0 \in K[t] : f(\alpha) = 0$, hence $L : K$ is algebraic. Similarly, since L extends K any $f \neq 0 \in K[t]$ must exist in $L[t]$, hence we that $\forall \alpha \in M\ \exists f \neq 0 \in L[t] : f(\alpha) = 0$, hence $M : L$ is algebraic.

Exercise 7.3.2

Using Lemma 7.3.1, show that every automorphism of a field is an automorphism over its prime subfield. In other words, $Aut(M) = Gal(M : K)$ whenever M is a field with prime subfield K.

Solution: By **Lemma 7.3.1** we have that $\forall S \subseteq Aut(M),\ Fix(S) \subseteq M$. Since K is the prime subfield of M we have that $K \subseteq Fix(S) \subseteq M$, and we also have that $K \subseteq Fix(S) \subseteq M : K$. Hence we have that:

$$\begin{aligned} Aut(M) &= \{S : Fix(S) \subseteq M\} \\ &= \{S : K \subseteq Fix(S) \subseteq M\} \\ &= \{S : K \subseteq Fix(S) \subseteq M : K\} \\ &= \{S : Fix(S) \subseteq M : K\} \\ &= Gal(M : K) \quad \square \end{aligned}$$

Exercise 7.3.5

Find another example of Theorem 7.3.3.

Solution: We follow **Example 7.3.4**. If we have $\kappa : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ representing complex conjugation, then $H = \{id, \kappa\}$ is a subgroup of $Aut(\mathbb{Q}(\sqrt{2}))$. By **Theorem 7.3.3**, we have that $[\mathbb{Q}(\sqrt{2}) : \mathrm{Fix}(H)] \leq |H| = 2$. Since $\mathrm{Fix}(H) = \mathbb{Q}$, and we know that $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, the inequality holds.

Chapter 8. The fundamental theorem of Galois theory

Exercise 8.1.4

Prove the first half of Lemma 8.1.2(i).

Solution: We assume that $L_1 \subseteq L_2$ and let $\phi \in Gal(M : L_2)$. Then we have that $\phi(\alpha) = \alpha \ \forall \alpha \in L_2$. Hence we have that $\phi(\alpha) = \alpha \ \forall \alpha \in L_1$, hence $\phi \in Gal(M : L_1)$