MATH 6122: selected solutions

Written and formatted by John M. Campbell
jmaxwellcampbell@gmail.com

1 MATH 6122 exercises

Exercise 1.1. If possible, construct countable products and countable coproducts in the category **Ring**.

Solution 1.2. Recall that a product of objects A and B in a category $\mathscr{C}$, provided that it exists according to the following construction, may be defined in the following manner, and consists of:

- An object $P \in \text{ob}(\mathscr{C})$;
- A morphism $\pi_A \colon P \to A$; and
- A morphism $\pi_B \colon P \to B$,

such that there exists a unique morphism $\phi \colon C \to P$ such that the following diagram commutes, where $C \in \text{ob}(\mathscr{C})$ is arbitrary.

$$\begin{tikzcd}
 & & A \\
C \arrow[rru, bend left, "f"] \arrow[r, dotted, "\phi"] \arrow[rrd, bend right, "g"'] \arrow[ru, phantom, "\equiv"] \arrow[rd, phantom, "\equiv"] & P \arrow[ru, "\pi_A"'] \arrow[rd, "\pi_B"] & \\
 & & B
\end{tikzcd}$$

Similarly, for objects A and B in a category $\mathscr{C}$, the ordered tuple (P, i_A, i_B) is a coproduct of A and B if the universal property indicated below is satisfied.

$$\begin{tikzcd}
A \arrow[rd, "i_A"'] \arrow[rrd, bend left] \arrow[rr, phantom, "\equiv"'] & & \\
 & P \arrow[r, dotted, "\phi"] & C \\
B \arrow[ru, "i_B"] \arrow[rru, bend right] \arrow[rr, phantom, "\equiv"] & &
\end{tikzcd}$$

So, let I be a countable index set, and let A_i be an object in **Ring** for each index $i \in I$.

So, we define the product of the objects in the family $\{A_i\}_{i \in I}$ in **Ring** so as to consist of an object P in **Ring**, together with a projection morphism

$$\pi_{A_i} : P \to A_i$$

for each index $i \in I$ such that: for each object C in **Ring**, and for each morphism $f_i : C \to A_i$, there exists a unique morphism ϕ such that the following diagram commutes, and the morphism ϕ is the same for each index i.

$$\begin{tikzcd}
A_i & \\
C \arrow[u, "f_i"] \arrow[r, dotted, "\phi"'] \arrow[ur, phantom, "\equiv"] & P \arrow[ul, "\pi_i"']
\end{tikzcd}$$

Similarly, we define the coproduct of the objects in $\{A_i\}_{i \in I}$ so as to consist of an object P in **Ring**, along with a morphism $j_i : A_i \to P$ for each index $i \in I$ such that: for all objects C in **Ring**, and for all morphisms $f_i : A_i \to C$, there exists a unique morphism ϕ such that the following diagram commutes, and the morphism ϕ is the same for all $i \in I$.

$$\begin{tikzcd}
A_i \arrow[d, "f_i"] \arrow[dr, "j_i"] & \\
C & P \arrow[l, dotted, "\phi"]
\end{tikzcd}$$

Exercise 1.3. Prove that in a given category, coproducts, if they exist, are unique up to isomorphism.

Solution 1.4. Let A and B be objects in a category $\mathscr{C}$, so that the ordered tuple (P, i_A, i_B) is a coproduct of A and B, with the universal property indicated below being satisfied.

$$\begin{tikzcd}
A \arrow[dr, "i_A"'] \arrow[drr, bend left] \arrow[drr, phantom, "\equiv"] & & \\
 & P \arrow[r, dotted, "\phi"] & C \\
B \arrow[ur, "i_B"] \arrow[urr, bend right] \arrow[urr, phantom, "\equiv"] & &
\end{tikzcd}$$

Now, suppose that (P', i'_A, i'_B) is also coproduct of A and B, so that the universal property indicated below holds.

$$\begin{tikzcd}
A \arrow[ddr, "i'_A"'] \arrow[ddrr, bend left] & & \\
 & \equiv & \\
 & P' \arrow[r, dashed, "\phi'"] & C \\
 & \equiv & \\
B \arrow[uur, "i'_B"] \arrow[uurr, bend right] & &
\end{tikzcd}$$

Our proof of the unicity of coproducts is heavily based upon a similar proof which is available through the `https://proofwiki.org/` website. With respect to the former diagram, let C be equal to P', let the morphism from A to C be i'_A, and let the morphism from B to $C = P'$ be equal to i'_B. Given the universal property satisfied with respect to the coproduct (P', i'_A, i'_B) of A and B, we thus obtain a commutative diagram of the following form.

$$\begin{tikzcd}
A \arrow[ddr, "i_A"'] \arrow[ddrr, bend left, "i'_A"] \arrow[ddrrr, bend left=40] & & & \\
 & \equiv & & \\
 & P \arrow[r, dashed, "\phi"] & P' \arrow[r, dashed, "\phi'"] & C \\
 & \equiv & & \\
B \arrow[uur, "i_B"] \arrow[uurr, bend right, "i'_B"'] \arrow[uurrr, bend right=40] & & &
\end{tikzcd}$$

Now, with respect to the above commutative diagram, let C be equal to P, and let the unlabeled morphism in this diagram from A to C be equal to i_A. Also, let the unlabeled morphism from B to C be equal to i_B, as illustrated below.

$$\begin{tikzcd}
A \arrow[ddr, "i_A"'] \arrow[ddrr, bend left, "i'_A"] \arrow[ddrrr, bend left=40, "i_A"] & & & \\
 & \equiv & & \\
 & P \arrow[r, dashed, "\phi"] & P' \arrow[r, dashed, "\phi'"] & P \\
 & \equiv & & \\
B \arrow[uur, "i_B"] \arrow[uurr, bend right, "i'_B"'] \arrow[uurrr, bend right=40, "i_B"'] & & &
\end{tikzcd}$$

So, from the above diagram, we have that the following diagram commutes.

$$\begin{tikzcd}
A \arrow[ddr, "i_A"'] \arrow[ddrr, bend left, "i_A"] & & \\
& \equiv & \\
& P \arrow[r, "\phi' \circ \phi"] & P \\
& \equiv & \\
B \arrow[uur, "i_B"] \arrow[uurr, bend right, "i_B"'] & &
\end{tikzcd}$$

By definition of a coproduct, we have that the endomorphism on P in the above diagram must be unique. Since P is an object of the category $\mathscr{C}$, we have that the set $\mathrm{Hom}_{\mathscr{C}}(P, P)$ is nonempty, by definition of a category, with an identity morphism $1_P = \mathrm{id}_P \in \mathrm{Hom}_{\mathscr{C}}(P, P)$. So, from the identity morphism axiom, we have that the following diagram must commute.

$$\begin{tikzcd}
A \arrow[ddr, "i_A"'] \arrow[ddrr, bend left, "i_A"] & & \\
& \equiv & \\
& P \arrow[r, "1_P"] & P \\
& \equiv & \\
B \arrow[uur, "i_B"] \arrow[uurr, bend right, "i_B"'] & &
\end{tikzcd}$$

Since the endomorphism on P in the above diagram must be unique, we thus have that

$$\phi' \circ \phi = 1_P.$$

A symmetric argument may be used to prove that:

$$\phi \circ \phi' = 1_{P'},$$

thus proving that $P \cong P'$, as desired.

Exercise 1.5. Show how free groups may be constructed using the category-theoretic definition of a free object given in class.

Solution 1.6. Let **Grp** denote the category of groups, and let

$$\mathcal{U} = \mathcal{U}_{\mathbf{Grp}} \colon \mathbf{Grp} \to \mathbf{Set}$$

denote the canonical forgetful functor on **Grp**, which, informally, "forgets" the group structures on objects in **Grp**. We thus have that $(\mathbf{Grp}, \mathcal{U})$ is a concrete category.

We thus proceed to construct an appropriate functor

$$F \colon \mathbf{Set} \to \mathbf{Grp}$$

in order to apply the category-theoretic definition of a free object given in class. The following discussion is heavily based upon the section on free groups given in Fraleigh's "A First Course in Abstract Algebra".

Given a set X, let $F[X]$ denote the set of all reduced words formed from the alphabet X. We define a *word* over X as a finite string of symbols of the form x^z for $z \in \mathbb{Z}$ and $x \in X$, written in juxtaposition. The *elementary contractions* consist of functions given by the replacement of an occurrence of the form $x^m x^n$ with x^{m+n}, as well as the mapping given by the removal of an occurrence of x^0. A *reduced word* is a word for which no more elementary contractions are possible.

Letting $F[X]$ be as given above, we endow $F[X]$ with the binary operation $\cdot$ so that for elements w_1 and w_2 in $F[X]$, the expression $w_1 \cdot w_2$ is equal to the reduced form of the word obtained by the concatenation $w_1 w_2$.

In the following solution, we show how this construction agrees with the universal property given in the category-theoretic definition of a free object.

Exercise 1.7. In **Grp**, what is $F[X]$, with respect to the commutative diagram used to define a free object? Study some different ways of defining free objects in **Grp**. How can these different definitions be reformulated in terms of a category-theoretic framework? How can these different definitions be reformulated using forgetful functors?

Solution 1.8. As above, we may let $F[X]$ denote the set of all reduced words from the alphabet $X \in \text{ob}(\textbf{Set})$, letting $F[X]$ be endowed with the binary operation $\cdot$ given above. Equivalently, $F[X]$ may be informally defined as "the group generated by X" or "the smallest group containing X", which agrees with the above definition.

It can be shown that the definition of $F[X]$ involving reduced words given above agrees with the category-theoretic definition of a free object. To show this, we make use of the following theorem from Fraleigh's "A First Course in Abstract Algebra":

Theorem: Let G be generated by the family $X = \{x_i \mid i \in I\}$ and let G' be any group. If x_i' is an element in G' for each index $i \in I$, such that expressions of these forms are not necessarily distinct, then there is at most one homomorphism $\phi: G \to G'$ such that $\phi(x_i) = x_i'$. If G is free on A, then there is exactly one such homomogrphism.

So, let X be an object in **Set**, and let $F[X]$ be defined in a concrete way with respect to reduced words as above. So, for an arbitrary object G' in **Grp**, and given an arbitrary morphism $f: X \to \mathcal{U}[G']$, there is a unique homomorphism $\phi: F[X] \to G'$ such that the following diagram commutes, where the injective mapping from X to $\mathcal{U}[F[X]]$ is canonical.

$$\begin{tikzcd}
\mathcal{U}[F[X]] \arrow[r, dotted, "\mathcal{U}[\phi]"] & \mathcal{U}[G'] \\
X \arrow[u, hook, "i_X"] \arrow[ur, "f"'] &
\end{tikzcd}$$

Exercise 1.9. Let $(\mathscr{C}, \mathcal{U})$ be a concrete category, and let $F: \textbf{Set} \to \mathscr{C}$ be the functor mapping objects X in **Set** to corresponding free objects $F[x]$ in $\mathscr{C}$. Prove that if $X \cong X' \implies F[X] \cong F[X']$.

Solution 1.10. Given a category $\mathscr{C}$, and objects A and B in $\text{ob}(\mathscr{C})$, the objects A and B are said to be isomorphic if there exist morphisms ϕ and ψ such that the diagram illustrated below commutes. This is denoted by: $A \cong B$.

$$\begin{tikzcd}
A \arrow[loop left, "1_A"] \arrow[r, bend left, "\phi"] & B \arrow[l, bend left, "\psi"] \arrow[loop right, "1_B"]
\end{tikzcd}$$

So, suppose that $X \cong X'$ in the category **Set**. By the category-theoretic definition of an isomorphism, we have that there exist morphisms b and a such that the following diagram commutes.

$$\begin{tikzcd}
X \arrow[loop left, "1_X"] \arrow[r, bend left, "b"] & X' \arrow[l, bend left, "a"] \arrow[loop right, "1_{X'}"]
\end{tikzcd}$$

By definition of the free object $F[X]$, we have that: for each object G in $\mathscr{C}$, and each morphism $f\colon X \to \mathcal{U}[G]$, there exists a unique morphism $\phi\colon F[X] \dashrightarrow G$ such that the following diagram commutes.

$$\begin{tikzcd}
\mathcal{U}[F[X]] \arrow[r, dotted, "\mathcal{U}[\phi]"] & \mathcal{U}[G] \\
X \arrow[u, hook, "i_X"] \arrow[ur, "f"']
\end{tikzcd} \tag{1.1}$$

With respect to the commutative diagram given in (1.1), let $G = F[X']$, and let $f = i_{X'} \circ b$, letting $i_{X'}\colon X' \hookrightarrow \mathcal{U}[F[X']]$. Since the morphisms a and b essentially "cancel" with each other, we obtain a diagram of the following form.

$$\begin{tikzcd}
\mathcal{U}[F[X]] \arrow[r, dotted, "\mathcal{U}[\phi]"] & \mathcal{U}[F[X']] \\
X \arrow[u, hook, "i_X"] \arrow[ur, "f=i_{X'}\circ b"'] & \\
X' \arrow[u, hook, "a"] \arrow[uur, hook, "i_{X'}"'] &
\end{tikzcd}$$

By essentially repeating the above argument, we obtain a commutative diagram of the following form.

$$\begin{tikzcd}
\mathcal{U}[F[X]] \arrow[r, dotted, "\mathcal{U}[\phi]"] & \mathcal{U}[F[X']] \arrow[r, dotted, "\mathcal{U}[\psi]"] & \mathcal{U}[F[X]] \\
X' \arrow[u, "i_X\circ a"] \arrow[ur, "i_{X'}"'] \arrow[urr, "i_X\circ a"'] & &
\end{tikzcd}$$

From the above diagram together with (1.1), it is clear that $\psi \circ \phi$ must be equal to the identity morphism on $F[X]$, by unicity of the "upper" morphism illustrated in (1.1). A symmetric argument shows that the reverse composition also must be an identity morphism.

Exercise 1.11. Letting R be a unital ring, and letting X be a set, show that the underlying operations on the free R-module generated by X are well-defined in the sense that the expressions resulting from applying these operations are in $\bigoplus_{x \in X} R$.

Solution 1.12. Recall that we defined the functor $F\colon \mathbf{Set} \to \mathbf{R\text{-}Mod}$ so that an object X in **Set** is mapped to

$$\bigoplus_{x \in X} R = \{f\colon X \to R \mid f \text{ has finite support}\},$$

where the support of a function $f\colon X \to R$ is precisely $\{x \in X \mid f(x) \neq 0\}$.

We thus endow $\bigoplus_{x \in X} R$ with an additive operation given by componentwise addition, so that

$$(f + g)(x) \coloneqq f(x) +_R g(x)$$

for f and g in $\bigoplus_{x \in X} R$, letting x be an element in X. Similarly, we define the operation $\cdot$ so that $(r \cdot f)(x) \coloneqq r(f(x))$ for $r \in R$.

Since the set of elements $x \in X$ such that $f(x)$ is nonzero is finite, and since the set of elements $y \in X$ such that $g(y)$ is nonzero is also finite, it is clear that the set of elements $z \in X$ such that $f(x) +_R g(x)$ is nonzero must be finite. In particular, if $f(x) +_R g(x)$ is nonzero, then it is obvious that either $f(x)$ or $g(x)$ must be nonzero, thus proving the inclusion whereby:

$$\mathrm{Supp}(f + g) \subseteq \mathrm{Supp}(f) \cup \mathrm{Supp}(g).$$

This shows that the additive operation on $\bigoplus_{x \in X} R$ given by componentwise addition is a binary operation on $\bigoplus_{x \in X} R$.

Now consider the expression $r \cdot f$. Since there are only finitely many elements $x \in X$ such that $f(x)$ is nonzero, it is obvious that there are only finitely many elements $y \in X$ such that $r \cdot f(y)$ is nonzero. If $r = 0$, then it is obvious that

$$\mathrm{Supp}(rf) \subseteq \mathrm{Supp}(f).$$

Now suppose that $r \neq 0$. Then if $r \cdot f(y)$ is nonzero, then it cannot be the case that $f(y)$ is nonzero, thus proving the desired inclusion whereby

$$\mathrm{Supp}(rf) \subseteq \mathrm{Supp}(f)$$

for $r \neq 0$. This shows that the operation $\cdot$ is such that $r \cdot f \in \bigoplus_{x \in X} R$.

Exercise 1.13. Letting X be a set, prove that $F[X]$ is free in **R-Mod**.

Solution 1.14. Let N be an arbitrary object in **R-Mod**, and let $f\colon X \to \mathcal{U}[N]$ be an arbitrary morphism in **Set**. Writing $\bigoplus_{x \in X} R$ in place of $F[X]$ as above, let X be written as a family, writing $X = \{x_i\}_{i \in I}$ and $f(x_i) = n_i \in \mathcal{U}[N]$ for each index i in I.

We may let the injective morphism

$$i_X\colon X \to \mathcal{U}[X]$$

be such that for $i \in I$, with $x_i \in X$ as an arbitrary element in X, $i_X(x_i)$ is equal to the function $g_i\colon X \to R$ which maps x_i to 1 and which maps x_j to 0 for $j \in I \setminus \{i\}$.

Given an arbitrary element $g\colon X \to R$ in $F[X] = \bigoplus_{x \in X} R$, we have that g has finite support. First suppose that the support of g is not equal to $\varnothing$. Letting $\{x_{i_1}, x_{i_2}, \ldots, x_{i_m}\} \subseteq X$ denote the support of

$g \in \bigoplus_{x\in X} R$ for some $m \in \mathbb{N}$, write $g(x_j) = r_j \in R$, for all indices j. Now, observe that the mapping g may be rewritten so that:

$$g = r_{i_1} i_X(x_{i_1}) + r_{i_2} i_X(x_{i_2}) + \cdots + r_{i_m} i_X(x_{i_m}).$$

Now, suppose that ϕ is a morphism such that the following diagram commutes:

$$\begin{tikzcd}
\mathcal{U}[F[X]] \arrow[r, "\mathcal{U}[\phi]"] & \mathcal{U}[N] \\
X \arrow[u, hook, "i_X"] \arrow[ur, "f"'] &
\end{tikzcd}$$

Since ϕ is a morphism, and since $\mathcal{U}$ is a functor, we have that the following holds, writing ϕ in place of $\mathcal{U}[\phi]$ for the sake of clarity, and similarly for objects such as $g \in F[X]$:

$$\begin{aligned}
\phi(g) &= \phi\big(r_{i_1} i_X(x_{i_1}) + r_{i_2} i_X(x_{i_2}) + \cdots + r_{i_m} i_X(x_{i_m})\big) \\
&= \phi\big(r_{i_1} i_X(x_{i_1})\big) + \phi\big(r_{i_2} i_X(x_{i_2})\big) + \cdots + \phi\big(r_{i_m} i_X(x_{i_m})\big) \\
&= r_{i_1}\phi\big(i_X(x_{i_1})\big) + r_{i_2}\phi\big(i_X(x_{i_2})\big) + \cdots + r_{i_m}\phi\big(i_X(x_{i_m})\big) \\
&= r_{i_1} f(x_{i_1}) + r_{i_2} f(x_{i_2}) + \cdots + f(x_{i_m}) \\
&= r_{i_1} n_{i_1} + r_{i_2} n_{i_2} + \cdots + n_{i_m}.
\end{aligned}$$

So, we have shown that if ϕ is a morphism such that the above diagram commutes, ϕ must be uniquely defined on non-identity elements in the domain of ϕ, as above. Given that ϕ is a morphism, it must map the additive identity element in the domain of ϕ to the additive identity element in N, thus proving the unicity of ϕ.

Exercise 1.15. Assume R is a commutative ring with 1. For an ideal $I \subseteq R$, show: $R^n/IR^n \cong (R/I)^n$.

Solution 1.16. Let $n \in \mathbb{N}$, and let $r_1, r_2, \ldots, r_n \in R$, so that the ordered n-tuple $(r_1, r_2, \ldots, r_n)$ is an arbitrary element in R^n. So, the expression

$$(r_1, r_2, \ldots, r_n) + IR^n$$

is an arbitrary element in R^n/IR^n. Define the mapping

$$\phi \colon R^n/IR^n \to (R/I)^n$$

so that

$$\phi\big((r_1, r_2, \ldots, r_n) + IR^n\big) = (r_1 + I, r_2 + I, \ldots, r_n + I) \in (R/I)^n.$$

Letting $q_1, q_2, \ldots, q_n \in R$, suppose that:

$$(r_1, r_2, \ldots, r_n) + IR^n = (q_1, q_2, \ldots, q_n) + IR^n.$$

Equivalently,

$$(r_1 - q_1, r_2 - q_2, \ldots, r_n - q_n) \in IR^n.$$

So, each expression of the form $r_i - q_i$ is in the ideal I, for each index i. We thus have that

$$(r_1 - q_1 + I, r_2 - q_2 + I, \ldots, r_n - q_n + I) = (0 + I, 0 + I, \ldots, 0 + I),$$

so that

$$(r_1 + I, r_2 + I, \ldots, r_n + I) = (q_1 + I, q_2 + I, \ldots, q_n + I),$$

thus proving that the mapping ϕ is well-defined. It is clear that ϕ preserves addition, as indicated below.

$$\begin{aligned}
&\phi\big((r_1, r_2, \dots, r_n) + IR^n\big) + \phi\big((q_1, q_2, \dots, q_n) + IR^n\big)\\
&= (r_1 + I, r_2 + I, \dots, r_n + I) + (q_1 + I, q_2 + I, \dots, q_n + I)\\
&= (r_1 + q_1 + I, r_2 + q_2 + I, \dots, r_n + q_n + I)\\
&= \phi\big((r_1 + q_1, r_2 + q_2, \dots, r_n + q_n) + IR^n\big)\\
&= \phi\big((r_1, r_2, \dots, r_n) + IR^n + (q_1, q_2, \dots, q_n) + IR^n\big).
\end{aligned}$$

Similarly, we have that ϕ preserves multiplication, as shown below.

$$\begin{aligned}
&\phi\big((r_1, r_2, \dots, r_n) + IR^n\big) \cdot \phi\big((q_1, q_2, \dots, q_n) + IR^n\big)\\
&= (r_1 + I, r_2 + I, \dots, r_n + I) \cdot (q_1 + I, q_2 + I, \dots, q_n + I)\\
&= (r_1 \cdot q_1 + I, r_2 \cdot q_2 + I, \dots, r_n \cdot q_n + I)\\
&= \phi\big((r_1 \cdot q_1, r_2 \cdot q_2, \dots, r_n \cdot q_n) + IR^n\big)\\
&= \phi\big(((r_1, r_2, \dots, r_n) + IR^n) \cdot ((q_1, q_2, \dots, q_n) + IR^n)\big).
\end{aligned}$$

Since the unity element in the domain of ϕ is

$$(1, 1, \dots, 1) + IR^n \in R^n/IR^n,$$

and since

$$\phi((1, 1, \dots, 1) + IR^n) = (1 + I, 1 + I, \dots, 1 + I) \in (R/I)^n,$$

we have that ϕ is a ring homomorphism. Given an element

$$(r_1 + I, r_2 + I, \dots, r_n + I) \in (R/I)^n$$

we have that

$$\phi\big((r_1, r_2, \dots, r_n) + IR^n\big) = (r_1 + I, r_2 + I, \dots, r_n + I) \in (R/I)^n,$$

thus establishing the surjectivity of ϕ. Now, suppose that:

$$\phi\big((r_1, r_2, \dots, r_n) + IR^n\big) = \phi\big((q_1, q_2, \dots, q_n) + IR^n\big).$$

Equivalently,

$$(r_1 + I, r_2 + I, \dots, r_n + I) = (q_1 + I, q_2 + I, \dots, q_n + I).$$

Since

$$(r_1 - q_1 + I, r_2 - q_2 + I, \dots, r_n - q_n + I) = (0 + I, 0 + I, \dots, 0 + I),$$

writing

$$(r_1 - q_1, r_2 - q_2, \dots, r_n - q_n) = (i_1, i_2, \dots, i_n) \in I^n$$

where $i_1, i_2, \dots, i_n \in I$, we have that the following equality holds.

$$\begin{aligned}
&(r_1 - q_1, r_2 - q_2, \dots, r_n - q_n)\\
&= i_1(1, 0, 0, \dots, 0) + i_2(0, 1, 0, 0, \dots, 0) + \cdots + i_n(0, 0, \dots, 1) \in IR^n.
\end{aligned}$$

Since

$$(r_1 - q_1, r_2 - q_2, \dots, r_n - q_n) \in IR^n$$

we have that

$$(r_1 - q_1, r_2 - q_2, \ldots, r_n - q_n) + IR^n = 0 + IR^n.$$

Therefore,

$$(r_1, r_2, \ldots, r_n) + IR^n = (q_1, q_2, \ldots, q_n) + IR^n,$$

thus proving the injectivity of ϕ. So, we have shown that ϕ is a bijective ring homomorphism, thus proving the desired equivalence whereby $R^n/IR^n \cong (R/I)^n$.

Exercise 1.17. Recall that we can find maximal ideals in a commutative ring R with 1. Conclude that for any finite sets A and B,

$$F[A] \cong F[B] \iff |A| = |B|,$$

letting $F[X]$ denote the free R-module generated by a given set X.

Solution 1.18. Let $m \in \mathbb{N}_0$ and $n \in \mathbb{N}_0$ respectively denote the cardinalities of A and B. Let I denote a fixed maximal ideal in R. First suppose that $F[A] \cong F[B]$. We thus have that $R^m \cong R^n$, since $F[A] \cong R^m$, and similarly for $F[B]$. From our results given in the previous solution, we have that:

$$R^m/IR^m \cong (R/I)^m$$

and that

$$R^n/IR^n \cong (R/I)^n.$$

But since $R^m \cong R^n$, we have that:

$$R^m/IR^m \cong R^n/IR^n.$$

Therefore,

$$(R/I)^m \cong (R/I)^n.$$

Since I is a maximal ideal within R, we have that R/I is a field. So, since $(R/I)^m$ and $(R/I)^n$ are isomorphic as vector spaces, we have that $m = n$ as desired, thus proving that A and B are bijectively equivalent. Conversely, suppose that $m = n$. In this case, since $F[A] \cong R^m$ and $F[B] \cong R^n$, we have that $F[A]$ and $F[B]$ must be isomorphic, since $R^m \cong R^n$ are isomorphic, since $m = n$.

Exercise 1.19. Find a ring R and an R-module M with bases of cardinality 1 and 2.

Solution 1.20. The following discussion is based upon the linked Wikipedia article on invariant basis numbers[1]. A ring R has invariant basis number (IBN) if for all natural numbers m and n, if R^m and R^n are isomorphic as left R-modules, then $m = n$.

Let $\mathbb{CFM}_{\mathbb{N}}(R)$ denote the ring of column finite matrices, i.e., the matrices over R with entries indexed by $\mathbb{N} \times \mathbb{N}$ with each column having only finitely many non-zero entries. We claim that: $\mathbb{CFM}_{\mathbb{N}}(R)$ and $\mathbb{CFM}_{\mathbb{N}}(R) \times \mathbb{CFM}_{\mathbb{N}}(R)$ are isomorphic as left modules. This is easily seen using the mapping

$$\psi \colon \mathbb{CFM}_{\mathbb{N}}(R) \to \mathbb{CFM}_{\mathbb{N}}(R)^2$$

mapping a given matrix M in the above domain to the matrix obtained by listing the odd columns of M, and then listing the even columns of M.

Exercise 1.21. Assume R is a commutative ring with 1. We say that an R-module M is irreducible if there are no non-trivial proper R-submodules. Show that the following are equivalent.

[1] See `https://en.wikipedia.org/wiki/Invariant_basis_number`.

(a) M is irreducible;

(b) $M \cong R/I$ for some maximal ideal $I \subseteq R$;

(c) $M = Ra$ for all $0 \neq a \in M$.

Solution 1.22. Let (a), (b), and (c) respectively denote the first, second, and third statements given in the above list.

(a) $\Longrightarrow$ (b) Suppose that M is irreducible. So, given an arbitrary nonzero element $m \neq 0$ such that $m \in M$, we find that the R-submodule generated by $m \in M$ must be equal to M. Therefore, $M = Rm$. Now, let $m \neq 0$ be a fixed nonzero element in M. Now, consider the set

$$I = \{r \in R \mid rm = 0\} \subseteq R.$$

Given two elements r_1 and r_2 in this set, we have that $r_1 m = 0$ and $r_2 m = 0$, so that $r_1 m + r_2 m = (r_1 + r_2)m = 0$, thus proving that I is closed with respect to the underlying additive binary operation on R, letting r_1 and r_2 be arbitrary elements in R. Now, given an element $r \in I$, with $rm = 0$, and given an element $s \in R$, we have that $s(rm) = 0$, so that $(sr)m = 0$, thus proving that I is an ideal of R. Now consider the quotient ring R/I. Let the expression R/I denote the R-module whereby addition is as given in the quotient ring R/I, and such that multiplication is defined in the following way. Letting $s \in R$, let multiplication by an element $r \in R$ in this R-module be such that $r(s+I) = rs + I \in R/I$. Now, define

$$\phi \colon M = Rm \to R/I$$

so that given an element $r \in R$, so that rm is an arbitrary element in $M = Rm$, we have that

$$\phi(rm) = r + I \in R/I.$$

It is clear that ϕ preserves addition:

$$\phi(r_1 m) + \phi(r_2 m) = (r_1 + I) + (r_2 + I) = r_1 + r_2 + I = \phi((r_1 + r_2)m)$$

letting $r_1, r_2 \in R$. Similarly, ϕ preserves multiplication by elements in R: $s\phi(rm) = s(r + I) = sr + I = \phi(s(rm))$. Given an element $r \in R$, so that $r + I$ is an arbitrary element in the codomain of ϕ, we have that

$$\phi(rm) = r + I,$$

which shows that ϕ is surjective. Now, suppose that

$$\phi(r_1 m) = \phi(r_2 m),$$

letting r_1 and r_2 be elements in R. We thus have that:

$$r_1 + I = r_2 + I,$$

so that

$$r_1 - r_2 \in I,$$

thus proving that

$$(r_1 - r_2)m = 0,$$

which shows that

$$r_1 m = r_2 m,$$

thus proving that ϕ is an R-module isomorphism. Now, we must prove that I is a maximal ideal of R. By way of contradiction, suppose that there exists an ideal $J \subsetneq R$ such that:

$$\{r \in R \mid rm = 0\} \subsetneq J \subsetneq R.$$

So, let s be an element in J so that $sm \neq 0$. Write $sm = n \in M$, with $n \neq 0$. Now let t be another element such that $tm \neq 0$. Since $Rn = Rm$, we have that $t'n = tm$ for some $t' \in R$. So $t'sm = tm$. That is, $t's = t$. But then t has to be in the ideal J, which shows that J must be equal to R, contradicting that $J \subsetneq R$.

(b) $\Longrightarrow$ (c) Suppose that $M \cong R/I$ for some maximal ideal $I \subsetneq R$, letting the R-module structure on R/I be as given above. Since $I \subsetneq R$ is a maximal ideal, we have that there must be some element $r \in R$ such that $r \notin I$. But then the ideal generated by the union of the singleton set $\{r\} \subseteq R$ and I must strictly contain I, and must be contained in R. By maximality of I, we thus have that the ideal generated by $\{r\} \cup I$ is R. That is, each element in R may be written in the form $sr + i$ for some $s \in R$ and some $i \in I$. Now consider the expression $r + I \in R/I$. Since each element in R may be written in the form $sr + i$ as above, we have that R/I, as an R-module, consists precisely of expressions of the form $sr + i + I$ for $s \in R$. That is, as an R-module, R/I consists precisely of expressions of the form $sr + I$ for $s \in R$. That is,

$$R/I = R(r + I),$$

thus proving that $M = Ra$ for some $a \in M$.

(c) $\Longrightarrow$ (a) Finally, suppose that $M = Ra$ for each nonzero element a in M. Given a nontrivial submodule N of M, and given a nonzero element $n \neq 0$ in N, we have that the submodule generated by n is equal to M, thus proving that $N = M$.

2 Problems from former exams

Exercise 2.1. Let G be a finite group, and let $Z(G)$ be the center of G. Show that the order of $G/Z(G)$ is not a prime.

Solution 2.2. Letting G be a finite group, we have that the center $Z(G)$ of G is equal to $\{z \in G : \forall g \in G \; gz = zg\}$. The center of $Z(G)$ is a normal subgroup of G, so $G/Z(G)$ has the structure of a quotient group. By way of contradiction, assume that the order of $G/Z(G)$ is equal to a prime number $p \in \mathbb{N}$. We thus have that the order of $G/Z(G)$ must be nontrivial. By Lagrange's theorem, we have that the order of each non-identity element in $G/Z(G)$ must be equal to $|G/Z(G)|$. This shows that $G/Z(G)$ must be a cyclic group. So, there exists an element g in G such that the coset $gZ(G)$ generates the cyclic group $G/Z(G)$. So, given elements a and b in G, we have that the coset $aZ(G)$ is equal to $g^n Z(G)$ for some integer n, and we have that $bZ(G)$ is equal to $g^m Z(G)$ for some integer m. We thus have that $a = g^n z_1$ and $b = g^m z_2$ for some element z_1 in the center of G and some element $z_2 \in Z(G)$. So, we have that the composition ab may be written as

$$ab = g^n z_1 g^m z_2,$$

and since z_1 and z_2 are in the center of G, we have that the expression $g^n z_1 g^m z_2$ may be rewritten in the following manner:

$$ab = g^n z_1 g^m z_2$$

$$\begin{aligned}
&= g^n g^m z_1 z_2\\
&= g^{n+m} z_1 z_2\\
&= g^{m+n} z_1 z_2\\
&= g^m g^n z_1 z_2\\
&= g^m g^n z_2 z_1\\
&= g^m z_2 g^n z_1\\
&= ba.
\end{aligned}$$

So, we have shown that $ab = ba$ for elements a and b in G. Therefore, G is abelian. Therefore, the center of G is equal to G. Therefore, the cardinality of the quotient $G/Z(G)$ is equal to 1, thus contradicting that the cardinality of $G/Z(G)$ is equal to a prime number.

Exercise 2.3. Given an example where the order of G/C is 4, where G denotes a group and C denotes the center of G.

Solution 2.4. Let G denote the dihedral group of order 8. Let the elements in the underlying set of this dihedral group be denoted as planar isometries. Then the center of G consists of the identity isometry, together with an isometry given by a half-turn rotation, so that the center of G is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. Letting C denote the center of G, since G is of order 8 and since C is of order 2, we have that G/C is of order 4.

Exercise 2.5. Let A be the abelian group generated by $\{x, y, z\}$ subject to the relations $2x+2y+2z = 0$, $2x + 2y = 0$ and $2x + 2z = 0$. Describe A as the direct sum of cyclic groups.

Solution 2.6. Let B denote the free abelian group generated by $\{x, y, z\}$, so that $B \cong \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}$. Now, let

$$C = \langle 2x + 2y + 2z, 2x + 2y, 2x + 2z \rangle$$

denote the abelian group generated by the set $\{2x + 2y + 2z, 2x + 2y, 2x + 2z\}$. Since B is abelian, we have that C is a normal subgroup B, and we find that the quotient B/C is isomorphic to A. So, our strategy is to find an ordered basis

$$\{b_1, b_2, b_3\} \subseteq B$$

of B and a basis

$$\{c_1, c_2, c_3\} \subseteq C$$

of C such that $c_i = s_i b_i$ for all indicates i, and such that $s_1|s_2|s_3$. Consider the following matrix product:

$$\begin{bmatrix} 2 & 2 & 2\\ 2 & 2 & 0\\ 2 & 0 & 2 \end{bmatrix} \begin{bmatrix} x\\ y\\ z \end{bmatrix} = \begin{bmatrix} 2x + 2y + 2z\\ 2x + 2y\\ 2x + 2z \end{bmatrix}.$$

Let M denote te above 3×3 matrix. Basically, it remains to determine the Smith Normal Form of M. We can apply row and column operations to find the Smith Normal Form of this matrix, as indicated below.

$$\begin{bmatrix} 2 & 2 & 2\\ 2 & 2 & 0\\ 2 & 0 & 2 \end{bmatrix} \xrightarrow{R_2 \longrightarrow R_2 - R_1}$$

$$\begin{bmatrix} 2 & 2 & 2 \\ 0 & 0 & -2 \\ 2 & 0 & 2 \end{bmatrix} \xrightarrow{R_3 \longrightarrow R_3 - R_1}$$

$$\begin{bmatrix} 2 & 2 & 2 \\ 0 & 0 & -2 \\ 0 & -2 & 0 \end{bmatrix} \xrightarrow{R_1 \longrightarrow R_1 + R_2}$$

$$\begin{bmatrix} 2 & 2 & 0 \\ 0 & 0 & -2 \\ 0 & -2 & 0 \end{bmatrix} \xrightarrow{R_1 \longrightarrow R_1 + R_3}$$

$$\begin{bmatrix} 2 & 0 & 0 \\ 0 & 0 & -2 \\ 0 & -2 & 0 \end{bmatrix} \xrightarrow{R_2 \longrightarrow -R_2}$$

$$\begin{bmatrix} 2 & 0 & 0 \\ 0 & 0 & 2 \\ 0 & -2 & 0 \end{bmatrix} \xrightarrow{R_3 \longrightarrow -R_3}$$

$$\begin{bmatrix} 2 & 0 & 0 \\ 0 & 0 & 2 \\ 0 & 2 & 0 \end{bmatrix} \xrightarrow{R_2 \longleftrightarrow R_3}$$

$$\begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix}.$$

So, since $B \cong \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}$, and since $C \cong (2\mathbb{Z}) \oplus (2\mathbb{Z}) \oplus (2\mathbb{Z})$, we may deduce that

$$A \cong B/C \cong (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z}).$$

Exercise 2.7. Let $K/\mathbb{Q}$ be the splitting field of $(x^2-2)(x^2-3)(x^2-5)$. How many distinct Galois extensions $F/\mathbb{Q}$ with $F \subseteq K$ can you find?

Solution 2.8. Since the polynomial $(x^2-2)(x^2-3)(x^2-5)$ has no repeated roots, we have that this polynomial is separable as an element in $\mathbb{Q}[x]$. We thus have that $K/\mathbb{Q}$ is the splitting field of a separable polynomial over $\mathbb{Q}$. So, we have that $K/\mathbb{Q}$ is a Galois extension. Exercise 3.166, which is given below, requires the evaluation of the Galois group of $(x^2-2)(x^2-3)(x^2-5)$, and the determination of all of the subfields of the splitting field of this polynomial. In our solution to Exercise 3.166, we showed that $\mathrm{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q})$ is an abelian group of order 8 such that σ^2 is the identity automorphism on $\mathrm{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q})$ for each element σ in $\mathrm{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q})$, so that

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}).$$

Now, by the Fundamental Theorem of Galois theory, we know that an intermediate field $F/\mathbb{Q}$ such that $\mathbb{Q} \subseteq F \subseteq K$ is Galois over $\mathbb{Q}$ if and only if subgroup corresponding to F is normal in $\mathrm{Gal}(K/\mathbb{Q})$. But since $\mathrm{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q})$ is an abelian group, every subgroup of this group is a normal subgroup, which shows that every corresponding subfield is Galois. In our solution for Exercise 3.166, we determined all of the intermediate fields between $\mathbb{Q}$ and K, which are also listed below. All of these fields are Galois, as indicated above.

Galois subfields
$\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$
$\mathbb{Q}(\sqrt{2},\sqrt{3})$
$\mathbb{Q}(\sqrt{2},\sqrt{5})$
$\mathbb{Q}(\sqrt{2},\sqrt{15})$
$\mathbb{Q}(\sqrt{3},\sqrt{5})$
$\mathbb{Q}(\sqrt{3},\sqrt{10})$
$\mathbb{Q}(\sqrt{5},\sqrt{6})$
$\mathbb{Q}(\sqrt{6},\sqrt{10},\sqrt{15})$
$\mathbb{Q}(\sqrt{2})$
$\mathbb{Q}(\sqrt{3})$
$\mathbb{Q}(\sqrt{6})$
$\mathbb{Q}(\sqrt{5})$
$\mathbb{Q}(\sqrt{10})$
$\mathbb{Q}(\sqrt{15})$
$\mathbb{Q}(\sqrt{30})$
$\mathbb{Q}$

Exercise 2.9. Let R be a commutative ring with identity. Prove that (x) is a prime ideal in $R[x]$ if and only if R is an integral domain.

Solution 2.10. In general, given a commutative unital ring S and an ideal I of S, we have that the quotient ring S/I is an integral domain if and only if I is a prime ideal in S, as we later prove. So, we have that (x) is a prime ideal in $R[x]$ if and only if $R[x]/(x)$ is an interal domain. We have that the ideal (x) consists precisely of elements in $R[x]$ with a constant term equal to 0. So, we have that $R[x]/(x) \cong R$. So, since (x) is a prime ideal in $R[x]$ if and only if $R[x]/(x)$ is an interal domain, and since $R[x]/(x) \cong R$, we have that (x) is a prime ideal in $R[x]$ if and only if R is an interal domain.

Recall that given a commutative ring S, and given an ideal I of this ring S, the ideal I is said to be a prime ideal[2] if $S \neq I$, and for $a, b \in S$, if $ab \in I$ then $a \in I$ or $b \in I$, by direct analogy with Euclid's lemma. Also recall that an integral domain is a commutative ring with unity and no zero divisors. Using these definitions, we proceed to prove that: given a commutative unital ring S and an ideal I of S, the quotient ring S/I is an integral domain if and only if I is a prime ideal in S.

($\Longrightarrow$) Assume that the quotient ring S/I is an integral domain. So we have that $S \neq I$. By definition of an integral domain, we have that there are no zero divisors in S/I. So, given arbitrary elements a and b in S, we have that the cosets $a + I \in S/I$ and $b + I \in S/I$ are such that: if the product

$$(a + I)\,(b + I)$$

is equal to the additive identity element in S/I, then either $a + I = 0 + I$ or $b + I = 0 + I$. That is,

$$(a + I)\,(b + I) = 0 + I \Longrightarrow (a + I = 0 + I) \vee (b + I = 0 + I).$$

Equivalently,

$$ab + I = 0 + I \Longrightarrow (a + I = 0 + I) \vee (b + I = 0 + I).$$

[2] See https://en.wikipedia.org/wiki/Prime_ideal.

Equivalently,

$$ab \in I \implies (a \in I) \vee (b \in I),$$

which shows that I must be prime.

($\Longleftarrow$) Conversely, assume that the ideal I is prime. So, by definition of a prime ideal, we have that $S \neq I$, and we have that: for all $a, b \in S$, if $ab \in I$, then either a or b is in I. Also, recall that we let the ring S be commutative and unital. Now, consider the quotient ring S/I. Since S is commutative and unital, we have that S/I is commutative and unital. So, to prove that S/I is an integral domain, it remains to prove that S/I has no zero divisors. By way of contradiction, suppose that a and b are elements in S such that:

(i) $a + I \neq 0 + I$;

(ii) $b + I \neq 0 + I$; and

(iii) $ab + I = 0 + I$.

Equivalently,

(i) $a \notin I$;

(ii) $b \notin I$; and

(iii) $ab \in I$.

But this contradicts that the ideal I is a prime ideal. □

Exercise 2.11. Let R be a commutative ring with identity. Prove that (x) is a maximal ideal in $R[x]$ if and only if R is a field.

Solution 2.12. In general, letting S denote a commutative unital ring, and letting I denote an ideal contained in S, we have that I is a maximal ideal with respect to S if and only if the quotient ring S/I is a field. We later prove this general result. Now, letting R be as given above, consider the principal ideal (x) generated by x in the polynomial ring $R[x]$, and observe that the ideal (x) consists precisely of polynomials in $R[x]$ with a constant term equal to 0. So, we find that the quotient ring $R[x]/(x)$ is isomorphic to the ring R consisting of constant polynomials in $R[x]$. So, we have that (x) is a maximal ideal in $R[x]$ if and only if $R[x]/(x)$ is a field, so that (x) is a maximal ideal in $R[x]$ if and only if R is a field, since $R \cong R[x]/(x)$. We proceed to prove the following more general result, letting S and I be as given above: I is a maximal ideal with respect to S if and only if the quotient ring S/I is a field.

($\Longrightarrow$) Assume that I is a maximal ideal with respect to S. So, we have that given an arbitrary ideal J of S satisfying

$$I \subseteq J \subseteq S,$$

it follows that either $I = J$ or $J = S$. That is, there does not exist any ideal K of S such that

$$I \subsetneq K \subsetneq S.$$

Now, consider the quotient ring S/I. Let s be an element in S, so that $s + I$ is a coset in S/I. Now, suppose that $s \notin I$, so that

$$s + I \neq 0 + I,$$

i.e., $s + I$ is not equal to the additive identity element in S/I. Now, consider the ideal J of S generated by $I \cup \{s\}$. Now, since s is not in I, we have that the ideal J generated by $I \cup \{s\}$ must strictly contain I. So, by maximality of I, we may deduce that $J = S$. That is, the ideal generated by $I \cup \{s\}$ is equal to S. In particular, since $1 \in S$, and since $1 \notin I$ we have that

$$i_1 t_1 + i_2 t_2 + \cdots + i_n t_n + s \cdot t_{n+1} = 1,$$

for some elements $i_1, i_2, \ldots, i_n \in I$, with $t_1, t_2, \ldots, t_{n+1} \in S$. Accordingly, we have that

$$(i_1 t_1 + i_2 t_2 + \cdots + i_n t_n + s \cdot t_{n+1}) + I = 1 + I,$$

so that

$$s \cdot t_{n+1} + I = 1 + I,$$

which shows that each element in S/I which is not equal to the additive identity element in S/I must be a unit in S/I. We thus have that S/I is a field, as desired.

($\Longleftarrow$) Conversely, assume that the quotient ring S/I is a field. Now, suppose that J is an ideal of I which strictly contains I. So, there exists at least one element s in J which is not in I. Since s is not in I, we have that

$$s + I \neq 0 + I,$$

i.e., $s + I$ is not equal to the additive identity element in the quotient ring S/I. Now, from our initial assumtion that the quotient ring S/I is a field, we have that there must be an element t in S such that:

$$st + I = 1 + I.$$

So, there must be an element i in the ideal I such that

$$i + st = 1.$$

Not, let r be an arbitrary element in S. From the equality

$$i + st = 1.$$

we have that

$$ir + rst = r.$$

But since J contains I, with $i \in J$, and since $s \in J$, we have that

$$ir + rst = r \in J,$$

which shows that J must be equal to S, which shows that the ideal I must be maximal. □

Exercise 2.13. Give an example of a commutative ring R which has a non-zero prime ideal that is not a maximal ideal.

Solution 2.14. If R is a commutative ring and if I is a non-zero prime ideal of R that is not a maximal ideal, then we have that R/I is an integral domain which is not a field. Now, consider the ring $\mathbb{Z}[x]$ consisting of polynomials with integer coefficients. Now, consider the principal ideal (x) generated by the polynomial x consisting of polynomials in $\mathbb{Z}[x]$ with constant term equal to 0. Since $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$, we have that the quotient ring $\mathbb{Z}[x]/(x)$ is an integral domain, but not a field. This shows that the principal ideal (x) is a prime ideal in $\mathbb{Z}[x]$, but not a maximal ideal. So, we have that $\mathbb{Z}[x]$ is a commutative ring which has a non-zero prime ideal that is not a maximal ideal.

3 Textbook exercises

The solutions given in this section are for assigned exercises given in the class textbook by Dummit and Foote.

3.1 Exercises from Appendix II

Exercise 3.1. Let N be a group and let $\mathbf{Nor}$–N be the collection of all groups that contain N as a normal subgroup. A morphism between objects A and B is any group homomorphism that maps N into N. Prove that $\mathbf{Nor}$–N is a category.

Solution 3.2. We begin by briefly reviewing the definition of a category given in the aforementioned class textbook:

Definition: (p.911-912) A *category* $\mathbf{C}$ consists of a class of *objects* and sets of *morphisms* between those objects. For every ordered pair (A, B) consisting of objects, there exists a set $\text{Hom}_{\mathbf{C}}(A, B)$ of morphisms from A to B, and for every triple A, B, C of objects there is a *law of composition* of morphisms, i.e., a map

$$\text{Hom}_{\mathbf{C}}(A, B) \times \text{Hom}_{\mathbf{C}}(B, C) \longrightarrow \text{Hom}_{\mathbf{C}}(A, C)$$

where $(f, g) \mapsto gf$, and gf is called the composition of g with f. The objects and morphisms satisfy the following axioms: for objects A, B, C, and D:

(i) if $A \neq C$ or $B \neq D$, then $\text{Hom}_{\mathbf{C}}(A, B)$ and $\text{Hom}_{\mathbf{C}}(C, D)$ are disjoint sets;

(ii) composition of morphisms is associative; and

(iii) each object has an identity morphism.

Now, let N and $\mathbf{Nor}$–N be as given above. So, we have that $\mathbf{Nor}$–N consists of a class of objects and sets of morphisms between those objects, whereby morphisms between objects A and B are precisely group homomorphisms mapping N into N. In particular, we let $\text{Hom}_{\mathbf{Nor}-N}(A, B)$ denote the set of morphisms from A to B. Now, let A, B, and C be objects in $\mathbf{Nor}$–N. Let f be in $\text{Hom}_{\mathbf{C}}(A, B)$, and let g be in $\text{Hom}_{\mathbf{C}}(B, C)$. So, $f\colon A \to B$ is a group homomorphism that maps N into N, and $g\colon B \to C$ is a group morphism that maps N into N. Since f and g are both group homomorphisms, we have that

$$gf(a_1 \bullet a_2) = g(f(a_1 \bullet a_2)) = g(f(a_1) \bullet' f(a_2)) = g(f(a_1)) \bullet'' g(f(a_2)),$$

given elements a_1 and a_2 in A, and given appropriately-defined binary operations $\bullet$, $\bullet'$, and $\bullet''$. This shows that gf is also a group morphism. Since $f(N) \subseteq N$ and $g(N) \subseteq N$, we have that $gf(N) \subseteq g(N) \subseteq N$, thus proving that $gf(N) \subseteq N$.

Now, let A, B, C, and D be objects in $\mathbf{Nor}$–N. If $A \neq C$, then the domain of each element in $\text{Hom}_{\mathbf{C}}(A, B)$ is not equal to the domain of each element $\text{Hom}_{\mathbf{C}}(C, D)$. Similarly, if B is not equal to D, then the codomain of each element in $\text{Hom}_{\mathbf{C}}(A, B)$ is not equal to the codomain of each element in $\text{Hom}_{\mathbf{C}}(C, D)$. This shows that $\text{Hom}_{\mathbf{C}}(A, B)$ and $\text{Hom}_{\mathbf{C}}(C, D)$ are disjoint in the case whereby $A \neq C$ or $B \neq D$. So, the above axiom listed enumerated as (i) holds. In general, the composition of functions is associative, so axiom (ii) as above holds. Finally, it is clear that each object A has an identity morphism, since the identity morphism on A maps N to N.

Exercise 3.3. Show how the projection homomorphism $G \mapsto G/N$ may be used to define a functor from **Nor**–N to **Grp**.

Solution 3.4. We begin by reviewing the definition of a functor from the class textbook. Letting $\mathbf{C}$ and $\mathbf{D}$ be categories, we have that $\mathcal{F}$ is a *coinvariant functor* from $\mathbf{C}$ to $\mathbf{D}$ if: for every object A in $\mathbf{C}$, $\mathcal{F}A$ is an object in $\mathbf{D}$, and for every element f in $\mathrm{Hom}_{\mathbf{C}}(A, B)$ we have $\mathcal{F}(f) \in \mathrm{Hom}_{\mathbf{D}}(\mathcal{F}A, \mathcal{F}B)$ such that the following axioms hold:

(i) if gf is a composition of morphisms in $\mathbf{C}$, then $\mathcal{F}(gf) = \mathcal{F}(g)\mathcal{F}(f)$ in $\mathbf{D}$; and

(ii) $\mathcal{F}(1_A) = 1_{\mathcal{F}A}$.

Now, define $\mathcal{F}$ in the following manner. For an object G in **Nor**–N, with N as a normal subgroup of G by definition of **Nor**–N, let $\mathcal{F}G$ be equal to G/N. Since $N \trianglelefteq G$, we have that G/N is an object in **Grp**. Now, let $f\colon G_1 \to G_2$ be a homomorphism that maps N into N, letting G_1 and G_2 be objects in **Nor**–N. Define

$$\mathcal{F}(f)\colon G_1/N \to G_2/N$$

so that

$$\mathcal{F}(f)(gN) = f(g)N,$$

letting g be an arbitrary element in G_1, so that the coset gN is an arbitrary element in the quotient group G_1/N. We need to show that

$$\mathcal{F}(f)\colon G_1/N \to G_2/N$$

is well-defined in the sense that an expression of the form

$$\mathcal{F}(f)(gN)$$

does not depend on any particular choice of a coset representative for the input coset gN. So, suppose that $gN = g'N$. Equivalently, $(g')^{-1}gN = N$. But recall that $f\colon G_1 \to G_2$ is a homomorphism that maps N into N. We thus have that $f((g')^{-1}gN) \subseteq N$. Since f is a homomorphism, we have that $f(g)N \subseteq f(g')N$. Again since $gN = g'N$, we have that $g^{-1}g'N = N$. So, $f(g^{-1}g')N \subseteq N$, with $f(g')N \subseteq f(g)N$, thus proving that $\mathcal{F}(f)$ is well-defined.

We claim that $\mathcal{F}(f)$ is a group homomorphism. To show this, we begin by letting g and h be elements in G_1. We have that $\mathcal{F}(f)(gNhN) = \mathcal{F}(f)(ghN) = f(gh)N = f(g)f(h)N = f(g)Nf(h)N = \mathcal{F}(f)(gN)\mathcal{F}(f)(hN)$. This proves that that $\mathcal{F}(f) \in \mathrm{Hom}_{\mathbf{Grp}}(\mathcal{F}(G_1), \mathcal{F}(G_2))$. Now suppose that gf is a composition of morphisms f and g in **Nor**–N. Let $f\colon G_1 \to G_2$, and let $g\colon G_2 \to G_3$, with

$$gf\colon G_1 \to G_3.$$

So, we have that

$$\mathcal{F}(gf)\colon G_1/N \to G_3/N$$

is such that

$$\mathcal{F}(gf)(xN) = gf(x)N = g(f(x))N$$

for $x \in G_1$. Similarly, we have that

$$\mathcal{F}(g)\mathcal{F}(f)(xN) = \mathcal{F}(g)f(x)N = g(f(x))N.$$

Letting $1_A\colon A \to A$ denote the identity morphism for an object A in **Nor**–N, we have that

$$\mathcal{F}(1_A)\colon A/N \to A/N$$

is such that

$$\mathcal{F}(1_A)(aN) = 1_A(a)N = aN,$$

as desired.

Exercise 3.5. Let H be a group. Defione a map $\mathcal{H}\times$ from **Grp** to itself on objects and morphisms as follows:

$$\mathcal{H}\times\colon G \to H \times G,$$

and if $\phi\colon G_1 \to G_2$ then $\mathcal{H} \times (\phi)\colon H \times G_1 \to H \times G_2$ by $(h, g) \mapsto (h, \phi(g))$. Prove that $\mathcal{H}\times$ is a functor.

Solution 3.6. Given an input group G in **Grp**, we have that $H \times G$ is in **Grp**, which shows that $\mathcal{H}\times$ is from **Grp** to itself, as indicated above. If $\phi\colon G_1 \to G_2$, then

$$\mathcal{H} \times (\phi)\colon H \times G_1 \to H \times G_2$$

is given by the mapping

$$(h, g) \mapsto (h, \phi(g)),$$

with

$$(h_1, \phi(g_1))(h_2, \phi(g_2)) = (h_1h_2, \phi(g_1)\phi(g_2)) = (h_1h_2, \phi(g_1g_2)),$$

so that

$$\mathcal{H} \times (h_1, g_1)\mathcal{H} \times (h_2, g_2) = \mathcal{H} \times (h_1h_2, g_1g_2).$$

Now suppose that gf is a composition of morphisms in **Grp**. Let $f\colon G_1 \to G_2$ and let $g\colon G_2 \to G_3$, with G_1, G_2, and G_3 as objects in **Grp**. We have that

$$\mathcal{H} \times (gf)\colon H \times G_1 \to H \times G_3$$

with

$$\mathcal{H} \times (gf)(x, y) = (x, g(f(y))).$$

Similarly,

$$\mathcal{H} \times (f)\colon H \times G_1 \to H \times G_2$$

maps (x, y) to $(x, f(y))$, and

$$\mathcal{H} \times (g)\colon H \times G_2 \to H \times G_3$$

maps $(x, f(y))$ to $(x, g(f(y)))$. Also, $\mathcal{H} \times (1_A)$ maps (x, y) to $(x, 1_A(y)) = (x, y)$. We thus have that the functor axioms holds.

Exercise 3.7. Show that the map **Ring** to **Grp** by mapping a ring to its group of units (i.e., $R \mapsto R^{\times}$) defines a functor. Show by explicit examples that this functor is neither faithful nor full.

Solution 3.8. Since the set of all units of a given ring R forms a group with respect to the underlying multiplicative binary operation on R, we have that the mapping $\mathcal{F}$ indicated in the above exercise is a rule of assignment from **Ring** to **Grp**. That is, for every object R in **Ring**, we have that $\mathcal{F}R$ is an object in **Grp**. Now, given an arbitrary ring homomorphism f in $\text{Hom}_{\mathbf{Ring}}(A, B)$, we have that f preserves the multiplicative operations of A and B, with $f(a_1a_2) = f(a_1)f(a_2)$ for elements a_1 and a_2

in A. So, for f in $\operatorname{Hom}_{\mathbf{Ring}}(A,B)$, let $\mathcal{F}f$ denote the mapping from $A^{\times}$ to $B^{\times}$ such that $\mathcal{F}f(a) = f(a)$ for each element a in $A^{\times}$. Now, we must show that this mapping is well-defined in the sense that $\mathcal{F}f(a)$ is actually an element in the given codomain $B^{\times}$, given an input unit $a \in A^{\times}$. Since a is a unit, we have that there exists an element $a' \in A$ such that

$$a \cdot a' = a' \cdot a = 1.$$

By definition of a unit, we have that a' must also be a unit, with $a' \in A^{\times}$. Since f is a morphism, from the equalities

$$f(a \cdot a') = f(a' \cdot a) = f(1),$$

we obtain the equalities whereby

$$f(a) \cdot f(a') = f(a') \cdot f(a) = 1,$$

thus showing that $\mathcal{F}f(a)$ is a unit, as desired.

Since $f \in \operatorname{Hom}_{\mathbf{Ring}}(A,B)$ preserves multiplication, we have that

$$\mathcal{F}f = \operatorname{Hom}_{\mathbf{Grp}}(\mathcal{F}A, \mathcal{F}B) = \operatorname{Hom}_{\mathbf{Grp}}(A^{\times}, B^{\times}),$$

as desired. Now, suppose that gf is a composition of morphisms in **Ring**, letting $f\colon A \to B$ and $g\colon B \to C$. We thus have that $\mathcal{F}(gf)$ maps each element a in $A^{\times}$ to $gf(a) \in C^{\times}$. Also, $\mathcal{F}(g)\mathcal{F}(f)(a)$ is equal to to $\mathcal{F}(g)f(a)$, which, in turn, is also equal to $gf(a) \in C^{\times}$, which shows that the initial functor axiom holds.

Now, consider the identity morphism 1_A on an object A in **Ring**. By definition of $\mathcal{F}$, we have that $\mathcal{F}(1_A)$ maps each element a in $A^{\times}$ to $1_A(a) = a \in A^{\times}$. That is, $\mathcal{F}(1_A) = 1_{A^{\times}}$, which shows that the latter functor axiom holds.

As stated in the class textbook, a functor $\mathcal{G}$ from $\mathbf{C}$ to $\mathbf{D}$ is called *faithful*, respectively *full*, if for every pair of objects A and B in $\mathbf{C}$ the map $\mathcal{G}\colon \operatorname{Hom}(A,B) \to \operatorname{Hom}(\mathcal{G}A, \mathcal{G}B)$ is injective, or surjective respectively.

Let

$$f\colon (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \to (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$$

denote the identity mapping on the ring $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$. Let

$$g\colon (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \to (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$$

denote the mapping whereby $g(a,b) = (b,a)$ for elements a and b in $\mathbb{Z}/2\mathbb{Z}$. It is clear that g is a ring homomorphism, since $g(a_1,b_1) + g(a_2,b_2) = (b_1,a_1) + (b_2,a_2) = (b_1 + b_2, a_1 + a_2) = g(a_1 + a_2, b_1 + b_2) = g\big((a_1,b_1) + (a_2,b_2)\big)$ and since $g(a_1,b_1) \cdot g(a_2,b_2) = (b_1,a_1) \cdot (b_2,a_2) = (b_1 \cdot b_2, a_1 \cdot a_2) = g(a_1 \cdot a_2, b_1 \cdot b_2) = g\big((a_1,b_1) \cdot (a_2,b_2)\big)$ and since $(1,1) \mapsto (1,1)$ under g. Since there is only one unit in $\mathbb{Z}/2\mathbb{Z}$, we have that $\mathcal{F}f$ and $\mathcal{F}g$ are both the identity morphisms on $\{(1,1)\}$. But $f \neq g$, since $f(0,1) = (0,1)$ whereas $g(0,1) = (1,0)$. This shows that the map $\mathcal{F}\colon \operatorname{Hom}((\mathbb{Z}/2\mathbb{Z})\times(\mathbb{Z}/2\mathbb{Z}), (\mathbb{Z}/2\mathbb{Z})\times(\mathbb{Z}/2\mathbb{Z})) \to \operatorname{Hom}(\mathcal{F}((\mathbb{Z}/2\mathbb{Z})\times (\mathbb{Z}/2\mathbb{Z})), \mathcal{F}((\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})))$ is not injective.

Now, consider the set $\operatorname{Hom}(\mathbb{Z}, M_{2\times 2}(\mathbb{C}))$ and the set $\operatorname{Hom}(\mathcal{F}\mathbb{Z}, \mathcal{F}M_{2\times 2}(\mathbb{C}))$. Since $\mathbb{Z}$ is cyclic, and since ring homomorphisms must may unity elements to unity elements, it is clear that there is only one element in $\mathrm{Hom}(\mathbb{Z}, M_{2\times 2}(\mathbb{C}))$, namely, the morphism which maps $z \in \mathbb{Z}$ to zI_2. Again consider the set $\mathrm{Hom}(\mathcal{F}\mathbb{Z}, \mathcal{F}M_{2\times 2}(\mathbb{C}))$, which is also equal to

$$\mathrm{Hom}(\{1, -1\}, \mathrm{GL}_2(\mathbb{C})).$$

But it is clear that there are several different elements in this set. For example, consider the morphism which maps 1 to I_2 and which maps -1 to $\mathrm{diag}(1, -1) \in \mathrm{GL}_2(\mathbb{C})$. This is certainly a group homomorphism, but it is clear that nothing maps to this group homomorphism with respect to $\mathcal{F}$, since there is only one element in $\mathrm{Hom}(\mathbb{Z}, M_{2\times 2}(\mathbb{C}))$

Exercise 3.9. Show that for each $n \geq 1$ the map $\mathcal{GL}_n\colon R \to \mathrm{GL}_n(R)$ defines a functor from **CRing** to **Grp**. [Define $\mathcal{GL}_n$ on morphisms by applying each ring homomorphism to the entries of a matrix.]

Solution 3.10. Let $n \in \mathbb{N}$. For every object R in **CRing**, we have that the general linear group $\mathrm{GL}_n(R)$ is indeed an object in **Grp**. Now, letting A and B be objects in **CRing**, and letting f be in $\mathrm{Hom}_{\mathbf{CRing}}(A, B)$, we have that $\mathcal{GL}_n(f)$ may be defined by applying the ring homomorphism f to the entries of a given matrix. Given matrices

$$\begin{pmatrix} x_{1,1} & x_{1,2} & \cdots & x_{1,n} \\ x_{2,1} & x_{2,2} & \cdots & x_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n,1} & x_{n,2} & \cdots & x_{n,n} \end{pmatrix}, \begin{pmatrix} y_{1,1} & y_{1,2} & \cdots & y_{1,n} \\ y_{2,1} & y_{2,2} & \cdots & y_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ y_{n,1} & y_{n,2} & \cdots & y_{n,n} \end{pmatrix} \in \mathcal{GL}_n(A) = \mathrm{GL}_n(A),$$

we have that:

$$\begin{aligned}
&\mathcal{GL}_n(f)\left(\begin{pmatrix} x_{1,1} & x_{1,2} & \cdots & x_{1,n} \\ x_{2,1} & x_{2,2} & \cdots & x_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n,1} & x_{n,2} & \cdots & x_{n,n} \end{pmatrix} \cdot \begin{pmatrix} y_{1,1} & y_{1,2} & \cdots & y_{1,n} \\ y_{2,1} & y_{2,2} & \cdots & y_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ y_{n,1} & y_{n,2} & \cdots & y_{n,n} \end{pmatrix}\right) \\
&= \mathcal{GL}_n(f)\begin{pmatrix} \sum_{k=1}^n x_{1,k}y_{k,1} & \sum_{k=1}^n x_{1,k}y_{k,2} & \cdots & \sum_{k=1}^n x_{1,k}y_{k,n} \\ \sum_{k=1}^n x_{2,k}y_{k,1} & \sum_{k=1}^n x_{2,k}y_{k,2} & \cdots & \sum_{k=1}^n x_{2,k}y_{k,n} \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{k=1}^n x_{n,k}y_{k,1} & \sum_{k=1}^n x_{n,k}y_{k,2} & \cdots & \sum_{k=1}^n x_{n,k}y_{k,n} \end{pmatrix} \\
&= \begin{pmatrix} f\left(\sum_{k=1}^n x_{1,k}y_{k,1}\right) & f\left(\sum_{k=1}^n x_{1,k}y_{k,2}\right) & \cdots & f\left(\sum_{k=1}^n x_{1,k}y_{k,n}\right) \\ f\left(\sum_{k=1}^n x_{2,k}y_{k,1}\right) & f\left(\sum_{k=1}^n x_{2,k}y_{k,2}\right) & \cdots & f\left(\sum_{k=1}^n x_{2,k}y_{k,n}\right) \\ \vdots & \vdots & \ddots & \vdots \\ f\left(\sum_{k=1}^n x_{n,k}y_{k,1}\right) & f\left(\sum_{k=1}^n x_{n,k}y_{k,2}\right) & \cdots & f\left(\sum_{k=1}^n x_{n,k}y_{k,n}\right) \end{pmatrix} \\
&= \begin{pmatrix} \sum_{k=1}^n f\left(x_{1,k}y_{k,1}\right) & \sum_{k=1}^n f\left(x_{1,k}y_{k,2}\right) & \cdots & \sum_{k=1}^n f\left(x_{1,k}y_{k,n}\right) \\ \sum_{k=1}^n f\left(x_{2,k}y_{k,1}\right) & \sum_{k=1}^n f\left(x_{2,k}y_{k,2}\right) & \cdots & \sum_{k=1}^n f\left(x_{2,k}y_{k,n}\right) \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{k=1}^n f\left(x_{n,k}y_{k,1}\right) & \sum_{k=1}^n f\left(x_{n,k}y_{k,2}\right) & \cdots & \sum_{k=1}^n f\left(x_{n,k}y_{k,n}\right) \end{pmatrix} \\
&= \begin{pmatrix} \sum_{k=1}^n f\left(x_{1,k}\right)f\left(y_{k,1}\right) & \sum_{k=1}^n f\left(x_{1,k}\right)f\left(y_{k,2}\right) & \cdots & \sum_{k=1}^n f\left(x_{1,k}\right)f\left(y_{k,n}\right) \\ \sum_{k=1}^n f\left(x_{2,k}\right)f\left(y_{k,1}\right) & \sum_{k=1}^n f\left(x_{2,k}\right)f\left(y_{k,2}\right) & \cdots & \sum_{k=1}^n f\left(x_{2,k}\right)f\left(y_{k,n}\right) \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{k=1}^n f\left(x_{n,k}\right)f\left(y_{k,1}\right) & \sum_{k=1}^n f\left(x_{n,k}\right)f\left(y_{k,2}\right) & \cdots & \sum_{k=1}^n f\left(x_{n,k}\right)f\left(y_{k,n}\right) \end{pmatrix} \\
&= \begin{pmatrix} f\left(x_{1,1}\right) & f\left(x_{1,2}\right) & \cdots & f\left(x_{1,n}\right) \\ f\left(x_{2,1}\right) & f\left(x_{2,2}\right) & \cdots & f\left(x_{2,n}\right) \\ \vdots & \vdots & \ddots & \vdots \\ f\left(x_{n,1}\right) & f\left(x_{n,2}\right) & \cdots & f\left(x_{n,n}\right) \end{pmatrix} \cdot \begin{pmatrix} f\left(y_{1,1}\right) & f\left(y_{1,2}\right) & \cdots & f\left(y_{1,n}\right) \\ f\left(y_{2,1}\right) & f\left(y_{2,2}\right) & \cdots & f\left(y_{2,n}\right) \\ \vdots & \vdots & \ddots & \vdots \\ f\left(y_{n,1}\right) & f\left(y_{n,2}\right) & \cdots & f\left(y_{n,n}\right) \end{pmatrix}
\end{aligned}$$

$$= \mathcal{GL}_n(f)\begin{pmatrix} x_{1,1} & x_{1,2} & \cdots & x_{1,n} \\ x_{2,1} & x_{2,2} & \cdots & x_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n,1} & x_{n,2} & \cdots & x_{n,n} \end{pmatrix} \cdot \mathcal{GL}_n(f)\begin{pmatrix} y_{1,1} & y_{1,2} & \cdots & y_{1,n} \\ y_{2,1} & y_{2,2} & \cdots & y_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ y_{n,1} & y_{n,2} & \cdots & y_{n,n} \end{pmatrix}.$$

This shows that $\mathcal{GL}_n(f)$ is in $\mathrm{Hom}_{\mathbf{Grp}}(\mathcal{GL}_nA, \mathcal{GL}_nB)$. Now, suppose that gf is a composition of morphisms in **CRing**. Let $f: A \to B$ and let $g: B \to C$. Since gf is a ring homomorphism from A to C, we have that $\mathcal{GL}_n(gf)$ is a group homomorphism from $\mathrm{GL}_n(A)$ to $\mathrm{GL}_n(C)$. Given an input matrix

$$\begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \end{pmatrix} \in \mathrm{GL}_n(A),$$

we have that:

$$\mathcal{GL}_n(gf)\begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \end{pmatrix} = \begin{pmatrix} gf(a_{1,1}) & gf(a_{1,2}) & \cdots & gf(a_{1,n}) \\ gf(a_{2,1}) & gf(a_{2,2}) & \cdots & gf(a_{2,n}) \\ \vdots & \vdots & \ddots & \vdots \\ gf(a_{n,1}) & gf(a_{n,2}) & \cdots & gf(a_{n,n}) \end{pmatrix}.$$

Similarly, we have that

$$\mathcal{GL}_n(f)\begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \end{pmatrix} = \begin{pmatrix} f(a_{1,1}) & f(a_{1,2}) & \cdots & f(a_{1,n}) \\ f(a_{2,1}) & f(a_{2,2}) & \cdots & f(a_{2,n}) \\ \vdots & \vdots & \ddots & \vdots \\ f(a_{n,1}) & f(a_{n,2}) & \cdots & f(a_{n,n}) \end{pmatrix},$$

so that

$$\mathcal{GL}_n(g)\mathcal{GL}_n(f)\begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \end{pmatrix} = \begin{pmatrix} gf(a_{1,1}) & gf(a_{1,2}) & \cdots & gf(a_{1,n}) \\ gf(a_{2,1}) & gf(a_{2,2}) & \cdots & gf(a_{2,n}) \\ \vdots & \vdots & \ddots & \vdots \\ gf(a_{n,1}) & gf(a_{n,2}) & \cdots & gf(a_{n,n}) \end{pmatrix}.$$

We thus have that

$$\mathcal{GL}_n(gf) = \mathcal{GL}_n(g)\mathcal{GL}_n(f),$$

as desired. Now, letting A be an object in **Ring**, consider the identity mapping 1_A on A. It is clear that $\mathcal{GL}_n(1_A)$ maps each matrix in $\mathrm{GL}_n(A)$ to itself, so that $\mathcal{GL}_n(1_A) = I_n$, as desired.

Exercise 3.11. Supply the details that show the double dual map satisfies the axioms of a functor.

Solution 3.12. The double dual map is described as follows in the class textbook. Let K be a field and let K–**fdVec** be the category of all finite dimensional vector spaces over K. The double dual functor $\mathcal{D}^2$ is defined from K–**fdVec** to itself. Recall that the dual space V^* of V is defined as $V^* = \mathrm{Hom}_K(V, K)$. Then $\mathcal{D}^2$ is defined on objects by mapping a vector space V to V^{**}. If $\phi: V \to W$ is a linear transformation of objects in K–**fdVec**, define

$$\mathcal{D}^2(\phi): V^{**} \to W^{**}$$

so that

$$\mathcal{D}^2(\phi)(E_v) = E_{\phi(v)},$$

where E_v denotes "evaluation at v" for $v \in V$. We proceed to check that the two functor axioms hold. Suppose that gf is a composition of morphisms in K–**fdVec**. Let $f: A \to B$ and let $g: B \to C$. For an "evaluation at A" object E_a in A^{**}, we have that $\mathcal{D}^2(f)(E_a) = E_{f(a)}$. Similarly, we have that

$$\mathcal{D}^2(g)\mathcal{D}^2(f)(E_a) = \mathcal{D}^2(g)E_{f(a)} = E_{gf(a)} = \mathcal{D}^2(gf)(E_a),$$

thus proving that the initial functor axiom holds. Letting A be an object in K–**fdVec**, letting 1_A denote the identity mapping on A, and letting E_a be as given above, we have that

$$\mathcal{D}^2(1_A)(E_a) = E_{1_A(a)} = E_a,$$

which shows that

$$\mathcal{D}^2(1_A) = 1_{\mathcal{D}^2 A},$$

we desired.

Exercise 3.13. Let **Nor**–N be the category described above, and let $\mathcal{F}$ be the inclusion functor from **Nor**–N into **Grp**. Describe a functor $\mathcal{G}$ from **Nor**–N into **Grp** such that the transformation η defined by $\eta_G: G \to G/N$ is a natural transformation from $\mathcal{F}$ to $\mathcal{G}$.

Solution 3.14. Letting N be a group, we have that **Nor**–N is the collection of all groups that contain N as a normal subgroup, such that a morphism between objects A and B with respect to **Nor**–N is any group homomorphism that maps N into N. We have previously shown that **Nor**–N is a category. From the above definition for η_G, we have that $\mathcal{G}$ should be defined so that for an object M in **Nor**–N, $\mathcal{G}(M) = M/N$. Furthermore, given a morphism f from M_1 to M_2, letting M_1 and M_2 be objects in **Nor**–N, define

$$\mathcal{G}(f): M_1/N \to M_2/N$$

so that for $m \in M_1$, with $mN \in M_1/N$, we have that $\mathcal{G}(f)(mN) = f(m)N$. We have that

$$\mathcal{G}(f)\eta_{M_1} = \eta_{M_2}\mathcal{F}(f),$$

because if we let m be an object in $\mathcal{F}M_1 = M_1$, we have that

$$\eta_{M_2}\mathcal{F}(f)m = \eta_{M_2}f(m) = f(m)N$$

and

$$\mathcal{G}(f)\eta_{M_1}m = \mathcal{G}(f)mN = f(m)N.$$

We observe that $\mathcal{G}(f)$ is indeed a morphism of groups, given that f is a morphism: letting m and m' be elements in M_1, so that mN and $m'N$ are elements in the quotient group M_1/N, we have that:

$$\begin{aligned}\mathcal{G}(f)((mN)(m'N)) &= \mathcal{G}(f)(mm'N)\\ &= f(mm')N\\ &= f(m)f(m')N\\ &= f(m)Nf(m')N\\ &= \mathcal{G}(f)(mN)\mathcal{G}(f)(m'N).\end{aligned}$$

We should also show that $\mathcal{G}(f)$ is well-defined in the sense that an expression of the form $\mathcal{G}(f)(mN)$ does not depend on any particular choice of the coset representative m. So, suppose that $mN = m'N$.

We thus have that $\mathcal{G}(f)(mN) = f(m)N$ and $\mathcal{G}(f)(m'N) = f(m')N$. Since $mN = m'N$, we have that there exists an element $n \in N$ such that $mn = m'$. So, we have that

$$\mathcal{G}(f)(m'N) = f(m')N = f(mn)N = f(m)f(n)N.$$

But recall that the category **Nor**–N was constructed so that morphisms with respect to **Nor**–N must map N into N. So, we have that $f(n) = n'$, for some element $n' \in N$. We thus have that

$$\mathcal{G}(f)(m'N) = f(m')N = f(mn)N = f(m)f(n)N = f(m)n'N = f(m)N = \mathcal{G}(f)(mN),$$

as desired.

3.2 Exercises from Section 10.1

In the following exercises R is a ring with 1 and M is a left R-module.

Exercise 3.15. Prove that $0m = 0$ and $(-1)m = -m$ for all $m \in M$.

Solution 3.16. Observe that:

$$0m + 0m = (0 + 0)m = 0m.$$

Since

$$0m + 0m = 0m,$$

and since M is an abelian group, by adding the additive inverse of $0m$ to both sides of the above equation, we have that $0m$ must be equal to the additive identity element in the underlying abelian group of M, i.e., $0m = 0$.

Now, recall that 1 denotes the underlying unity of the ring R. Similarly, -1 denotes the unique additive inverse of $1 \in R$, with respect to the underlying group structure on R. Again letting $m \in M$ be arbitrary, we have that:

$$1m + (-1)m = (1 + (-1))m = 0m.$$

So, from the previous component of our solution, we find that:

$$1m + (-1)m = 0.$$

Now, recall that

$$1m = m,$$

by definition of a unital module. We thus have that:

$$m + (-1)m = 0.$$

But since M forms an additive abelian group, we have that $(-1)m$ and m are additive inverses of one another: that is: $(-1)m$ is precisely the unique additive inverse $-m$ of $m \in M$, as desired.

Exercise 3.17. Prove that $R^\times$ and M satisfy the two axioms for a group action of the multiplicative group $R^\times$ on the set M.

Solution 3.18. We have that $(rs)m = r(sm)$ for $r, s \in R^\times$ by definition of a module, letting $m \in M$ and we have that $1m = m$, again by definition of a module.

Exercise 3.19. Assume that $rm = 0$ for some $r \in R$ and some $m \in M$ with $m \neq 0$. Prove that r does not have a left inverse (i.e., there is no $s \in R$ such that $sr = 1$).

Solution 3.20. As above, we assume that $rm = 0$, with $r \in R$, and $m \in M$ such that $m \neq 0$. By way of contradiction, suppose that there exists an element s in R such that $sr = 1$. From the equality

$$rm = 0,$$

we have that

$$s(rm) = s \cdot 0 = 0,$$

and we thus obtain the equality whereby

$$(sr)m = 0.$$

Since $sr = 1$, we have that

$$1m = 0.$$

By definition of a module, we have that $1m = m$. So, the equality $1m = 0$ implies that $m = 0$, thus contradicting that m is nonzero.

Exercise 3.21. Let M be the module R^n and let $I_1, I_3, \ldots, I_n$ be left ideals of R. Prove ithat the following are submodules of M:

(a) $\{(x_1, x_2, \ldots, x_n) \mid x_i \in I_i\}$

(b) $\{(x_1, x_2, \ldots, x_n) \mid x_i \in R \text{ and } x_1 + x_2 + \cdots + x_n = 0\}$.

Solution 3.22. As we later discuss, the submodule criterion basically states that a subset N of an R-module M is a submodule of M iff N is nonempty and $x + ry \in N$ for $r \in R$ and $x, y \in N$. Since ideals are nonempty, it is clear that $\{(x_1, x_2, \ldots, x_n) \mid x_i \in I_i\}$ is nonempty. Let r be an element in R. Let $(y_1, y_2, \ldots, y_n)$ and $(z_1, z_2, \ldots, z_n)$ be elements in $\{(x_1, x_2, \ldots, x_n) \mid x_i \in I_i\}$, with $y_i \in I_i$ and $z_i \in I_i$ for all indices i. Now consider the expression $r(z_1, z_2, \ldots, z_n)$. Since

$$r(z_1, z_2, \ldots, z_n) = (r \cdot z_1, r \cdot z_2, \ldots, r \cdot z_n)$$

and since ideals of the form I_i are informally "closed under multiplication" by elements in R, we thus have that $r \cdot z_i \in I_i$ for each index i. Since $y_i \in I_i$ for all indices i, and since $r \cdot z_i \in I_i$ for all i, we thus have that $y_i + r \cdot z_i \in I_i$ for all i, as desired.

Now, consider the family

$$F = \{(x_1, x_2, \ldots, x_n) \mid x_i \in R \text{ and } x_1 + x_2 + \cdots + x_n = 0\}.$$

Since the ordered n-tuple consisting of 0-entries is in this family, we find that F is nonempty. Let $(y_1, y_2, \ldots, y_n)$ and $(z_1, z_2, \ldots, z_n)$ be elements in this family, and let r be an element in R. Since $(z_1, z_2, \ldots, z_n)$ is in F, we have that $z_1 + z_2 + \cdots + z_n = 0$. By the distributivity axiom, we have that $r \cdot z_1 + r \cdot z_2 + \cdots + r \cdot z_n = r \cdot 0 = 0$. So, we have that $(r \cdot z_1, r \cdot z_2, \ldots, r \cdot z_n)$ is in F. Since

$$y_1 + y_2 + \cdots + y_n = 0,$$

and since

$$r \cdot z_1 + r \cdot z_2 + \cdots + r \cdot z_n = 0$$

we have that

$$(y_1 + r \cdot z_1) + (y_2 + r \cdot z_2) + \cdots + (y_n + r \cdot z_n) = 0,$$

which shows that the ordered n-tuple

$$(y_1 + r \cdot z_1, y_2 + r \cdot z_2, \dots, y_n + r \cdot z_n)$$

is in F, thus proving that F is a submodule, as desired.

Exercise 3.23. For any left ideal I of R define

$$IM = \{ \sum_{\text{finite}} a_i m_i \mid a_i \in I, m_i \in M\}$$

to be the collection of all finite sums of elements of the form am where $a \in I$ and $m \in M$. Prove that IM is a submodule of M.

Solution 3.24. Recall that the submodule criterion basically states that a subset N of an R-module M is a submodule of M iff N is nonempty and $x + ry \in N$ for $r \in R$ and $x, y \in N$. So, let I be a left ideal of R, and let IM be as given above. Letting $a_i \in I$ and $m_i \in M$, let $\sum_{\text{finite}} a_i m_i$ be an element in IM. Similarly, letting $b_i \in I$ and $n_i \in M$, let $\sum_{\text{finite}} b_i n_i$ be in IM. Also, let r be an element in R. Since

$$r \cdot \sum_{\text{finite}} b_i n_i = \sum_{\text{finite}} r \cdot (b_i n_i) = \sum_{\text{finite}} (rb_i) n_i,$$

and since b_i is in the ideal I for all indices i, we have that $rb_i \in I$ for all $i \in I$. Since $\sum_{\text{finite}} (rb_i) n_i$ is a finite sum of expressions of the form $(rb_i)n_i$ for $rb_i \in I$ and $n_i \in M$, we have that $r \cdot \sum_{\text{finite}} b_i n_i$ is in IM. But since

$$\sum_{\text{finite}} a_i m_i + \sum_{\text{finite}} (rb_i) n_i$$

is a finite sum of expressions of the form $\iota\mu$ for $\iota \in I$ and $\mu \in M$, we have that

$$\sum_{\text{finite}} a_i m_i + \sum_{\text{finite}} (rb_i) n_i$$

must be in IM. By the submodule criterion, we have that IM is a submodule of M.

Exercise 3.25. Show that the intersection of any nonempty collection of submodules of an R-module is a submodule.

Solution 3.26. Let M be an R-module. Let $I \neq \varnothing$ be an index set, and let S_i be a submodule of M for each index i in I. Now, consider the following expression:

$$\bigcap_{i \in I} S_i.$$

Now, let r be an element in R, and let s and t be elements in $\bigcap_{i \in I} S_i$. Consider the expression rt. Since t is in S_i for $i \in I$, we have that rt is in S_i for $i \in I$, since S_i is closed under scalar multiplication for all indices i. Since $s \in S_i$ for all i, and since rt is in S_i for $i \in I$, we thus find that $s + rt \in S_i$ for all i, since each expression of the form S_i is closed under addition. Since $s + rt \in S_i$ for all i, by the submodule criterion, we have that $\bigcap_{i \in I} S_i$ is a submodule of M, as desired.

Exercise 3.27. Let $N_1 \subseteq N_2 \subseteq$ be an ascending chain of submodules of M. Prove that $\bigcup_{i=1}^{\infty} N_i$ is a submodule of M.

Solution 3.28. Let x and y be elements in $\bigcup_{i=1}^{\infty} N_i$, and let r be an element in R. Let j_1 and j_2 be indices such that $x \in N_{j_1}$ and $y \in N_{j_2}$. We may assume without loss of generality that $N_{j_1} \subseteq N_{j_2}$. Since N_{j_2} is a submodule of M, we have that N_{j_2} is closed under scalar multiplication, so that $ry \in N_{j_2}$. Since $x \in N_{j_1} \subseteq N_{j_2}$, and since N_{j_2} is closed under addition, we thus have that $x + ry \in N_{j_2}$, as desired.

Exercise 3.29. An element m of the R-module M is called a *torsion element* if $rm = 0$ for some nonzero element $r \in R$. The set of torsion elements is denoted

$$\mathrm{Tor}(M) = \{m \in M \mid rm = 0 \text{ for some nonzero } r \in R\}.$$

Prove that if R is an integral domain then $\mathrm{Tor}(M)$ is a submodule of M (called the *torsion* submodule of M).

Solution 3.30. Suppose that R is an integral domain. By definition of an integral domain, we find that R has to be a commutative ring with unity and no zero divisors. Let r be an element in R, and let x and y be elements in $\mathrm{Tor}(M)$. Since $y \in \mathrm{Tor}(M)$, we have that there exists a nonzero scalar s_2 in R such that $s_2 y = 0$. Similarly, we have that there exists a nonzero scalar $s_1 \in R$ such that $s_1 x$ vanishes. Since R is an integral domain, and since s_1 and s_2 are both nonzero, we find that the product $s_1 s_2$ must be nonzero. Now, consider the expression $x + ry$. By the distributivity axiom, we have that

$$s_1 s_2 (x + ry) = (s_1 s_2)x + (s_1 s_2)ry$$

and since R, as an integral domain, is a commutative ring, we have that

$$s_1 s_2 (x + ry) = (s_2 s_1)x + (s_1 r s_2)y.$$

Since M is an R-module, we have that

$$s_1 s_2 (x + ry) = s_2 (s_1 x) + s_1 r (s_2 y).$$

Therefore,

$$s_1 s_2 (x + ry) = s_2 \cdot 0 + s_1 r \cdot 0,$$

which shows that

$$s_1 s_2 (x + ry) = 0,$$

with $s_1 s_2 \neq 0$. So, by the submodule criterion, we have that $\mathrm{Tor}(M)$ forms a submodule.

Exercise 3.31. Give an example of a ring R and an R-module M such that $\mathrm{Tor}(M)$ is not a submodule. [Consider the torsion elements in the R-module R.]

Solution 3.32. We have previously shown that if R is an integral domain then $\mathrm{Tor}(M)$ is a submodule of M. We begin by letting R denote the ring $\mathbb{Z}/15\mathbb{Z}$. We have that R is not an integral domain, since, for example, the product $3 \cdot 5$ vanishes with respect to the ring $\mathbb{Z}/15\mathbb{Z}$. Now, letting M be equal to $\mathbb{Z}/15\mathbb{Z}$, let the ring $\mathbb{Z}/15\mathbb{Z}$ be considered as an R-module over itself. In this case, we have that $\mathrm{Tor}(M)$ is equal to $\{0, 3, 5, 6, 9, 10, 12\}$. But this is clearly not a submodule, because it is not closed under addition, since, for example, 3 and 5 are in $\mathrm{Tor}(M)$, but 8 is not in $\mathrm{Tor}(M)$, since the integer tuple

$$((8 \cdot i) \pmod{15} : i = 1, 2, \ldots, 14)$$

is equal to

$$(8, 1, 9, 2, 10, 3, 11, 4, 12, 5, 13, 6, 14, 7).$$

3.3 Exercises from Section 10.2

Throughout the following exercises, R denotes a ring with 1 and M is a left R-module.

Exercise 3.33. Use the submodule criterion to show that kernels and images of R-module homomorphisms are submodules.

Solution 3.34. The submodule criterion may be formulated in the following manner: Letting R be a ring and letting M be an R-module, a subset N of M is a submodule of M iff N is nonempty and $x + ry \in N$ for $r \in R$ and $x, y \in N$.

So, let M and N be modules, and let $\phi: M \to N$ be an R-module homomorphism. Since ϕ maps the additive identity element in M to the additive identity element in N, we have that the kernel of ϕ is nonempty. Let $r \in R$, and let x and y be elements in $\ker(\phi)$. Since ϕ is a morphism, we have that $\phi(x + ry) = \phi(x) + \phi(ry) = 0 + \phi(ry) = \phi(ry) = r\phi(y) = r0 = 0$, as desired.

Let M, N and ϕ be as given above. let x and y be elements in the image of ϕ. Let a and b be elements in the domain of ϕ such that $\phi(a) = x$ and $\phi(b) = y$. Since ϕ is a morphism, we have that $x + ry = \phi(a) + r\phi(b) = \phi(a) + \phi(rb) = \phi(a + rb)$. This shows that $x + ry$ must be in the image of ϕ.

Exercise 3.35. Show that the relation "is R-module isomorphic to" is an equivalence relation on any set of R-modules.

Solution 3.36. Let $\cong$ denote the binary relation given above. Let S be a set of R-modules. Given an element M in S, the identity mapping on M is an R-module isomorphism, so that $M \cong M$, thus proving the reflexivity of M. Given elements M_1 and M_2 in S, and given an isomorphism ϕ from M_1 to M_2, we have that ϕ is bijective, and that ϕ^{-1} is also an isomorphism, as may be verified, thus establishing the symmetry of $\cong$. Finally, given elements M_1, M_2, and M_3 in S, if $M_1 \cong M_2$ and $M_2 \cong M_3$, letting $\phi: M_1 \to M_2$ and letting $\psi: M_2 \to M_3$, then the composition $\psi \circ \phi$ is also an isomorphism from M_1 to M_3, as may be verified, thus proving the transitivity of $\cong$.

Exercise 3.37. Give an explicit example of a map from one R-module to another which is a group homomorphism but not an R-module homomorphism.

Solution 3.38. Consider the polynomial ring $\mathbb{Q}[x]$. Letting

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Q}[x],$$

we define

$$\phi: \mathbb{Q}[x] \to \mathbb{Q}[x]$$

so that

$$\phi(a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0) = a_n x^{n+1} + a_n x^{n-1} + \cdots + a_1 x^2 + a_0.$$

Note that $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ and $\phi(a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0)$ have the same constant term. We claim that ϕ preserves addition. To show this, let

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Q}[x],$$

and let

$$q(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0 \in \mathbb{Q}[x],$$

with $m \geq n$. If $m = n$, then ϕ evaluated at the sum of the above polynomials is equal to:

$$(a_n + b_n)x^{n+1} + (a_{n-1} + b_{n-1})x^n + \cdots + (a_1 + b_1)x^2 + a_0 + b_0.$$

Since

$$\phi(a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0)$$

is equal to $a_n x^{n+1} + a_{n-1}x^n + \cdots + a_1 x^2 + a_0$, and since

$$\phi(b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0)$$

is equal to $b_n x^{n+1} + b_{n-1}x^n + \cdots + b_1 x^2 + b_0$, we find that ϕ preserves addition for equal-degree polynomials. If $m > n$, then ϕ evaluated at $p(x) + q(x)$ is equal to:

$$b_m x^{m+1} + \cdots + b_{n+1}x^{n+2} + (a_n + b_n)x^{n+1} + \cdots + (a_1 + b_1)x^2 + a_0 + b_0.$$

In this case, since

$$\phi(p(x)) = a_n x^{n+1} + a_{n-1}x^n + \cdots + a_1 x^2 + a_0$$

and since

$$\phi(q(x)) = b_m x^{m+1} + \cdots + b_{n+1}x^{n+2} + b_n x^{n+1} + \cdots + b_1 x^2 + b_0,$$

we have that ϕ preserves addition in general. Also observe that $\phi(0) = 0$. Letting the unital ring $\mathbb{Q}[x]$ be regarded as a $\mathbb{Q}[x]$-module over itself, we thus have that the mapping

$$\phi : \mathbb{Q}[x] \to \mathbb{Q}[x]$$

given above is a map from one $\mathbb{Q}[x]$-module to another which is a group homomorphism. However, since $x\phi(1) = x \cdot 1 = x$, and since $\phi(x) = x^2$, we have that ϕ does not preserve scalar multiplication. So, we have given an explicit example oif a map from one $\mathbb{Q}[x]$-module to another which is a group homomorphism but not an $\mathbb{Q}[x]$-module homomorphism.

Exercise 3.39. Let A be any $\mathbb{Z}$-module, let a be any element of A and let n be a positive integer. Prove that the map $\phi_a : \mathbb{Z}/n\mathbb{Z} \to A$ given by $\phi_a(\overline{k}) = ka$ is a well-defined $\mathbb{Z}$-module homomorphism if and only if $na = 0$. Prove that $\text{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A) \cong A_n$, where $A_n = \{a \in A \mid na = 0\}$, so that A_n is the annihilator in A of the ideal (n) of $\mathbb{Z}$.

Solution 3.40. We begin by proving the following proposition, letting A, a, and n be as given above.

Proposition 3.41. *The map $\phi_a : \mathbb{Z}/n\mathbb{Z} \to A$ given by $\phi_a(\overline{k}) = ka$ is a well-defined $\mathbb{Z}$-module homomorphism if and only if $na = 0$.*

Proof. ($\Longrightarrow$) First, suppose that the map $\phi_a : \mathbb{Z}/n\mathbb{Z} \to A$ given by $\phi_a(\overline{k}) = ka$ is a well-defined $\mathbb{Z}$-module homomorphism. Consider the expression $\phi_a(\overline{n})$. Since ϕ_a is well-defined map, we have that $\phi_a(\overline{n}) = na$. Similarly, we have that $\phi_a(\overline{0}) = 0 \cdot a = 0$. But since $\overline{0} = \overline{n}$, and since ϕ_a is well-defined, we have that $\phi_a(\overline{n}) = na = \phi_a(\overline{0}) = 0 \cdot a = 0$, as desired.

($\Longleftarrow$) Conversely, suppose that $na = 0$. Now let $\overline{k_1}$ and $\overline{k_2}$ be elements in the given domain of ϕ_a, so that the representative elements k_1 and k_2 are not necessarily equal. Suppose that $\overline{k_1} = \overline{k_2}$. Since $\overline{k_1}$ and $\overline{k_2}$ are equal in $\mathbb{Z}/n\mathbb{Z}$, we have that:

$$k_1 \equiv k_2 (\text{mod } n).$$

Equivalently, n divides $k_1 - k_2$. So, we have that there exists an element z in $\mathbb{Z}$ such that $k_1 = zn + k_2$. Now, consider the expressions $\phi_a(\overline{k_1}) = k_1 a$ and $\phi_a(\overline{k_2}) = k_2 a$. From the equality

$$k_1 a = (zn + k_2)a$$

we have that

$$k_1 a = (zn)a + k_2 a.$$

Equivalently,

$$k_1 a = z(na) + k_2 a.$$

From our initial assumption whereby $na = 0$, we find that

$$k_1 a = k_2 a,$$

thus proving that ϕ_a is well-defined. We proceed to prove that ϕ_a is a $\mathbb{Z}$-module homomorphism. Let $\overline{\ell_1}$ and $\overline{\ell_2}$ be elements in $\mathbb{Z}/n\mathbb{Z}$. Let $\ell_1 = y_1 n + \overline{\ell_1}$ and let $\ell_2 = y_2 n + \overline{\ell_2}$. Since

$$\ell_1 + \ell_2 = (y_1 + y_2)n + \overline{\ell_1} + \overline{\ell_2},$$

we have that

$$\overline{\ell_1 + \ell_2} = \overline{\ell_1} + \overline{\ell_2}.$$

We may thus show that ϕ_a preserves addition:

$$\begin{aligned}
\phi_a(\overline{\ell_1} + \overline{\ell_2}) &= \phi_a(\overline{\ell_1 + \ell_2}) \\
&= (\ell_1 + \ell_2)a \\
&= \ell_1 a + \ell_2 a \\
&= \phi_a(\overline{\ell_1}) + \phi_a(\overline{\ell_2}).
\end{aligned}$$

Letting ℓ_1 be as given above, let s denote a scalar in $\mathbb{Z}$. Recall that $\ell_1 = y_1 n + \overline{\ell_1}$. Since $s\ell_1 = sy_1 n + s\overline{\ell_1}$, we have that $\overline{s\ell_1} = s\overline{\ell_1}$. We can use this equality to show that ϕ_a preserves scalar multiplication:

$$\begin{aligned}
\phi_a(s\overline{\ell_1}) &= \phi_a(\overline{s\ell_1}) \\
&= (s\ell_1)a \\
&= s(\ell_1 a) \\
&= s\phi_a(\overline{\ell_1}).
\end{aligned}$$

Since ϕ_a preserves addition and scalar multiplication, we have that ϕ_a is module homomorphism, as desired. □

We proceed to prove the isomorphic equivalence whereby $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A) \cong A_n$. Let $\psi\colon \mathbb{Z}/n\mathbb{Z} \to A$ be a $\mathbb{Z}$-module homomorphism. Consider the expression $\psi(\overline{1}) \in A$. We define the function

$$f\colon \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A) \to A_n$$

so that

$$f(\psi) = \psi(\overline{1}).$$

We proceed to show that f is well defined in the sense that $f(\psi)$ is an element in the given codomain of f for each element ψ in the domain of f. Since ψ is a mapping from $\mathbb{Z}/n\mathbb{Z}$ to A, we have that $\psi(\overline{1})$ is in A. Furthermore, since

$$n\psi(\overline{1}) = \psi(n\overline{1}) = \psi(\overline{n}) = \psi(\overline{0}),$$

and since ψ is a morphism, we have that $n\psi(\overline{1})$ vanishes, as desired. Now, suppose that $\psi = \psi'$, letting ψ and ψ' be elements in the domain of f. Then $f(\psi) = \psi(\overline{1}) = \psi'(\overline{1}) = f(\psi')$, as desired. So, we have shown that f is well-defined. Again letting ψ and ψ' be elements in $\mathrm{dom}(f)$, suppose that $f(\psi) = f(\psi')$. Then $\psi(\overline{1}) = \psi'(\overline{1})$. But then

$$s\psi(\overline{1}) = s\psi'(\overline{1})$$

for each scalar s, so that

$$\psi(s\overline{1}) = \psi'(s\overline{1})$$

for an arbitrary scalar s, with

$$\psi(\overline{s}) = \psi'(\overline{s})$$

for each element $\overline{s}$ in $\mathbb{Z}/n\mathbb{Z}$. We thus have that

$$f(\psi) = f(\psi') \Longrightarrow \psi = \psi',$$

thus proving the injectivity of f. Now, let $a \in A$ be such that $na = 0$. From Proposition 3.41, we have that the map $\phi_a\colon \mathbb{Z}/n\mathbb{Z} \to A$ whereby $\phi_a(\overline{k}) = ka$ is a well-defined $\mathbb{Z}$-module homomorphism, since $na = 0$. Since $\phi_a(\overline{1}) = 1a = a$, we have that $f(\phi_a) = a$, the proving the surjectivity of f. So, we have thus far shown that f is a well-defined bijective mapping. So, it remains to prove that f is a module morphism. Letting ψ and ψ' be elements in the domain of f, we have that:

$$\begin{aligned} f(\psi + \psi') &= (\psi + \psi')(\overline{1}) \\ &= \psi(\overline{1}) + \psi'(\overline{1}) \\ &= f(\psi) + f(\psi'). \end{aligned}$$

Similarly, for a scalar s, we have that:

$$\begin{aligned} f(s\psi) &= (s\psi)(\overline{1}) \\ &= s\psi(\overline{1}) \\ &= s \cdot f(\psi). \end{aligned}$$

So, we have that $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A) \cong A_n$, as desired.

Exercise 3.42. Exhibit all $\mathbb{Z}$-module homomorphisms from $\mathbb{Z}/30\mathbb{Z}$ to $\mathbb{Z}/21\mathbb{Z}$.

Solution 3.43. A $\mathbb{Z}$-module morphism $\phi\colon \mathbb{Z}/30\mathbb{Z} \to \mathbb{Z}/21\mathbb{Z}$ is unique determined by the value of $\phi(1)$.

So, suppose that $\phi(1) = n$. We thus have that $\phi(k) = kn$, modulo 21, for each scalar k. In particular, we have that $\phi(21) = 0$, so that $\phi(29) = 8n$, and $\phi(0) = 9n$. But since ϕ is a morphism, we have that $9n = 0$, modulo 21. This implies that n must be a multiple of 7. We thus find that $\phi(1)$ must be in $\{0, 7, 14, 21, 28\}$. So, we find that there are a total of five $\mathbb{Z}$-module homomorphisms from $\mathbb{Z}/30\mathbb{Z}$ to $\mathbb{Z}/21\mathbb{Z}$, as determined by the above condition whereby $\phi(1)$ must be in $\{0, 7, 14, 21, 28\}$.

Exercise 3.44. Prove that $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/(n, m)\mathbb{Z}$.

Solution 3.45. To prove the isomorphic equivalence whereby:

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/(n,m)\mathbb{Z},$$

our strategy is to construct an explicit isomorphism from $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$ to $\mathbb{Z}/(n,m)\mathbb{Z}$. Now, let ϕ be a $\mathbb{Z}$-module homomorphism from $\mathbb{Z}/n\mathbb{Z}$ to $\mathbb{Z}/m\mathbb{Z}$. For a natural number $\ell \in \mathbb{N}$, let the elements in $\mathbb{Z}/\ell\mathbb{Z}$ be denoted as integers, for the sake of clarity. Now, consider the expression $\phi(1) \in \mathbb{Z}/m\mathbb{Z}$. Suppose that $\phi(1) = a$, for some element a in the codomain of ϕ. We thus find that:

$$\begin{aligned}
&\phi(1) = a(\mathrm{mod}\ m)\\
&\phi(2) = 2a(\mathrm{mod}\ m)\\
&\vdots\\
&\phi(n-1) = (n-1)a(\mathrm{mod}\ m)\\
&\phi(0) = (n \cdot \phi(1))(\mathrm{mod}\ m)
\end{aligned}$$

But since ϕ is a $\mathbb{Z}$-module homomorphism, we find that

$$n \cdot \phi(1) \equiv 0(\mathrm{mod}\ m),$$

so that

$$m \mid (n \cdot \phi(1)).$$

We also have that $0 \leq \phi(1) < m$. The number of values for $\phi(1)$ such that

$$m \mid (n \cdot \phi(1)).$$

and

$$0 \leq \phi(1) < m$$

must be equal to (m,n), as may be verified using the Fundamental Theorem of Arithmetic, in the following manner: since

$$m \mid (n \cdot \phi(1)),$$

we have that $\phi(1)$ may be an arbitrary integer multiple of $\frac{m}{\gcd(n,m)}$ satisfying

$$0 \leq \phi(1) < m,$$

and this shows that $\phi(1)$ must be of the form $i\frac{m}{\gcd(n,m)}$ for $i \in \mathbb{N}_0$ with

$$0 \leq i\frac{m}{\gcd(n,m)} < m,$$

which shows that the possible values for $i \in \mathbb{N}_0$ are precisely integers $i \in \mathbb{N}_0$ such that

$$0 \leq i\frac{1}{\gcd(n,m)} < 1,$$

so that the possible values for $i \in \mathbb{N}_0$ are precisely integers $i \in \mathbb{N}_0$ such that

$$0 \leq i < \gcd(n,m).$$

We thus observe that

$$|\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})| = (n, m).$$

Furthermore, we have a complete classification of the morphisms in $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$. In particular, the $\mathbb{Z}$-module homomorphisms in $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$ are precisely $\mathbb{Z}$-linear ϕ such that

$$\phi(1) \in \left\{0, 1 \cdot \frac{m}{\gcd(n,m)}, 2 \cdot \frac{m}{\gcd(n,m)}, \dots, (\gcd(n,m) - 1) \cdot \frac{m}{\gcd(n,m)}\right\}.$$

For an integer $i \in \mathbb{N}_0$ such that $i \in \{0, 1, 2, \dots, \gcd(n,m) - 1\}$, let ϕ_i denote the morphism whereby $1 \mapsto i \cdot \frac{m}{\gcd(n,m)}$. We thus have that:

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) = \{\phi_0, \phi_1, \phi_2, \dots, \phi_{\gcd(n,m)-1}\}.$$

Now, let

$$\Psi \colon \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \to \mathbb{Z}/(n,m)\mathbb{Z}$$

denote the mapping whereby

$$\Psi(\phi_i) = i \in \mathbb{Z}/(n,m)\mathbb{Z},$$

letting i be as given above, with $i \in \{0, 1, 2, \dots, \gcd(n,m) - 1\}$. We immediately see that Ψ is surjective, since for $j \in \mathbb{Z}/(n,m)\mathbb{Z}$, we have that $\Psi(\phi_j) = j$, with ϕ_j as an element in the domain of Ψ. Letting $i, j \in \{0, 1, 2, \dots, \gcd(n,m) - 1\}$, we see that:

$$\begin{aligned} \Psi(\phi_i) = \Psi(\phi_j) &\Longrightarrow i = j \\ &\Longrightarrow i \cdot \frac{m}{\gcd(n,m)} = j \cdot \frac{m}{\gcd(n,m)} \\ &\Longrightarrow \phi_i(1) = \phi_j(1). \end{aligned}$$

From the equality whereby $\phi_i(1) = \phi_j(1)$, we find that $\phi_i = \phi_j$, since ϕ_i and ϕ_j are both $\mathbb{Z}$-linear morphisms. Consider the sum $\phi_1 + \phi_1$. The sum $\phi_1 + \phi_1$ evaluated at 1 must be equal to $2 \cdot \frac{m}{\gcd(m,n)}$, the sum $\phi_1 + \phi_1 + \phi_1$ evaluated at 1 is equal to $3 \cdot \frac{m}{\gcd(m,n)}$, and so forth. Continuing in this manner, we find that Ψ must be $\mathbb{Z}$-linear. Since Ψ must be bijective and $\mathbb{Z}$-linear, we obtain the desired isomorphic equivalence.

3.4 Exercises from Section 10.3

In the following exercises, R is a ring with 1 and M is a left R-module.

Exercise 3.46. Prove that if A and B are sets of the same cardinality, then the free modules $F(A)$ and $F(B)$ are isomorphic.

Solution 3.47. This follows immediately from the results given in our solution to Exercise 1.9, letting $\mathscr{C}$ be the category **R-Mod** of left R-modules.

Exercise 3.48. Assume R is commutative. Prove that $R^n \cong R^m$ if and only if $n = m$, i.e., two free R-modules of finite rank are isomorphic if and only if they have the same rank. [Apply Exercise 12 of Section 2 with I a maximal ideal of R. You may assume that if F is a field, then $F^n \cong F^m$ if and only if $n = m$, i.e., two finite dimensional vector spaces over F are isomorphic if and only if they have the same dimension – this will be proved later in Section 11.1.]

Solution 3.49. This is proven in our solution for Exercise 1.17.

Exercise 3.50. Show that the $F[x]$-modules in Exercises 18 and 19 of Section 1 are both cyclic.

Solution 3.51. Letting M denote an R-module, we recall that a submodule N of M is said to be *cyclic* if there exists an element $a \in M$ such that $N = Ra$, that is, if N is generated by one element, with:

$$N = Ra = \{ra \mid r \in R\}.$$

Exercise 18 from Section 1 is given as follows:

"Let $F = \mathbb{R}$, let $V = \mathbb{R}^2$ and let T be the linear transformation from V to V which is rotation clockwise about the origin by $\pi/2$ radians. Show that V and 0 are the only $F[x]$-submodules for this T." (p. 344)

We can basically make $\mathbb{R}^2$ into an $\mathbb{R}[x]$-module using the given linear map T. In particular, we can turn $\mathbb{R}^2$ into an $\mathbb{R}[x]$-module so that given a polynomial $p(x)$ in $\mathbb{R}[x]$, and given a vector $\mathbf{v}$ in $\mathbb{R}^2$, we have that the polynomial $p(x)$ acts through substitution of the linear transformation T for x with respect to $p(x)$, and then by applying the resultant linear mapping to v.

So, we regard the plane $\mathbb{R}^2$ as an $\mathbb{R}[x]$-module with respect to the linear map T, in the sense described above. So, we need to show that there exists an element $\mathbf{v} \in \mathbb{R}^2$ such that $\mathbb{R}[x]\mathbf{v}$ is equal to $\mathbb{R}^2$.

We claim that the vector

$$\mathbf{v} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \in \mathbb{R}^2$$

generates the $\mathbb{R}[x]$-module $\mathbb{R}^2$ with respect to T. We thus find that

$$T\mathbf{v} = T\big|_{\mathbf{v}} = T\left(\begin{bmatrix} 1 \\ 0 \end{bmatrix}\right) = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \in \mathbb{R}^2$$

Basically, we can create an arbitrary point in the plane $\mathbb{R}^2$ as an $\mathbb{R}$-linear combination of $\mathbf{v}$ and $T\mathbf{v}$. In particular, letting a and b be arbitrary elements in $\mathbb{R}$, so that

$$\begin{bmatrix} a \\ b \end{bmatrix} \in \mathbb{R}^2$$

is given by an arbitrary point in the plane, we find that:

$$\begin{aligned} (bx + a)\mathbf{v} &= (bT + a)\mathbf{v} \\ &= bT(\mathbf{v}) + a\mathbf{v} \\ &= bT\left(\begin{bmatrix} 1 \\ 0 \end{bmatrix}\right) + a\begin{bmatrix} 1 \\ 0 \end{bmatrix} \\ &= b\begin{bmatrix} 0 \\ 1 \end{bmatrix} + a\begin{bmatrix} 1 \\ 0 \end{bmatrix} \\ &= \begin{bmatrix} 0 \\ b \end{bmatrix} + \begin{bmatrix} a \\ 0 \end{bmatrix} \\ &= \begin{bmatrix} a \\ b \end{bmatrix} \in \mathbb{R}^2. \end{aligned}$$

So, we have shown that each point in $\mathbb{R}^2$ must be an element in $\mathbb{R}[x]\mathbf{v}$. Conversely, we have that $\mathbb{R}[x]\mathbf{v} \subseteq \mathbb{R}^2$, so that $\mathbb{R}[x]\mathbf{v} = \mathbb{R}^2$.

In the class textbook, Exercise 19 from Section 1 is given as follows:

"Let $F = \mathbb{R}$, let $V = \mathbb{R}^2$ and let T be the linear transformation from V to V which is projection onto the y-axis. Show that V, 0, the x-axis and teh y-axis are te only $F[x]$-submodules for this T." (p. 344)

Letting T be as given in Exercise 19 from Section 1, we claim that the vector

$$\mathbf{w} = \begin{bmatrix} 1 \\ 1 \end{bmatrix} \in \mathbb{R}^2$$

generates the $\mathbb{R}[x]$-module $\mathbb{R}^2$ with respect to T. First of all, begin by observing that

$$T\mathbf{w} = T\big|_{\mathbf{w}} = T\left(\begin{bmatrix} 1 \\ 1 \end{bmatrix}\right) = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \in \mathbb{R}^2.$$

So, we find that:

$$(-x+1)\mathbf{w} = (-x+1)\begin{bmatrix} 1 \\ 1 \end{bmatrix} = (-T+1)\begin{bmatrix} 1 \\ 1 \end{bmatrix} = -T\left(\begin{bmatrix} 1 \\ 1 \end{bmatrix}\right) + \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ -1 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}.$$

So, since

$$(bx)\mathbf{w} = \begin{bmatrix} 0 \\ b \end{bmatrix}$$

and since

$$(-ax+a)\mathbf{w} = \begin{bmatrix} a \\ 0 \end{bmatrix},$$

we thus have that

$$(bx)\mathbf{w} + (-ax+a)\mathbf{w} = \begin{bmatrix} a \\ b \end{bmatrix} \in \mathbb{R}^2,$$

so that

$$((-a+b)x+a)\mathbf{w} = \begin{bmatrix} a \\ b \end{bmatrix} \in \mathbb{R}^2,$$

which shows that $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ generates $\mathbb{R}^2$ as an $\mathbb{R}[x]$-module, with respect to the projection mapping T.

3.5 Exercises from Section 12.1

Exercise 3.52. Let M be a module over the integral domain R. Suppose x is a nonzero torsion element in M. Show that x and 0 are "linearly dependent." Conclude that the rank of $\mathrm{Tor}(M)$ is 0, so that in particular any torsion R-module has rank 0.

Solution 3.53. Since x is a nonzero torsion element in M, we have that there exists a element r of the ring R that is neither a left nor a right zero divisor such that $rm = 0$. Since $r \neq 0$, we have that

$$rm + r0 = rm = 0,$$

thus proving that x and 0 are linearly dependent.

Recall that for any integral domain R, the *rank* of an R-module M is the maximum number of R-linearly independent elements of M. Since

$$\mathrm{Tor}(M) = \{x \in M \mid rx = 0 \text{ for some nonzero } r \in R\}.$$

But then $\mathrm{Tor}(M)$ cannot contain a linearly independent set with at least one element, since $rx = 0$ for some nonzero $r \in R$ for each element x in $\mathrm{Tor}(M)$.

Exercise 3.54. Letting M and R be as given above, show that the rank of M is the same as the rank of the (torsion free) quotient $M/\mathrm{Tor}M$.

Solution 3.55. Again, for any integral domain R, the *rank* of an R-module M is the maximum number of R-linearly independent elements of M. Suppose that the rank of M is n. Now, consider the quotient module $M/\mathrm{Tor}M$. By way of contradiction, suppose that there exist $n' > n$ R-linearly independent elements in $M/\mathrm{Tor}M$, so that

$$r_1(a_1 + \mathrm{Tor}M) + r_2(a_2 + \mathrm{Tor}M) + \cdots + r_{n'}(a_{n'} + \mathrm{Tor}M) = 0 + \mathrm{Tor}M$$

implies that the above coefficients in R are all equal to 0. Equivalently,

$$r_1a_1 + r_2a_2 + \cdots + r_{n'}a_{n'} + \mathrm{Tor}M = 0 + \mathrm{Tor}M$$

implies that the above coefficients in R are all equal to 0. Equivalently, we have that if

$$r_1a_1 + r_2a_2 + \cdots + r_{n'}a_{n'} \in \mathrm{Tor}M$$

then the above R-coefficients all must be equal to 0. So, suppose that

$$r_1a_1 + r_2a_2 + \cdots + r_{n'}a_{n'} \in \mathrm{Tor}M.$$

Then the above R-coefficients must be equal to zero, and there exists an R-coefficient q such that

$$(qr_1)a_1 + (qr_2)a_2 + \cdots + (qr_{n'})a_{n'} = 0.$$

But since $n' > n$, we have that there exists an expression of the form qr_i which must be nonzero. But this is impossible since $r_i = 0$. So, we have shown that the rank n' of $M/\mathrm{Tor}M$ is less than or equal to the rank n of M. Now, suppose that $\{b_1, b_2, \ldots, b_n\}$ is a set of linearly independent elements in M. By way of contradiction, suppose that it is not the case that

$$\{b_1 + \mathrm{Tor}M, b_2 + \mathrm{Tor}M, \ldots, b_n + \mathrm{Tor}M\}$$

is a set of linearly independent elements in $M/\mathrm{Tor}M$. So, we have that there exists a nontrivial linear combination

$$s_1(b_1 + \mathrm{Tor}M) + s_2(b_2 + \mathrm{Tor}M) + \cdots + s_n(b_n + \mathrm{Tor}M) = 0 + \mathrm{Tor}M$$

of the elements in $\{b_1 + \mathrm{Tor}M, b_2 + \mathrm{Tor}M, \ldots, b_n + \mathrm{Tor}M\}$ which vanishes. Since

$$s_1b_1 + s_2b_2 + \cdots + s_nb_n \in \mathrm{Tor}M$$

we have that there exists a regular coefficient t in R such that

$$ts_1b_1 + ts_2b_2 + \cdots + ts_nb_n = 0.$$

But recall that

$$s_1 (b_1 + \mathrm{Tor} M) + s_2 (b_2 + \mathrm{Tor} M) + \cdots + s_n (b_n + \mathrm{Tor} M) = 0 + \mathrm{Tor} M$$

is supposed to be a nontrivial linear combination of the elements in $\{b_1 + \mathrm{Tor} M, b_2 + \mathrm{Tor} M, \ldots, b_n + \mathrm{Tor} M\}$. So, we may assume that s_i is nonzero, for some index i. But since t is regular, we have that t is not a zero divisor. So, we have that s_i is nonzero, and thus ts_i is nonzero. But this is impossible, since $\{b_1, b_2, \ldots, b_n\}$ is linearly independent. So, we have shown that $n' \leq n$, and we have shown that there is a linearly independent n-set of elements in $M/\mathrm{Tor} M$, thus establishing the equality whereby $n' = n$.

Exercise 3.56. Let M be a module over the integral domain R. Suppose that M has rank n and that x_1, x_2, ..., x_n is any maximal set of linearly independent elements of M. Let $N = Rx_1 + \ldots + Rx_n$ be the submodule generated by $x_1, x_2, \ldots, x_n$. Prove that N is isomorphic to R^n and that the quotient M/N is a torsion R-module (equivalently, the elements $x_1, \ldots, x_n$ are linearly independent and for any $y \in M$ there is a nonzero element $r \in R$ such that ry can be written as a linear combination $r_1 x_1 + \ldots + r_n x_n$ of te x_i).

Solution 3.57. Given an integral domain R, the *rank* of an R-module M is the maximum number of R-linearly independent elements of M. So, let M, R, n, etc., be as given in the above exercise, with $x_1, x_2, \ldots, x_n$ as a maximal set of linearly independent elements in M, and with

$$N = Rx_1 + Rx_2 + \cdots + Rx_n.$$

To prove that $N \cong R^n$, we proceed to construct an explicit isomorphism $\phi \colon N \to R^n$. Letting $r_1, r_2, \ldots, r_n \in R$, so that

$$r_1 x_1 + r_2 x_2 + \cdots + r_n x_n$$

is an arbitrary element in the domain of N. We define the mapping ϕ so that

$$\phi(r_1 x_1 + r_2 x_2 + \cdots + r_n x_n) = (r_1, r_2, \ldots, r_n) \in R^n.$$

The injectivity of ϕ follows immediately from the linear independence of the set $\{x_1, x_2, \ldots, x_n\}$, and the surjectivity of ϕ follows in a straightforward way from the definition of ϕ. We have that ϕ must preserve addition, since

$$\phi(r_1 x_1 + r_2 x_2 + \cdots + r_n x_n) + \phi(s_1 x_1 + s_2 x_2 + \cdots + s_n x_n)$$

is equal to

$$(r_1, r_2, \ldots, r_n) + (s_1, s_2, \ldots, s_n) = (r_1 + s_1, r_2 + s_2, \ldots, r_n + s_n),$$

letting $s_1, s_2, \ldots, s_n \in R$. We also have that ϕ must preserve scalar multiplication, since, given a scalar $t \in R$, we find that

$$t \cdot \phi(r_1 x_1 + r_2 x_2 + \cdots + r_n x_n)$$

is equal to

$$t \cdot (r_1, r_2, \ldots, r_n) = (t \cdot r_1, t \cdot r_2, \ldots, t \cdot r_n).$$

Accordingly, we find that ϕ is a bijective morphism, as desired.

The following definition is taken directly from the class textbook:

"An R-module M is called a *torsion* module if for each $m \in M$ there is a nonzero element $r \in R$ such that $rm = 0$, where r may depend on m..." (p. 356)

Now, recall that given an arbitrary submodule B of a module A, we can always form the quotient module A/B. In particular, we find that the quotient module M/N is well-defined. The underlying set of this quotient module consists of additive cosets of the form $m + N$ for elements $m \in M$.

So, we must show that for all $m \in M$ there exists a nonzero scalar $y \in R \setminus \{0\}$ such that:

$$ym \in Rx_1 + Rx_2 + \cdots + Rx_n.$$

By way of contradiction, suppose that there exists some $m \in M$ such that for all nonzero $y \in R \setminus \{0\}$

$$ym \notin Rx_1 + Rx_2 + \cdots + Rx_n.$$

Equivalently, there exists an element $m \in M$ such that for all $y \in R \setminus \{0\}$ and $r_1, r_2, \dots, r_n \in R$,

$$ym \neq r_1x_1 + r_2x_2 + \cdots + r_nx_n.$$

But then we would have that the subset

$$\{m, x_1, x_2, \dots, x_n\}$$

of M would have to be linearly independent with respect to M, because otherwise, there would exist a nontrivial linear combination

$$zm + s_1x_1 + s_2x_2 + \cdots + s_nx_n = 0$$

which vanishes, with z nonzero since $\{x_1, x_2, \dots, x_n\}$ is linearly independent, so that

$$zm = (-s_1)x_1 + (-s_2)x_2 + \cdots + (-s_n)x_n$$

contradicting that for all $y \in R \setminus \{0\}$ and $r_1, r_2, \dots, r_n \in R$,

$$ym \neq r_1x_1 + r_2x_2 + \cdots + r_nx_n.$$

But then the maximality of $x_1, x_2, \dots, x_n\}$ would be contradicted.

3.6 Exercises from Section 12.2

Exercise 3.58. Prove that similar linear transformations of V (or $n \times n$ matrices) have the same characteristic and the same minimal polynomial.

Solution 3.59. Let A and B be $n \times n$ matrices such that A and B are similar. So, let C be a non-singular matrix such that:

$$A = CBC^{-1}.$$

Now, recall that the minimal polynomial $\mu_A(x)$ of A is the monic polynomial

$$\mu_A(x) = x^m + a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \cdots + a_1x + a_0$$

of minimal degree such that

$$A^m + a_{m-1}A^{m-1} + a_{m-2}A^{m-2} + \cdots + a_1A + a_0I_n = 0,$$

and similarly for the minimal polynomial

$$\mu_B(x) = x^\ell + b_{\ell-1}x^{\ell-1} + b_{\ell-2}x^{\ell-2} + \cdots + b_1x + b_0$$

for B, with:

$$B^\ell + b_{\ell-1}B^{\ell-1} + b_{\ell-2}B^{\ell-2} + \cdots + b_1 B + b_0 I_n = 0.$$

Multiplying both sides of the above equality on the left by C and on the right by C^{-1}, since $A^i = CB^iC^{-1}$ for $i \in \mathbb{N}_0$, we have that:

$$A^\ell + b_{\ell-1}A^{\ell-1} + b_{\ell-2}A^{\ell-2} + \cdots + b_1 A + b_0 I_n = 0.$$

By minimality of μ_A, we have that $\mu_A | \mu_B$. A symmetric argument shows that $\mu_B | \mu_A$, which shows that $\mu_B = \mu_A$.

Now, consider the characteristic polynomial of B:

$$c_B(x) = \det(xI - B).$$

From the above equality, we have that:

$$\det(C) c_B(x) \det(C^{-1}) = \det(C) \det(xI - B) \det(C^{-1}).$$

Therefore,

$$c_B(x) = \det(C(xI - B)C^{-1}).$$

Equivalently,

$$c_B(x) = \det(xI - CBC^{-1}),$$

with

$$c_B(x) = \det(xI - A),$$

as desired.

Exercise 3.60. Let M be as in Lemma 19. Prove that the minimal polynomial of M is the least common multiple of the minimal polynomials of $A_1, \ldots, A_k$.

Solution 3.61. Lemma 19 from the class textbook is formulated in the following manner:

Lemma 19. Let $a(x) \in F[x]$ be any monic polynomial.

(1) The characteristic polynomial of the companion matrix of $a(x)$ is $a(x)$.

(2) If M is the block diagonal matrix

$$M = \begin{pmatrix} A_1 & 0 & \ldots & 0 \\ 0 & A_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & A_k \end{pmatrix}$$

given by the direct sum of matrices A_1, A_2, …, A_k then the characteristic polynomial of M is the product of the characteristic polynomials of A_1, A_2, …, A_k.

By the above lemma, we have that the characteristic polynomial $\mathrm{ch}_x(M)$ of M is equal to:

$$\mathrm{ch}_x(A_1)\mathrm{ch}_x(A_2)\cdots\mathrm{ch}_x(A_k).$$

We know that the minimal polynomial $m_x(M)$ of M must divide

$$\mathrm{ch}_x(A_1)\mathrm{ch}_x(A_2)\cdots\mathrm{ch}_x(A_k).$$

For an integer $i \in \mathbb{N}_0$, we have that:

$$M^i = \begin{pmatrix} A_1^i & 0 & \dots & 0 \\ 0 & A_2^i & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & A_k^i \end{pmatrix}.$$

The minimal polynomial $m_x(A_1)$ is the smallest polynomial which vanishes under A_1. So, in order for the upper-left block of M to vanish under a polynomial

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0,$$

with

$$a_n \begin{pmatrix} A_1^n & 0 & \dots & 0 \\ 0 & A_2^n & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & A_k^n \end{pmatrix} + a_{n-1} \begin{pmatrix} A_1^{n-1} & 0 & \dots & 0 \\ 0 & A_2^{n-1} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & A_k^{n-1} \end{pmatrix} + \dots + a_0 I = \mathbf{0},$$

letting I denote an appropriate identity matrix, and letting $\mathbf{0}$ denote an appropriate zero matrix, we have that the polynomial $p(x)$ would have to be a multiple $m_x(A_1)$, since we would have to have that

$$a_n A_1^n + a_{n-1}A_1^{n-1} + \dots + a_0 I = \mathbf{0}.$$

Similarly, in order for a fixed block B of the block matrix M to vanish under a polynomial, we would have that the minimal polynomial for B would have to divide this polynomial. So, given a polynomial $q(x)$ such that *each* block B of M vanishes with respect to $q(x)$, we find that *each* minimal polynomial for *each* block B of M would have to divide $q(x)$. So, if M vanishes with respect to a polynomial $q(x)$, the polynomial $q(x)$ must be a multiple of all of the minimal polynomials of all the blocks of M. Since M vanishes under the minimal polynomial for M, we have that the minimal polynomial for M must be a multiple of all of the minimal polynomials for all of the blocks of M, and by minimality of the minimal polynomial for M, we may conclude that the minimal polynomial of M is the least common multiple of the minimal polynomials for the blocks of M.

3.7 Exercises from Section 12.3

Exercise 3.62. Suppose the vector space V is the direct sum of cyclic $F[x]$-modules whose annihilators are $(x+1)^2$, $(x-1)(x^2+1)^2$, (x^4-1) and $(x+1)(x^2-1)$. Determine the invariant factors and elementary divisors for V.

Solution 3.63. Our solution is based upon a solution given in the following link:

```
https://crazyproject.wordpress.com/2011/11/17/
compute-the-invariant-factors-and-elementary-divisors-of-a-given-module/
```

Letting V be as given above, we have that:

$$V = F[x]/\langle (x+1)^2 \rangle \oplus F[x]/\langle (x-1)(x^2+1)^2 \rangle \oplus F[x]/\langle x^4 - 1 \rangle \oplus F[x]/\langle (x+1)(x^2-1) \rangle.$$

Our strategy is to apply the following result from the class textbook, which is a corollary to the Chinese Remainder Theorem.

"**Proposition 16.** Let $g(x)$ be a nonconstant monic element of $F[x]$ and let

$$g(x) = f_1(x)^{n_1} f_2(x)^{n_2} \cdots f_k(x)^{n_k}$$

be its factorization into irreducibles, where the $f_i(x)$ are distinct. Then we have the following isomorphism of rings:

$$F[x]/\langle g(x)\rangle \cong F[x]/\langle f_1(x)^{n_1}\rangle \times F[x]/\langle f_2(x)^{n_2}\rangle \times \cdots \times F[x]/\langle f_k(x)^{n_k}\rangle.\text{" (p. 313)}$$

We also review the term *invariant factor*, as defined in the class textbook.

"**Theorem 5.** *(Fundamental Theorem, Existence: Invariant Factor Form)* Let R be a P.I.D. and let M be a finitely generated R-module.

(1) Then M is isomorphic to the direct sum of finitely many cyclic modules. More precisely,

$$M \cong R^r \oplus R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m)$$

for some integer $r \geq 0$ and nonzero elements $a_1, a_2, \ldots, a_m$ for R which are not units in R and which satisfy the divisibility relations

$$a_1 \mid a_2 \mid \cdots \mid a_m.\text{" (p. 462)}$$

"**Definition.** The integer r in Theorem 5 is called the *free rank* or the *Betti number* of M and the elements $a_1, a_2, \ldots, a_m \in R$ (defined up to multiplication by units in R) are called the *invariant factors* of M."

We also review the term *elementary divisor*, as defined in the class textbook.

"**Theorem 6.** *(Fundamental Theorem, Existence: Elementary Divisor Form)* Let R be a P.I.D. and let M be a finitely generated R-module. Then M is the direct sum of a finite number of cyclic modules whose annihilators are either (0) or generated by powers of primes in R, i.e.,

$$M \cong R^r \oplus R/(p_1^{\alpha_1}) \oplus R/(p_2^{\alpha_2}) \oplus \cdots \oplus R/(p_t^{\alpha_t})$$

where $r \geq 0$ is an integer and $p_1^{\alpha_1}$, …, $p_t^{\alpha_t}$ are positive powers of (not necessarily distinct) primes in R." (p. 464)

"**Definition.** Let R be a P.I.D. and let M be a finitely generated R-module as in Theorem 6. The prime powers $p_1^{\alpha_1}$, …, $p_t^{\alpha_1}$ (defined up to multiplication by units in R) are called the *elementary divisors* of M." (p. 465)

Now, letting V be as given in the above exercise, recall that:

$$V = F[x]/\langle (x+1)^2\rangle \oplus F[x]/\langle (x-1)(x^2+1)^2\rangle \oplus F[x]/\langle x^4-1\rangle \oplus F[x]/\langle (x+1)(x^2-1)\rangle.$$

We proceed to consider two separate cases, namely, the case whereby x^2+1 is irreducible in $F[x]$, and the case whereby x^2+1 is reducible in $F[x]$. First suppose that x^2+1 is irreducible in $F[x]$. So, in the case whereby x^2+1 is irreducible in $F[x]$, according to **Proposition 16** from the class textbook, we find that the irreducible factors of V are:

$$(x+1)(x-1)$$

$$(x+1)^2(x-1)(x^2+1)$$
$$(x+1)^2(x-1)(x^2+1)^2$$

The elementary divisors are the prime power divisors of the irreducible factors[3]:

$$\begin{aligned}&(x-1)\\&(x-1)\\&(x-1)\\&(x+1)\\&(x+1)^2\\&(x+1)^2\\&(x^2+1)\\&(x^2+1)^2\end{aligned}$$

Now, suppose that x^2+1 is reducible in $F[x]$. We may deduce that there exists an element $\alpha \in F$ such that $x^2+1 = (x+\alpha)(x-\alpha) = x^2-\alpha^2$. Now, recall that

$$V = F[x]/\langle (x+1)^2\rangle \oplus F[x]/\langle (x-1)(x^2+1)^2\rangle \oplus F[x]/\langle x^4-1\rangle \oplus F[x]/\langle (x+1)(x^2-1)\rangle.$$

So, we have that the invariant factors are:

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

The elementary divisors of V are:

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

3.8 Exercises from Section 10.5

Suppose that

[3] Another solution is given in : `http://orion.math.iastate.edu/maddux/505-Spring-2010/allhw.3.pdf`.

$$\begin{tikzcd}
A \arrow[r, "\psi"] \arrow[d, "\alpha"] & B \arrow[r, "\phi"] \arrow[d, "\beta"] & C \arrow[d, "\gamma"] \\
A' \arrow[r, "\psi'"] & B' \arrow[r, "\phi'"] & C'
\end{tikzcd}$$

is a commutative diagram of groups and that the rows are exact.

Exercise 3.64. With respect to the above diagram, if ϕ and α are surjective, and β is injective then γ is injective. [If $c \in \ker\gamma$, show there is a $b \in B$ with $\phi(b) = c$. Show that $\phi'(\beta(b)) = 0$ and deduce that $\beta(b) = \psi'(a')$ for some $a' \in A'$. Show there is an $a \in A$ with $\alpha(a) = a'$ and that $\beta(\psi(a)) = \beta(b)$. Conclude that $b = \psi(a)$ and hence $c = \phi(b) = 0$.]

Solution 3.65. With respect to the above diagram, assume that ϕ and α are surjective, and assume that β is injective. To prove that γ is injective, our strategy is to follow the method suggested above, by proving that the kernel of γ is trivial. As above, assume that $c \in \ker(\gamma)$. Since ϕ is a surjective mapping from B to C, and since the kernel of γ is contained in C, we have that there must be an element b in the domain of ϕ such that $\phi(b) = c$. Now, recall that c is an element in the kernel of γ, so that $\gamma(c) = 0$, letting 0 denote the identity element of the groups presently under consideration. Since ϕ is a morphism, and since $\gamma(c) = 0$, we have that:

$$\phi(\gamma(c)) = \phi(0) = 0.$$

Since

$$\phi(\gamma(c)) = 0,$$

and since the above diagram is commutative, we may deduce that

$$\phi'(\beta(b)) = 0.$$

Since the rows of the above diagram are exact, we have that:

$$\operatorname{im}(\psi') = \ker(\phi').$$

So, since

$$\phi'(\beta(b)) = 0,$$

we have that $\beta(b)$ must be an element in the kernel of ϕ'. Therefore, $\beta(b)$ must be an element in $\operatorname{im}(\psi')$. So, there must exist some element a' in A' such that

$$\beta(b) = \phi'(a').$$

Now, recall that we assumed that α is surjective. Since a' is an element in the codomain of α, there must be an element a in A such that $\alpha(a) = a'$. From the equality

$$\beta(b) = \phi'(a'),$$

we thus find that

$$\beta(b) = \phi'(\alpha(a)).$$

Since the above diagram commutes, we have that

$$\beta(b) = \beta(\psi(a)).$$

Since β is injective, we have that

$$b = \psi(a).$$

Therefore,

$$\phi(b) = \phi(\psi(a)).$$

That is,

$$c = \phi(b) = \phi(\psi(a)).$$

Now, since $\psi(a)$ is in $\text{im}\,(\psi) = \ker(\phi)$, we may conclude that $\phi(\psi(a)) = 0$, so that $c = 0$, as desired.

Exercise 3.66. Prove that if β is surjective and if γ and ψ' are injective then α is surjective.

Remark 3.67. The author previously constructed the following solution for an assigned problem in MATH 6121. This solution is available through the course website `http://garsia.math.yorku.ca/~zabrocki/math6121f16/` for MATH 6121.

Solution 3.68. Since the bottom row forms an exact sequence, we have that an element $b' \in B'$ is mapped to $e_{C'}$ iff it is in $\text{im}\psi'$. Since the top row forms an exact sequence, we have that an element $b \in B$ is mapped to e_C iff it is in $\text{im}\psi$.

Now, since γ is injective, an element $b \in B$ is mapped to $e_{C'}$ through $\gamma \circ \phi$ iff it is in $\text{im}\psi$.

So, since the given diagram commutes, with $\gamma \circ \phi = \phi' \circ \beta$, we have that an element $b \in B$ is mapped to $e_{C'}$ iff:

(i) $b \in \text{im}\psi$; and

(ii) $\beta(b) \in \text{im}(\psi')$.

We claim that the image of $\beta \circ \psi$ is equal to the image of ψ'. Given in element $a \in A$, we have that:

$$\psi(a) \in \text{im}\psi = \ker(\phi).$$

Again by injectivity of γ, we find that $\psi(a)$ must be mapped to $e_{C'}$. Given an element $a \in A$, we know that $\psi(a)$ is mapped to $e_{C'}$ iff $(\beta \circ \psi)(a) \in \text{im}(\psi')$. So, this shows that $\text{im}(\beta \circ \psi) \subseteq \text{im}(\psi')$.

Now, by way of contradiction, suppose that there exists an element $x \in \text{im}(\psi')$ outside of $\text{im}(\beta \circ \psi)$. But by surjectivity of β, there exists an element $y \in B$ such that $\beta(y) = x$. But y would be mapped to $e_{C'}$ y would have to be in the image of ψ, so that $\beta(y) \in \text{im}(\beta \circ \psi)$, contradicting our initial assumption that $\beta(y) \notin \text{im}(\beta \circ \psi)$.

So, we have shown that $\text{im}(\beta \circ \psi) = \text{im}(\psi')$. So, for each element $a' \in A'$, we have that

$$\psi'(a') \in \text{im}(\psi') = \text{im}(\beta \circ \psi),$$

so that there exists a corresponding element $a \in A$ such that:

$$\psi(\beta(a)) = \psi'(a').$$

But since the given diagram commutes, we have that

$$\psi(\beta(a)) = \psi'(a') = \psi'(\alpha(a)).$$

By injectivity of ψ', we have that:

$$\psi'(a') = \psi'(\alpha(a)) \Longrightarrow a' = \alpha(a),$$

thus proving the surjectivity of α.

3.9 Exercises from Section 13.1

Exercise 3.69. Show that $p(x) = x^3 + 9x + 6$ is irreducible in $\mathbb{Q}[x]$. Let θ be a root of $p(x)$. Find the inverse of $1 + \theta$ in $\mathbb{Q}(\theta)$.

Solution 3.70. Letting $p(x) = x^3 + 9x + 6$, begin by observing that $p'(x) = 3x^2 + 9$ is always positive, so that $p(x) = x^3 + 9x + 6$ is strictly increasing. So, we have that $p(x) = x^3 + 9x + 6$ has only one real root. It is easily seen that $\sqrt[3]{3} - 3^{2/3}$ is a root of p. If we accept that $\sqrt[3]{3} - 3^{2/3}$ is irrational, we have that the only real root of p is irrational. Alternatively, one may use the fact that a polynomial with integer coefficients is irreducible over $\mathbb{Q}$ iff it is irreducible over $\mathbb{Z}$.

Now, let θ be as given above, with θ as a root of $p(x)$. Since $\mathbb{Q}(\theta)$ is a field, we have that $\frac{1}{1+\theta}$ is in $\mathbb{Q}(\theta)$. By the Euclidean algorithm, in $\mathbb{Q}[x]$, there are polynomials $a(x)$ and $b(x)$ such that

$$a(x)(1 + x) + b(x)(x^3 + 9x + 6) = 1.$$

Let a and b be denoted as indicated below.

$$(c_2x^2 + c_1 + c_0)(x + 1) + b(x)(x^3 + 9x + 6) = 1.$$

$$(\theta + 1)^3 = \theta^3 + 3\theta^2 + 3\theta + 1$$

$$= 3\theta^2 - 6\theta - 6$$

So

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

$$(\theta + 1)^2 = \theta^2 + 2\theta + 1$$

$$\frac{1}{3}(\theta + 1)^3 - (\theta + 1)^2 = -4\theta - 3$$

$$\frac{1}{3}(\theta + 1)^3 - (\theta + 1)^2 + 4(\theta + 1) = 1$$

So, from the above evaluation, we find that:

$$\frac{1}{3}(\theta + 1)^2 - (\theta + 1) + 4 = \frac{1}{\theta + 1}$$

That is, $\frac{1}{\theta+1}$ is equal to:

$$\frac{\theta^2}{3} - \frac{\theta}{3} + \frac{10}{3}.$$

Exercise 3.71. Show that x^3-2x-2 is irreducible over $\mathbb{Q}$ and let θ be a root. Compute $(1+\theta)(1+\theta+\theta^2)$ and $\frac{1+\theta}{1+\theta+\theta^2}$ in $\mathbb{Q}(\theta)$.

Solution 3.72. Let $p(x) = x^3 - 2x - 2$. Then $p'(x) = 3x^2 - 2$. Since $p'(x)$ is only negative if x satisfies the condition whereby $-\sqrt{\frac{2}{3}} < x < \sqrt{\frac{2}{3}}$. So, since $p(x)$ is strictly increasing for $|x| > \sqrt{\frac{2}{3}}$, it is easily seen that $p(x)$ has only one real rool, namely

$$\frac{1}{3}\sqrt[3]{27-3\sqrt{57}} + \frac{\sqrt[3]{9+\sqrt{57}}}{3^{2/3}} = 1.76929...$$

Recall that a polynomial with integer coefficients is irreducible over $\mathbb{Q}$ iff it is irreducible over $\mathbb{Z}$. Since the only real root of p is the non-integer expression given above, we have that p is irreducible as an element in $\mathbb{Q}[x]$, as desired.

Letting θ be a root of the given polynomial $x^3 - 2x - 2$, expand the expression $(1+\theta)(1+\theta+\theta^2)$ as follows:

$$(1+\theta)(1+\theta+\theta^2) = 1 + 2\theta + 2\theta^2 + \theta^3.$$

Since

$$\theta^3 - 2\theta - 2 = 0,$$

we find that

$$\theta^3 = 2\theta + 2,$$

we find that

$$(1+\theta)(1+\theta+\theta^2) = 3 + 4\theta + 2\theta^2.$$

Now, to expand the expression

$$\frac{1+\theta}{1+\theta+\theta^2}$$

in $\mathbb{Q}(\theta)$, we begin by expanding the expression

$$\frac{1}{1+\theta+\theta^2}$$

in $\mathbb{Q}(\theta)$. So, it remains to find an expression of the form

$$a\theta^2 + b\theta + c \in \mathbb{Q}(\theta)$$

such that

$$(a\theta^2 + b\theta + c)(\theta^2 + \theta + 1) = 1.$$

From the above equality, we have that:

$$a\theta^4 + a\theta^3 + a\theta^2 + b\theta^3 + b\theta^2 + b\theta + c\theta^2 + c\theta + c = 1.$$

From the above equation, we find that:

$$2a + 2b + c + 4a\theta + 3b\theta + c\theta + 3a\theta^2 + b\theta^2 + c\theta^2 = 1.$$

We thus arrive at the following system of equalities:

$$2a + 2b + c = 1$$

$$4a + 3b + c = 0$$

$$3a + b + c = 0$$

Solving the above system, we find that $a = -\frac{2}{3}$, $b = \frac{1}{3}$, and $c = \frac{5}{3}$. Since

$$\left(-\frac{2}{3}\theta^2 + \frac{1}{3}\theta + \frac{5}{3}\right)(\theta^2 + \theta + 1) = 1,$$

we find that

$$-\frac{2}{3}\theta^2 + \frac{1}{3}\theta + \frac{5}{3} = \frac{1}{\theta^2 + \theta + 1}.$$

Therefore,

$$(1 + \theta)\left(-\frac{2}{3}\theta^2 + \frac{1}{3}\theta + \frac{5}{3}\right) = \frac{1 + \theta}{\theta^2 + \theta + 1}.$$

Therefore,

$$-\frac{2\theta^3}{3} - \frac{\theta^2}{3} + 2\theta + \frac{5}{3} = \frac{1 + \theta}{\theta^2 + \theta + 1}.$$

Equivalently,

$$-\frac{\theta^2}{3} + \frac{2\theta}{3} + \frac{1}{3} = \frac{1 + \theta}{\theta^2 + \theta + 1}.$$

Exercise 3.73. Show that $x^3 + x + 1$ is irreducible over $\mathbb{F}_2$ and let θ be a root. Compute the powers of θ in $\mathbb{F}_2(\theta)$.

Solution 3.74. By way of contradiction, suppose that $x^3 + x + 1$ is reducible over $\mathbb{F}_2$. We thus have that $x^3 + x + 1$ must be equal to a product of a degree-1 polynomial in $\mathbb{F}_2[x]$ and a degree-2 polynomial in $\mathbb{F}_2[x]$. By comparing the leading and constand coefficients of these polynomials, we have that

$$x^3 + x + 1 = (x + 1)(x^2 + cx + 1)$$

for some constant c. Expanding the above expression, we find that

$$x^3 + x + 1 = x^3 + (c + 1)x^2 + (c + 1)x + 1.$$

But then $c + 1$ must be equal to 0, since the coefficient of x^2 in the latter polynomial must be 0, but $c + 1$ must also be equal to 1, as given by the coefficient of x in this polynomial. We thus arrive at a contradiction.

Now, let θ denote a fixed root of the irreducible polynomial $x^3 + x + 1$. Since

$$\theta^3 + \theta + 1 = 0,$$

we have that

$$\theta^3 = \theta + 1.$$

We may thus compute the initial powers of θ in the following manner:

$$\begin{aligned} \theta &= \theta \\ \theta^2 &= \theta^2 \\ \theta^3 &= \theta + 1 \\ \theta^4 &= \theta^2 + \theta \end{aligned}$$

$$\begin{aligned}\theta^5 &= \theta^2 + \theta + 1\\ \theta^6 &= \theta^2 + 1\\ \theta^7 &= 1.\end{aligned}$$

From the above evaluations, we have that the following equalities hold for $m \in \mathbb{N}_0$:

$$\begin{aligned}\theta^{7m+1} &= \theta\\ \theta^{7m+2} &= \theta^2\\ \theta^{7m+3} &= \theta + 1\\ \theta^{7m+4} &= \theta^2 + \theta\\ \theta^{7m+5} &= \theta^2 + \theta + 1\\ \theta^{7m+6} &= \theta^2 + 1\\ \theta^{7m+7} &= 1.\end{aligned}$$

Exercise 3.75. Prove directly that the map $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ is an isomorphism of $\mathbb{Q}(\sqrt{2})$ to itself.

Solution 3.76. Recall that $\mathbb{Q}(\sqrt{2})$ consists precisely of expressions of the form $a + b\sqrt{2}$ for $a, b \in \mathbb{Q}$. Letting $\phi\colon \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ denote the mapping whereby $a + b\sqrt{2} \mapsto a - b\sqrt{2}$, we have that ϕ is well-defined in the sense that ϕ is defined for each element in the given domain of ϕ. Moreover, we find that ϕ is well-defined in the sense that for each input element q in the domain of ϕ, $\phi(q)$ is in the given codomain of ϕ. Given an arbitrary element $c + d\sqrt{2}$ in the codomain of ϕ, where c and d denote rational numbers, we have that $c - d\sqrt{2}$ maps to $c + d\sqrt{2} \in \operatorname{cod}(\phi)$ with respect to ϕ, thus proving the surjectivity of ϕ. Letting $a_1, a_2, b_1, b_2 \in \mathbb{Q}$, suppose that:

$$\phi(a_1 + b_1\sqrt{2}) = \phi(a_2 + b_2\sqrt{2}).$$

Equivalently,

$$a_1 - b_1\sqrt{2} = a_2 - b_2\sqrt{2}.$$

Comparing coefficients on both sides of the above equation, we may deduce that $a_1 = a_2$ and $b_1 = b_2$. Therefore, $a_1 + b_1\sqrt{2}$ must be equal to $a_2 + b_2\sqrt{2}$, thus proving the injectivity of ϕ. So, it remains to prove that ϕ is a ring homomorphism. As shown below, we find that ϕ preserves the underlying additive binary operation on $\mathbb{Q}(\sqrt{2})$:

$$\begin{aligned}\phi((a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2})) &= \phi(a_1 + a_2 + (b_1 + b_2)\sqrt{2})\\ &= a_1 + a_2 - (b_1 + b_2)\sqrt{2}\\ &= a_1 + a_2 - (b_1\sqrt{2} + b_2\sqrt{2})\\ &= a_1 + a_2 - b_1\sqrt{2} - b_2\sqrt{2}\\ &= a_1 - b_1\sqrt{2} + a_2 - b_2\sqrt{2}\\ &= \phi(a_1 + b_1\sqrt{2}) + \phi(a_2 + b_2\sqrt{2}).\end{aligned}$$

In a somewhat similar fashion, we find that ϕ preserves the underlying multiplicative binary operation on $\mathbb{Q}(\sqrt{2})$, as demonstrated below:

$$\begin{aligned}\phi((a_1 + b_1\sqrt{2}) \cdot (a_2 + b_2\sqrt{2})) &= \phi(a_1a_2 + a_2b_1\sqrt{2} + a_1b_2\sqrt{2} + 2b_1b_2)\\ &= \phi(a_1a_2 + 2b_1b_2 + (a_2b_1 + a_1b_2)\sqrt{2})\end{aligned}$$

$$\begin{aligned}&= a_1a_2 + 2b_1b_2 - (a_2b_1 + a_1b_2)\sqrt{2}\\ &= a_1a_2 + 2b_1b_2 - a_2b_1\sqrt{2} - a_1b_2\sqrt{2}\\ &= a_1a_2 - a_2b_1\sqrt{2} - a_1b_2\sqrt{2} + 2b_1b_2\\ &= (a_1 - b_1\sqrt{2})\cdot(a_2 - b_2\sqrt{2})\\ &= \phi(a_1 + b_1\sqrt{2})\cdot\phi(a_2 + b_2\sqrt{2}).\end{aligned}$$

We thus have that ϕ is a bijective morphism, as desired.

Exercise 3.77. Suppose α is a rational root of a monic polynomial in $\mathbb{Z}[x]$. Prove that α is an integer.

Solution 3.78. Letting α be as given above, suppose that α is a rational root of the monic polynomial

$$x^n + z_{n-1}x^{n-1} + z_{n-2}x^{n-2} + \cdots + z_1x + z_0 \in \mathbb{Z}[x],$$

letting $n \in \mathbb{N}$, and letting $z_0, z_1, \ldots, z_{n-1} \in \mathbb{Z}$. Since $\alpha \in \mathbb{Q}$, we may write $\alpha = \frac{a}{b}$, letting $a \in \mathbb{Z}$, with $b \in \mathbb{Z} \setminus \{0\}$. We thus have that:

$$\left(\frac{a}{b}\right)^n + z_{n-1}\left(\frac{a}{b}\right)^{n-1} + z_{n-2}\left(\frac{a}{b}\right)^{n-2} + \cdots + z_1\left(\frac{a}{b}\right) + z_0 = 0.$$

Let the fraction $\frac{a}{b}$ be in lowest terms. Since

$$\left(\frac{a}{b}\right)^n + z_{n-1}\left(\frac{a}{b}\right)^{n-1} + z_{n-2}\left(\frac{a}{b}\right)^{n-2} + \cdots + z_1\left(\frac{a}{b}\right) + z_0 = 0$$

we have that

$$\left(\frac{a}{b}\right)^n + \frac{z}{b^{n-1}} = 0$$

for some integer z. But then

$$\frac{a^n}{b^n} + \frac{bz}{b^n} = 0$$

so that

$$a^n = -bz.$$

If

$$a = \pm p_{\alpha_1}^{\beta_1} p_{\alpha_2}^{\beta_2} \cdots p_{\alpha_{m_1}}^{\beta_{m_1}}$$

is the prime factorization of a and

$$b = \pm p_{\gamma_1}^{\delta_1} p_{\gamma_2}^{\delta_2} \cdots p_{\gamma_{m_2}}^{\delta_{m_2}}$$

is the prime factorization of b, so that

$$\{p_{\alpha_1}, p_{\alpha_2}, \ldots, p_{\alpha_{m_1}}\}$$

and

$$\{p_{\gamma_1}, p_{\gamma_2}, \ldots, p_{\gamma_{m_2}}\}$$

are disjoint, since

$$a^n = \pm p_{\alpha_1}^{n\beta_1} p_{\alpha_2}^{n\beta_2} \cdots p_{\alpha_{m_1}}^{n\beta_{m_1}}$$

we have that the prime factorization of z must contain $p_{\alpha_1}^{n\beta_1} p_{\alpha_2}^{n\beta_2} \cdots p_{\alpha_{m_1}}^{n\beta_{m_1}}$. But this shows that the absolute value of $\frac{a^n}{z}$ must be less than or equal to 1, thus proving that $b \in \{1, -1\}$, as desired.

Exercise 3.79. Show that if α is a root of $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, then $a_n\alpha$ is a root of the monic polynomial $x^n + a_{n-1}x^{n-1} + a_n a_{n-2}x^{n-2} + \cdots + a_n^{n-2}a_1 x + a_n^{n-1}a_0$.

Solution 3.80. Assume that α is a root of $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. We thus have that:

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0.$$

Now, consider the following polynomial:

$$x^n + a_{n-1}x^{n-1} + a_n a_{n-2}x^{n-2} + \cdots + a_n^{n-2}a_1 x + a_n^{n-1}a_0.$$

Now, let the above expression be evaluated so that $x = a_n\alpha$. So, we find that:

$$\begin{aligned}
&x^n + a_{n-1}x^{n-1} + a_n a_{n-2}x^{n-2} + \cdots + a_n^{n-2}a_1 x + a_n^{n-1}a_0 \\
&= (a_n\alpha)^n + a_{n-1}(a_n\alpha)^{n-1} + a_n a_{n-2}(a_n\alpha)^{n-2} + \cdots + a_n^{n-2}a_1(a_n\alpha) + a_n^{n-1}a_0 \\
&= (a_n\alpha)^n + a_{n-1}a_n^{n-1}\alpha^{n-1} + a_{n-2}a_n^{n-1}\alpha^{n-2} + \cdots + a_n^{n-1}a_1\alpha + a_n^{n-1}a_0 \\
&= a_n^n\alpha^n + a_{n-1}a_n^{n-1}\alpha^{n-1} + a_{n-2}a_n^{n-1}\alpha^{n-2} + \cdots + a_n^{n-1}a_1\alpha + a_n^{n-1}a_0 \\
&= a_n a_n^{n-1}\alpha^n + a_{n-1}a_n^{n-1}\alpha^{n-1} + a_{n-2}a_n^{n-1}\alpha^{n-2} + \cdots + a_n^{n-1}a_1\alpha + a_n^{n-1}a_0 \\
&= a_n^{n-1}\left(a_n\alpha^n + a_{n-1}\alpha^{n-1} + a_{n-2}\alpha^{n-2} + \cdots + a_1\alpha + a_0\right) \\
&= a_n^{n-1}\cdot 0 \\
&= 0.
\end{aligned}$$

Exercise 3.81. Prove that $x^3 - nx + 2$ is irreducible for $n \neq -1, 3, 5$.

Solution 3.82. In a previous solution, we showed that if α is a rational root of a monic polynomial in $\mathbb{Z}[x]$, then α must be an integer. Now, suppose that $x^3 - nx + 2$ is not irreducible. Then $x^3 - nx + 2$ may be written as a product of a degree-1 polynomial $p(x)$ in $\mathbb{Q}[x]$ and a degree-2 element $q(x)$ in $\mathbb{Q}[x]$. But since $x^3 - nx + 2$ is a monic polynomial with integer coefficients, we find that the rational root of $p(x)$ must be an integer. Write

$$x^3 - nx + 2 = (x + z)\left(x^2 + \frac{a}{b}x + \frac{c}{d}\right)$$

where $a, b, c, d, z \in \mathbb{Z}$, and the fractions $\frac{a}{b}$ and $\frac{c}{d}$ are in lowest terms.

$$x^3 - nx + 2 = x^3 + \left(\frac{a}{b} + z\right)x^2 + \left(\frac{a}{b}z + \frac{c}{d}\right)x + \frac{cz}{d}.$$

Since $\frac{a}{b} + z$ vanishes, we find that $\frac{a}{b} = -z$. So, we find that:

$$x^3 - nx + 2 = x^3 + \left(-z^2 + \frac{c}{d}\right)x + \frac{cz}{d}.$$

Since

$$\frac{c}{d}z = 2,$$

we have that

$$\frac{c}{d} = \frac{2}{z}.$$

But since $-z^2 + \frac{c}{d}$ is an integer, we have that $\frac{c}{d}$ must be an integer. So, since $\frac{2}{z}$ must be an integer, we have that z must be in $\{-2, -1, 1, 2\}$. So, since the coefficient of x in

$$x^3 - nx + 2 = x^3 + \left(-z^2 + \frac{c}{d}\right) x + \frac{cz}{d}.$$

is equal to

$$-z^2 + \frac{c}{d} = -z^2 + \frac{2}{z}$$

and since z must be in $\{-2, -1, 1, 2\}$, we thus find that if $x^3 - nx + 2$ is reducible as an element in $\mathbb{Q}[x]$, then $x^3 - nx + 2$ must be one of the following polynomials:

$$x^3 - 5x + 2$$
$$x^3 - 3x + 2$$
$$x^3 + x + 2.$$

Contrapositively, if $x^3 - nx + 2$ is such that n is not in $\{-1, 3, 5\}$, then $x^3 - nx + 2$ is irreducible over $\mathbb{Q}$.

Exercise 3.83. Prove that $x^5 - ax - 1 \in \mathbb{Z}[x]$ is irreducible unless $a = 0, 2$ or -1. The first two correspond to linear factors, the third corresponds to the factorization $(x^2 - x + 1)(x^3 + x^2 - 1)$.

Solution 3.84. Assume that $x^5 - ax - 1$ is reducible. We first consider the case whereby $x^5 - ax - 1$ may be written as a product of a degree-1 polynomial $p(x)$ over $\mathbb{Q}$ and a degree-4 polynomial $q(x)$ in $\mathbb{Q}[x]$. We have previously shown that a rational root of a monic polynomial in $\mathbb{Z}[x]$ must be an integer. So, the unique root of the degree-1 polynomial $p(x)$ must be an integer, since the unique root of $p(x)$ must be a rational root of the monic polynomial $x^5 - ax - 1$. Write:

$$x^5 - ax - 1 = (x + z)\left(x^4 + q_3x^3 + q_2x^2 + q_1x + q_0\right),$$

where $z \in \mathbb{Z}$ and $q_0, q_1, q_2, q_3 \in \mathbb{Q}$. So, we find that:

$$x^5 - ax - 1 = x^5 + x^4(z + q_3) + (q_2 + q_3z)x^3 + (q_1 + q_2z)x^2 + (q_0 + q_1z)x + q_0z.$$

That is,

$$x^5 - ax - 1 = x^5 + (q_0 + q_1z)x + q_0z.$$

Since z is an integer, and since $q_0z = -1$, we have that $z \in \{-1, 1\}$. Writing $z = \pm 1$, we have that $q_0 = \mp 1$. We thus arrive at the following equality:

$$x^5 - ax - 1 = x^5 + (\mp 1 + q_1(\pm 1))x - 1.$$

Since $\mp 1 + q_1(\pm 1)$ is an integer, we have that q_1 must be an integer. Since $\pm 1 + q_3 = 0$, we have that $q_3 = \mp 1$. Since

$$q_2 + q_3(\pm 1) = 0$$

we have that

$$q_2 + (\mp 1)(\pm 1) = 0.$$

Therefore,

$$q_2 = 1.$$

Since

$$q_1 + q_2z = 0$$

we have that

$$q_1 + \pm 1 = 0$$

so that

$$q_1 = \mp 1.$$

So, from the equality whereby

$$x^5 - ax - 1 = x^5 + (\mp 1 + q_1(\pm 1))x - 1.$$

we thus obtain the following equation:

$$x^5 - ax - 1 = x^5 + (\mp 1 + (\mp 1)(\pm 1))x - 1.$$

Equivalently,

$$x^5 - ax - 1 = x^5 + (\mp 1 - 1)x - 1.$$

So, we find that $-a \in \{-2, 0\}$. That is, $a \in \{0, 2\}$.

Now suppose that $x^5 - ax - 1$ may be written as a product of a degree-2 polynomial $p(x)$ over $\mathbb{Q}$ and a degree-4 polynomial $q(x)$ over $\mathbb{Q}$. Write:

$$x^5 - ax - 1 = (x^2 + q_1 x + q_0)(x^3 + r_2 x^2 + r_1 x + r_0).$$

Equivalently,

$$x^5 - ax - 1 = q_0 r_0 + q_0 r_1 x + q_0 r_2 x^2 + q_0 x^3 + q_1 r_0 x + q_1 r_1 x^2 + q_1 r_2 x^3 + q_1 x^4 + r_0 x^2 + r_1 x^3 + r_2 x^4 + x^5.$$

That is,

$$x^5 - ax - 1 = x^5 + (q_1 + r_2)x^4 + (q_0 + q_1 r_2 + r_1)x^3 + (q_0 r_2 + q_1 r_1 + r_0)x^2 + (q_0 r_1 + q_1 r_0)x + q_0 r_0.$$

Since

$$-q_1 = r_2,$$

we have that:

$$x^5 - ax - 1 = x^5 + (q_0 - q_1^2 + r_1)x^3 + (-q_0 q_1 + q_1 r_1 + r_0)x^2 + (q_0 r_1 + q_1 r_0)x + q_0 r_0.$$

Since

$$r_0 = -\frac{1}{q_0}$$

we have that

$$q_0 \in \{-1, 1\},$$

with:

$$x^5 - ax - 1 = x^5 + (q_0 - q_1^2 + r_1)x^3 + (-q_0 q_1 + q_1 r_1 - \frac{1}{q_0})x^2 + (q_0 r_1 - \frac{q_1}{q_0})x - 1.$$

Since

$$r_1 = q_1^2 - q_0,$$

we find that:

$$x^5 - ax - 1 = x^5 + (-q_0 q_1 + q_1(q_1^2 - q_0) - \frac{1}{q_0})x^2 + (q_0(q_1^2 - q_0) - \frac{q_1}{q_0})x - 1$$

Since $q_0 \in \{-1, 1\}$, we may assume without loss of generality that $q_0 = 1$, with:

$$x^5 - ax - 1 = x^5 + (-q_1 + q_1(q_1^2 - 1) - 1)x^2 + ((q_1^2 - 1) - q_1)x - 1.$$

Now, q_1 must be an integer since $q_1^2 - q_1 - 1 = -a$. Since

$$-q_1 + q_1(q_1^2 - 1) - 1 = 0,$$

we have that

$$-q_1 + q_1(q_1^2 - 1) = 1,$$

so that $q_1 \in \{-1, 1\}$, since q_1 divides 1. From the above equality, we thus have that $q_1 = -1$. So, we have that

$$-a = q_1^2 - q_1 - 1$$

and that $q_1 = -1$, so that

$$a = -1$$

as desired.

3.10 Exercises from Section 13.2

Exercise 3.85. Let $\mathbb{F}$ be a finite field of characteristic p. Prove that $|\mathbb{F}| = p^n$ for some positive integer n.

Solution 3.86. Letting $\mathbb{F}$ be as given above, suppose that the cardinality of $\mathbb{F}$ is equal to $m \in \mathbb{N}$. Since $\mathbb{F}$ is of characteristic p, we have that the smallest natural number $\ell \in \mathbb{N}$ such that

$$\underbrace{1 + 1 + \cdots + 1}_{\ell} = 0$$

is such that $\ell = p$. So, we find that the following expressions are pairwise distinct, as elements in $\mathbb{F}$:

$$1, 1 + 1, \ldots, \underbrace{1 + 1 + \cdots + 1}_{\ell - 1}, 0.$$

It is possible that $\mathbb{F}$ consists precisely of the above expressions, in which case we find that $\mathbb{F}$ is of order p. Now, suppose that it is not the case that $\mathbb{F}$ consists only of the following expressions:

$$1, 1 + 1, \ldots, \underbrace{1 + 1 + \cdots + 1}_{p - 1}, 0.$$

So, suppose that $\mathbb{F}$ contains another element α, which is not equal to any of the above expressions. Since the underlying multiplicative group $\mathbb{F}^*$ of $\mathbb{F}$ is finite, we have that the order of $\alpha \neq 0$ as an element in $\mathbb{F}^*$ is finite. Let the order of $\alpha \in \mathbb{F}^*$ be denoted as $k_\alpha = k \in \mathbb{N}$. So, we find that minimal polynomial $m_{\alpha, \mathbb{Z}/p\mathbb{Z}}(x)$ of α over $\mathbb{Z}/p\mathbb{Z}$ is equal to $x^k - 1$. So, we have that

$$[(\mathbb{Z}/p\mathbb{Z})(\alpha) : \mathbb{Z}/p\mathbb{Z}] = k.$$

So, from the above equality, we have that the cardinality of $(\mathbb{Z}/p\mathbb{Z})(\alpha)$ is p^k. If $\mathbb{F}$ happens to be equal to $(\mathbb{Z}/p\mathbb{Z})(\alpha)$, then the cardinality of $\mathbb{F}$ is p^k. Otherwise, $\mathbb{F}$ must contain another element α' which is not in $(\mathbb{Z}/p\mathbb{Z})(\alpha)$. By repeating this argument inductively, we find that $\mathbb{F}$ must be of the form

$$(\mathbb{Z}/p\mathbb{Z})(\alpha, \alpha', \alpha'', \ldots, \alpha^{(r)}).$$

Since the order of $(\mathbb{Z}/p\mathbb{Z})(\alpha)$ is p^{k_α}, writing

$$[(\mathbb{Z}/p\mathbb{Z})(\alpha,\alpha') : (\mathbb{Z}/p\mathbb{Z})(\alpha)] = k_{\alpha'},$$

we have that the order of $(\mathbb{Z}/p\mathbb{Z})(\alpha,\alpha')$ must be $p^{k_\alpha k_{\alpha'}}$. Continuing in this manner inductively yields the desired result.

Exercise 3.87. Let $g(x) = x^2 + x - 1$ and let $h(x) = x^3 - x + 1$. Obtain fields of 4, 8, 9 and 27 elements by adjoining a root of $f(x)$ to the field F where $f(x) = g(x)$ or $h(x)$ and $F = \mathbb{F}_2$ or $\mathbb{F}_3$. Write down the multiplication tables for the fiels with 4 and 9 elements and show that the nonzero elements form a cyclic group.

Solution 3.88. We begin by letting $f(x) = g(x) = x^2 + x - 1$, and we let F be equal to $\mathbb{F}_2$. Let θ denote a fixed root of x^2+x-1. It is obvious that θ is not in $F = \mathbb{F}_2$, since $1^2+1-1 = -1$ and since $0^2+0-1 = -1$. Letting the elements of F be denoted so that $F = \{0,1\}$, it is clear that the field $F(\theta)$ consists precisely of the elements indicated below,

$$F(\theta) = \{0, 1, \theta, \theta^2 = \theta + 1\}.$$

Now, let $f(x) = h(x) = x^3 - x + 1$, and let $F = \mathbb{F}_2$. Let θ be a fixed root of $f(x) = h(x) = x^3 - x + 1 = x^3 + x + 1$. We claim that $x^3 - x + 1$ is irreducible over F. To show this, suppose that,

$$x^3 + x + 1 = (x^2 + ax + 1)(x + 1).$$

That is,

$$x^3 + x + 1 = x^3 + x^2(1 + a) + x(1 + a) + 1.$$

We have that $1 + a$ must be equal to 0, since the coefficient of x^2 on the right-hand side of

$$x^3 + x + 1 = x^3 + x^2(1 + a) + x(1 + a) + 1.$$

must be equal to 0, but we find that $1 + a$ must be equal to 1, thus yielding the desired contradiction. Letting θ denote a fixed root of $x^3 + x + 1$, we find that $x^3 + x + 1$ is the minimal polynomial of θ over F. So, since

$$[F(\theta) : F] = \deg\ m_\theta(x) = \deg\theta,$$

we find that

$$[F(\theta) : F] = 3,$$

so that the cardinality of $F(\theta)$ is equal to $2^3 = 8$.

Again let $f(x) = g(x) = x^2 + x - 1$. Now, let $F = \mathbb{F}_3$. Observe that as a polynomial over $F = \mathbb{F}_3$, we find that $f(x)$ is equal to $x^2 + x + 2$. We claim that $x^2 + x + 2$ is irreducible over $\mathbb{F}_3$. If

$$x^2 + x + 2 = (x + a)(x + b)$$

then

$$x^2 + x + 2 = x^2 + (a + b)x + ab.$$

Then $a + b = 1$, and $ab = 2$. If $a = 0$ and $b = 1$ or vice-versa, then $ab = 0$; if $a = 2$ and $b = 2$, then $ab = 1$. So, it is clear that $x^2 + x + 2$ is irreducible as an element in $F[x]$. So, letting θ be a root of this element in $\mathbb{F}_3[x]$, we find that the minimal polynomial of θ over $\mathbb{F}_3$ must be $x^2 + x + 2$. Since

$$[F(\theta) : F] = \deg m_\theta(x) = \deg\theta,$$

we have that

$$[F(\theta) : F] = 2,$$

so that the cardinality of $F(\theta)$ must be equal to $3^2 = 9$.

Now, let $f(x) = h(x) = x^3 - x + 1$, and let F denote the field $\mathbb{F}_3$. We claim that $x^3 - x + 1$ is irreducible over $\mathbb{F}_3$. Observe that $x^3 - x + 1$ is equivalent to $x^3 + 2x + 1$ in $\mathbb{F}_3[x]$. By way of contradiction, suppose that

$$x^3 + 2x + 1 = (x + a)(x^2 + bx + c),$$

so that

$$x^3 + 2x + 1 = x^3 + (a + b)x^2 + (ab + c)x + ac.$$

Since the expression $(a + b)x^2$ must vanish, we have that $-a = b$. We thus have that:

$$x^3 + 2x + 1 = x^3 + (-a^2 + c)x + ac.$$

It cannot be the case that $a = c = 1$, because the expression $(-a^2 + c)x$ cannot vanish. It cannot be the case that $a = c = 2$, because $-2^2 + 2 = -4 + 2 = -2 = 1$, modulo 3. We thus find that $x^3 + 2x + 1$ is irreducible as an element in $\mathbb{F}_3[x]$. Letting α denote a fixed roow of $x^3 + 2x + 1$, since

$$[F(\alpha)\ :\ F] = \deg\, m_\alpha(x) = \deg \alpha,$$

we find that

$$[F(\alpha)\ :\ F] = 3,$$

so that the cardinality of $F(\alpha)$ is $3^3 = 27$.

We have previously noted that in the case whereby $F = \mathbb{F}_2$ and $f(x) = g(x) = x^2 + x - 1$, we have that:

$$F(\theta) = \{0, 1, \theta, \theta^2 = \theta + 1\}.$$

So, from the above evaluation, we may compute the multiplication table for this order-4 field as follows.

$\circ$	0	1	θ	$\theta + 1$
0	0	0	0	0
1	0	1	θ	$\theta + 1$
θ	0	θ	$\theta + 1$	1
$\theta + 1$	0	$\theta + 1$	1	θ

Now, consider the multiplication table obtained by restricting the above composition table to the nonzero elements in $\mathbb{F}_2(\theta)$:

$\circ$	1	θ	$\theta + 1$
1	1	θ	$\theta + 1$
θ	θ	$\theta + 1$	1
$\theta + 1$	$\theta + 1$	1	θ

By comparing the above composition table with the following Cayley table for the additively cyclic group $\mathbb{Z}/3\mathbb{Z}$ of integers modulo 3, it is clear that $(\mathbb{F}_3(\theta))^* \cong \mathbb{Z}/3\mathbb{Z}$.

$\circ$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

We again consider the case whereby $f(x) = g(x) = x^2 + x - 1$ and $F = \mathbb{F}_3$. Letting θ denote a root of $f(x) = g(x) = x^2 + x - 1 \in \mathbb{F}_3[x]$, we have previously noted that the field $F(\theta)$ consists of 9 elements. We claim that the following expressions are pairwise distinct:

$$0, 1, 2, \theta, 2\theta, \theta + 1, \theta + 2, 2\theta + 1, 2\theta + 2.$$

The above expressions are all degree-0 or degree-1 polynomial expressions in terms of θ, and since the minimal polynomial for θ over F is quadratic, we have that it cannot be the case that two distinct expressions among

$$0, 1, 2, \theta, 2\theta, \theta + 1, \theta + 2, 2\theta + 1, 2\theta + 2$$

can be equal. Observe that since $\theta^2 + \theta - 1 = 0$, we have that $\theta^2 = 2\theta + 1$.

$\circ$	0	1	2	θ	2θ	$\theta+1$	$\theta+2$	$2\theta+1$	$2\theta+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	θ	2θ	$\theta+1$	$\theta+2$	$2\theta+1$	$2\theta+2$
2	0	2	1	2θ	θ	$2\theta+2$	$2\theta+1$	$\theta+2$	$\theta+1$
θ	0	θ	2θ	$2\theta+1$	$\theta+2$	1	$\theta+1$	$2\theta+2$	2
2θ	0	2θ	θ	$\theta+2$	$2\theta+1$	2	$2\theta+2$	$\theta+1$	1
$\theta+1$	0	$\theta+1$	$2\theta+2$	1	2	$\theta+2$	2θ	θ	$2\theta+1$
$\theta+2$	0	$\theta+2$	$2\theta+1$	$\theta+1$	$2\theta+2$	2θ	2	1	θ
$2\theta+1$	0	$2\theta+1$	$\theta+2$	$2\theta+2$	$\theta+1$	θ	1	2	2θ
$2\theta+2$	0	$2\theta+2$	$\theta+1$	2	1	$2\theta+1$	θ	2θ	$\theta+2$

Now, to show that the nonzero elements in the field of order 9 illustrated above forms a cyclic group, it suffices to find a nonzero element which is of order 8 with respect to the underlying multiplicative binary operation on this field. It is obvious that this element cannot be in $\{0, 1, 2\}$. We proceed to apply a brute-force approach towards the problem of finding an element of this form, as suggested by the following computations.

$$\begin{aligned}
\theta^2 &= 2\theta + 1 \\
\theta^3 &= \theta(2\theta + 1) \\
&= 2\theta^2 + \theta \\
&= 2(2\theta + 1) + \theta \\
&= 4\theta + 2 + \theta \\
&= 5\theta + 2 \\
&= 2\theta + 2 \\
\theta^4 &= \theta(2\theta + 2) \\
&= 2\theta^2 + 2\theta \\
&= 2(2\theta + 1) + 2\theta \\
&= 4\theta + 2 + 2\theta \\
&= 6\theta + 2 \\
&= 2 \\
\theta^5 &= 2\theta \\
\theta^6 &= 2\theta^2
\end{aligned}$$

$$
\begin{aligned}
&= 2(2\theta + 1)\\
&= 4\theta + 2\\
&= \theta + 2\\
\theta^7 &= \theta(\theta + 2)\\
&= \theta^2 + 2\theta\\
&= 2\theta + 1 + 2\theta\\
&= 4\theta + 1\\
&= \theta + 1\\
\theta^8 &= \theta(\theta + 1)\\
&= \theta^2 + \theta\\
&= 2\theta + 1 + \theta\\
&= 1.
\end{aligned}
$$

So, since the multiplicative order of θ is 8, and since there are a total of 8 nonzero elements in $F(\theta)$, we have that the nonzero elements in $F(\theta)$ form a cyclic group of order 8.

Exercise 3.89. Determine the minimal polynomial over $\mathbb{Q}$ for the element $1 + i$.

Solution 3.90. Letting i denote the imaginary unit, consider the expression $(1 + i)^2$. By the binomial theorem, we find that:

$$(1 + i)^2 = 1 + 2i + i^2.$$

Equivalently,

$$(1 + i)^2 = 2i.$$

Rewrite the above equality in the following manner:

$$(1 + i)^2 = 2i + 2 - 2.$$

Equivalently,

$$(1 + i)^2 = 2(i + 1) - 2.$$

Therefore,

$$(1 + i)^2 - 2(i + 1) + 2 = 0.$$

So, we find that the expression $1 + i$ must be a root of the following polynomial:

$$x^2 - 2x + 2 = 0.$$

The discriminant corresponding to the above quadratic equation is: -4. Consequently, the quadratic polynomial $x^2 - 2x + 2$ is irreducible as an element in $\mathbb{Q}[x]$. Since $1 + i$ is a root of the irreducible polynomial $x^2 - 2x + 2$, which is in $\mathbb{Q}[x]$, it is clear that the minimal polynomial over $\mathbb{Q}$ for the element $1 + i$ is $x^2 - 2x + 2$.

Exercise 3.91. Determine the degree over $\mathbb{Q}$ of $2 + \sqrt{3}$ and of $1 + \sqrt[3]{2} + \sqrt[3]{4}$.

Solution 3.92. To evaluate the degree over $\mathbb{Q}$ of $2+\sqrt{3}$, we begin by evaluating the expression $(2+\sqrt{3})^2$ in the following manner:

$$(2 + \sqrt{3})^2 = 7 + 4\sqrt{3}.$$

Now, consider the following equality:

$$\left(2+\sqrt{3}\right)^2-4\left(2+\sqrt{3}\right)=-1.$$

We thus obtain the following equality:

$$\left(2+\sqrt{3}\right)^2-4\left(2+\sqrt{3}\right)+1=0.$$

We thus find that $2+\sqrt{3}$ is a root of the following polynomial:

$$x^2-4x+1\in\mathbb{Q}[x].$$

Since the discriminant of $x^2-4x+1\in\mathbb{Q}[x]$ is equal to 12, it is clear that this polynomial is irreducible as an element in $\mathbb{Q}[x]$. So, we find that the degree over $\mathbb{Q}$ of $2+\sqrt{3}$ is equal to $2=\deg(x^2-4x+1)$. We make use of a similar approach to compute the degree over $\mathbb{Q}$ of $1+\sqrt[3]{2}+\sqrt[3]{4}$. Rewrite the expression

$$\left(1+\sqrt[3]{2}+2^{2/3}\right)^3+a\left(1+\sqrt[3]{2}+2^{2/3}\right)^2+b\left(1+\sqrt[3]{2}+2^{2/3}\right)+c$$

as follows:

$$(5a+b+c+19)+(4a+b+0c+15)\sqrt[3]{2}+(3a+b+0c+12)2^{2/3}.$$

Now, suppose that the above expression vanishes. We thus arrive at the following system of equations:

$$\begin{aligned}
&5a+b+c+19=0,\\
&4a+b+0\times c+15=0,\\
&3a+b+0\times c+12=0.
\end{aligned}$$

Equivalently,

$$\begin{aligned}
&5\times a+1\times b+1\times c=-19,\\
&4\times a+1\times b+0\times c=-15,\\
&3\times a+1\times b+0\times c=-12.
\end{aligned}$$

In matrix form, we have that:

$$\begin{bmatrix}5&1&1\\4&1&0\\3&1&0\end{bmatrix}\begin{bmatrix}a\\b\\c\end{bmatrix}=\begin{bmatrix}-19\\-15\\-12\end{bmatrix}.$$

Equivalently,

$$\begin{bmatrix}a\\b\\c\end{bmatrix}=\begin{bmatrix}0&1&-1\\0&-3&4\\1&-2&1\end{bmatrix}\begin{bmatrix}-19\\-15\\-12\end{bmatrix}.$$

Therefore,

$$\begin{bmatrix}a\\b\\c\end{bmatrix}=\begin{bmatrix}-3\\-3\\-1\end{bmatrix}.$$

So, we have thus far shown that $1+\sqrt[3]{2}+2^{2/3}$ is a root of the polynomial:

$$x^3-3x^2-3x-1\in\mathbb{Q}[x].$$

By way of contradiction, suppose that x^3-3x^2-3x-1 is not irreducible as an element in $\mathbb{Q}[x]$. From this assumption, we find that x^3-3x^2-3x-1 may be written as a product of a degree-1 monic polynomial $p(x)$ in $\mathbb{Q}[x]$ and a degree-2 monic polynomial in $\mathbb{Q}[x]$. Upon inspection of the graph of x^3-3x^2-3x-1, we find that x^3-3x^2-3x-1 has only one real root. Since $1+\sqrt[3]{2}+2^{2/3}$ is a root of this polynomial, we have that $1+\sqrt[3]{2}+2^{2/3}$ is the unique real root of this polynomial. So, we have that $1+\sqrt[3]{2}+2^{2/3}$ must be a root of $p(x)$, which is impossible, since $p(x)$ is a degree-1 polynomial in $\mathbb{Q}[x]$, if we accept that $1+\sqrt[3]{2}+2^{2/3}$ is irrational. Alternatively, one may make use of the fact that a rational root of a monic polynomial in $\mathbb{Z}[x]$ must be an integer.

Exercise 3.93. Let $F=\mathbb{Q}(i)$. Prove that x^3-2 and x^3-3 are irreducible over F.

Solution 3.94. By way of contradiction, suppose that it is not the case that x^3-2 is irreducible over $F=\mathbb{Q}(i)$. We thus have that x^3-2 may be written as a product of a monic degree-1 polynomial in $(\mathbb{Q}(i))[x]$ and a monic degree-2 polynomial in $(\mathbb{Q}(i))[x]$, as indicated below, letting $a,b,c,d,e,f\in\mathbb{Q}$:

$$x^3-2=(x+(a+ib))\left(x^2+x(c+id)+(e+if)\right).$$

We thus find that x^3-2 is equal to:

$$x^3+(a+c+i(b+d))x^2+(ac+ibc+iad-bd+e+if)x+(ae+ibe+iaf-bf)$$

So, $c=-a$, and $d=-b$:

$$x^3+(-a^2-i2ab+b^2+e+if)x+(ae+ibe+iaf-bf)$$

Therefore, $a^2-b^2=e$. Similarly, $f=2ab$. Since

$$ae-bf=-2$$

we have that

$$a(a^2-b^2)-b(2ab)=-2.$$

Equivalently,

$$a^3-3ab^2=-2.$$

Also, since $be+af=0$, we have that

$$b(a^2-b^2)+a(2ab)=0,$$

so that

$$3a^2b-b^3=0.$$

Since a is rational, and since

$$a^3-3ab^2=-2,$$

we have that b is nonzero. So we have that

$$3a^2=b^2.$$

But this is impossible, since the above equality implies that

$$\sqrt{3}a=b,$$

which is impossible, since a and b are both in $\mathbb{Q}$. An identical argument may be applied for the other given polynomial.

Exercise 3.95. Prove directly from the definitions that the field $F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is the composite of the fields $F(\alpha_1)$, $F(\alpha_2)$, ..., $F(\alpha_n)$.

Solution 3.96. We begin by presenting the following definition from the class textbook:

"**Definition.** Let K_1 and K_2 be two subfields of a field K. Then the *composite field* of K_1 and K_2, denoted K_1K_2, is the smallest subfield of K containing both K_1 and K_2. Similarly, the composite of any collection of subfields of K is the smallest subfield containing all the subfields." (p. 528)

Since it was not specified otherwise, we may assume without loss of generality that there exists an extension K of the field K such that $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$. By definition, we have that the smallest subfield of K containing both F and the elements α_1, α_2, ..., α_n is $F(\alpha_1, \alpha_2, \ldots, \alpha_n)$. In a similar fashion, we have that the compositie

$$F(\alpha_1)F(\alpha_2)\cdots F(\alpha_n)$$

of the fields $F(\alpha_1)$, $F(\alpha_2)$, ..., $F(\alpha_n)$, is precisely the smallest subfield of K containing: $F(\alpha_1)$, $F(\alpha_2)$, ..., $F(\alpha_n)$. Using these definitions, we must prove that:

$$F(\alpha_1, \alpha_2, \ldots, \alpha_n) = F(\alpha_1)F(\alpha_2)\cdots F(\alpha_n).$$

Since $F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is a subfield of K containing α_i and F, for each index i, and since $F(\alpha_i)$ the smallest subfield of K containing α_i and F, we have that:

$$F(\alpha_1, \alpha_2, \ldots, \alpha_n) \supseteq F(\alpha_i).$$

Now, since $F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is a subfield of K containing $F(\alpha_1)$, $F(\alpha_2)$, ..., $F(\alpha_n)$, and since $F(\alpha_1)F(\alpha_2)\cdots F(\alpha_n$ is the smallest subfield of K containing $F(\alpha_1)$, $F(\alpha_2)$, ..., $F(\alpha_n)$, we thus arrive at the following inclusion:

$$F(\alpha_1, \alpha_2, \ldots, \alpha_n) \supseteq F(\alpha_1)F(\alpha_2)\cdots F(\alpha_n).$$

Certainly, the composite field $F(\alpha_1)F(\alpha_2)\cdots F(\alpha_n)$ is a subfield of K containing both F and the elements α_1, α_2, ..., α_n. But, by definition, we have that $F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is the smallest subfield of K containing both F and the elements α_1, α_2, ..., α_n, thus proving the reverse inclusion whereby

$$F(\alpha_1, \alpha_2, \ldots, \alpha_n) \subseteq F(\alpha_1)F(\alpha_2)\cdots F(\alpha_n),$$

as desired.

Exercise 3.97. Prove that $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ [one inclusion is obvious, for the other consider $(\sqrt{2} + \sqrt{3})^2$, etc.]. Concluse that $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = 4$. Find an irreducible polynomial satisfied by $\sqrt{2} + \sqrt{3}$.

Solution 3.98. Since $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is the field generated by $\{\sqrt{2}, \sqrt{3}\}$ over $\mathbb{Q}$, we have that $\sqrt{2} + \sqrt{3}$ is in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, so that

$$\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}).$$

To prove the reverse inclusion, we begin by considering the expression $(\sqrt{2} + \sqrt{3})^3$. Expanding this expression using the binomial theorem, we find that:

$$\left(\sqrt{2} + \sqrt{3}\right)^3 = 11\sqrt{2} + 9\sqrt{3}.$$

Therefore,

$$-\frac{1}{2}\left(\sqrt{2}+\sqrt{3}\right)^3+\frac{11}{2}\left(\sqrt{2}+\sqrt{3}\right)=\sqrt{3}.$$

This proves that $\sqrt{3}$ is in $\mathbb{Q}(\sqrt{2}+\sqrt{3})$. In a somewhat similar fashion, we find that:

$$\frac{1}{2}\left(\sqrt{2}+\sqrt{3}\right)^3-\frac{9}{2}\left(\sqrt{2}+\sqrt{3}\right)=\sqrt{2}.$$

We accordingly deduce that $\sqrt{2}\in\mathbb{Q}(\sqrt{2}+\sqrt{3})$. So, since $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ which contains each element in $\mathbb{Q}$ and which contains $\sqrt{2}$ and $\sqrt{3}$, we find that each element in $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ must be in $\mathbb{Q}(\sqrt{2},\sqrt{3})$, thus proving the reverse inclusion whereby:

$$\mathbb{Q}(\sqrt{2}+\sqrt{3})\supseteq\mathbb{Q}(\sqrt{2},\sqrt{3}).$$

We thus arrive at the following equality:

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

Now, to compute the dimension of $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ as a $\mathbb{Q}$-vector space, it remains to compute the dimension of $\mathbb{Q}(\sqrt{2},\sqrt{3})$ as a vector space over $\mathbb{Q}$. We thus proceed to consider the following tower of fields.

$$\begin{tikzcd}
\mathbb{Q}(\sqrt{2},\sqrt{3}) \arrow[d, dash] \\
\mathbb{Q}(\sqrt{2}) \arrow[d, dash] \\
\mathbb{Q}
\end{tikzcd}$$

Since the minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $m_{\sqrt{2},\mathbb{Q}}(x)=x^2-2$, we find that:

$$[\mathbb{Q}(\sqrt{2})\ :\ \mathbb{Q}]=\deg(m_{\sqrt{2},\mathbb{Q}}(x))=2.$$

Now, consider the minimal polynomial of $\sqrt{3}$ over $\mathbb{Q}(\sqrt{2})$. Since $\sqrt{3}$ satisfies the degree-2 polynomial x^2-3 over $\mathbb{Q}(\sqrt{2})$, and since elements in $\mathbb{Q}(\sqrt{2})$ are of the form $a+b\sqrt{2}$ for rational numbers a and b, it is evident that

$$m_{\sqrt{3},\mathbb{Q}(\sqrt{2})}(x)=x^2-3,$$

so that

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

We thus find that:

$$[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]=[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2\times2=4.$$

So, we thus arrive at the following:

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

Letting $a, b, c, d \in \mathbb{Q}$, assume that the following expression vanishes:

$$\left(\sqrt{2}+\sqrt{3}\right)^4 + a\left(\sqrt{2}+\sqrt{3}\right)^3 + b\left(\sqrt{2}+\sqrt{3}\right)^2 + c\left(\sqrt{2}+\sqrt{3}\right) + d.$$

Equivalently,

$$49 + 20\sqrt{6} + 11\sqrt{2}a + 9\sqrt{3}a + 5b + 2\sqrt{6}b + \sqrt{2}c + \sqrt{3}c + d.$$

Equivalently,

$$(11a + c)\sqrt{2} + (9a + c)\sqrt{3} + (2b + 20)\sqrt{6} + 5b + d + 49 = 0.$$

Therefore,

$$(11a + c)\sqrt{2} + (9a + c)\sqrt{3} + (2b + 20)\sqrt{6} + 5b + d = -49.$$

So, we arrive at the following system of equations, presented in matrix form:

$$\begin{bmatrix} 11 & 0 & 1 & 0 \\ 9 & 0 & 1 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 5 & 0 & 1 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ -20 \\ -49 \end{bmatrix}.$$

Since the 4×4 matrix given in the above equality is invertible, we have that:

$$\begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix} = \begin{bmatrix} 11 & 0 & 1 & 0 \\ 9 & 0 & 1 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 5 & 0 & 1 \end{bmatrix}^{-1} \begin{bmatrix} 0 \\ 0 \\ -20 \\ -49 \end{bmatrix}.$$

Equivalently,

$$\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} 0 \\ -10 \\ 0 \\ 1 \end{pmatrix}.$$

So, we may deduce that $\sqrt{2}+\sqrt{3}$ is a root of the following degree-4 polynomial:

$$x^4 - 10x^2 + 1.$$

That is,

$$\left(\sqrt{2}+\sqrt{3}\right)^4 - 10\left(\sqrt{2}+\sqrt{3}\right)^2 + 1 = 0.$$

Since

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

we find that the degre of the minimal polynomial of $\sqrt{2}+\sqrt{3}$ over $\mathbb{Q}$ is 4. So, since $x^4 - 10x^2 + 1$ is a monic degree-4 polynomial over $\mathbb{Q}$ with $\sqrt{2}+\sqrt{3}$ as a root, we may accordingly deduce that $m_{\sqrt{2}+\sqrt{3},\mathbb{Q}}(x)$ is equal to $x^4 - 10x^2 + 1$.

Exercise 3.99. Let F be a field of characteristic $\neq 2$. Let D_1 and D_2 be elements of F, neither of which is a square in F. Prove that $F(\sqrt{D_1}, \sqrt{D_2})$ is of degree 4 over F if $D_1 D_2$ is not a square in F and is of degree 2 over F otherwise. When $F(\sqrt{D_1}, \sqrt{D_2})$ is of degree 3 over F the field is called a *biquadratic extension of* F.

Solution 3.100. Letting F, D_1, and D_2 be as given above, first suppose that D_1D_2 is not a square in F. We proceed to consider the following tower of fields.

$$\begin{tikzcd}
F(\sqrt{D_1}, \sqrt{D_2}) \arrow[d, dash] \\
F(\sqrt{D_1}) \arrow[d, dash] \\
F
\end{tikzcd}$$

Now, consider the dimension of $F(\sqrt{D_1})$ as a vector space over F. Recall that D_1 is not a square in F. We thus have that $\sqrt{D_1}$ is not an element in F. Therefore, $F(\sqrt{D_1})$ is not equal to F. That is, $[F(\sqrt{D_1}) : F]$ is not equal to 1. Now, observe that $\sqrt{D_1}$ is a root of the polynomial $x^2 - D_1 \in F[x]$. Since $\sqrt{D_1}$ cannot be a root of a degree-1 polynomial in $F[x]$, and since $\sqrt{D_1}$ is a root of the degree-2 polynomial

$$x^2 - D_1 \in F[x],$$

we may accordingly deduce that the minimal polynomial $m_{\sqrt{D_1},F}(x)$ of $\sqrt{D_1}$ over F is equal to $x^2 - D_1 \in F[x]$. We thus find that:

$$[F(\sqrt{D_1}) : F] = \deg(m_{\sqrt{D_1},F}(x)) = 2.$$

Now, consider the dimension of $F(\sqrt{D_1}, \sqrt{D_2})$ as a vector space over $F(\sqrt{D_1})$. Recall that we are working under the assumption that D_1D_2 is not a square in F. We thus have that D_1 and D_2 must be distinct. Observe that $\sqrt{D_2}$ is a root of the polynomial $x^2 - D_2 \in F(\sqrt{D_1})[x]$.

By way of contradiction, suppose that $\sqrt{D_2}$ is also a root of a degree-1 polynomial in $F(\sqrt{D_1})[x]$, i.e., that $\sqrt{D_2}$ is in $F(\sqrt{D_1})$. We thus have that $\sqrt{D_2}$ may be written as $f_1 + f_2\sqrt{D_1}$, letting f_1 and f_2 be elements in F. Since

$$\sqrt{D_2} = f_1 + f_2\sqrt{D_1},$$

we find that

$$D_2 = \left(f_1 + f_2\sqrt{D_1}\right)^2,$$

so that

$$D_2 = f_1^2 + 2f_1f_2\sqrt{D_1} + f_2^2D_1.$$

Equivalently,

$$D_2 - f_1^2 - f_2^2D_1 = 2f_1f_2\sqrt{D_1}.$$

Observe that the expression 2 does not vanish in F, under our assumption that F is not of characteristic 2. We claim that f_1 is nonzero, because otherwise, we would have that

$$D_2 = f_2^2D_1,$$

so that

$$D_1D_2 = f_2^2D_1^2,$$

which is impossible, since D_1D_2 is not a square in F. A symmetric argument shows that f_2 is nonzero. Since f_1 and f_2 are both nonzero elements in the field F, and since the field F is not of characteristic 2, we thus obtain the equality whereby

$$\frac{1}{2} \cdot \frac{1}{f_1} \cdot \frac{1}{f_2} \cdot \left(D_2 - f_1^2 - f_2^2D_1\right) = \sqrt{D_1}.$$

But this contradicts that D_1 is not a square in F.

So, we have thus far shown that $\sqrt{D_2}$ is a root of the degree-2 polynomial $x^2 - D_2 \in F(\sqrt{D_1})[x]$, and that $\sqrt{D_2}$ is not a root of any degree-1 polynomial in $F(\sqrt{D_1})[x]$. Accordingly, we deduce that the minimal polynomial $m_{\sqrt{D_2},F(\sqrt{D_1})}(x)$ of $\sqrt{D_2}$ over $F(\sqrt{D_1})$ is equal to $x^2 - D_2 \in F(\sqrt{D_1})[x]$. We thus find that:

$$[F(\sqrt{D_1},\sqrt{D_2}) : F(\sqrt{D_1})] = \deg(m_{\sqrt{D_2},F(\sqrt{D_1})}(x)) = 2.$$

So, we find that:

$$[F(\sqrt{D_1},\sqrt{D_2}) : F(\sqrt{D_1})][F(\sqrt{D_1}) : F] = 2 \cdot 2,$$

as desired.

Now, suppose that D_1D_2 is a square in F. By repeating a previous argument, we find that $[F(\sqrt{D_1}) : F] = 2$. Now, consider the degree of $F(\sqrt{D_1},\sqrt{D_2})$ over $F(\sqrt{D_1})$. Suppose that $D_1D_2 = f^2$, letting f be an element in F. Since D_1 is not a square in F, we have that D_1 is nonzero. So, we have that:

$$D_2 = \frac{f^2}{D_1}.$$

Therefore,

$$\sqrt{D_2} = \frac{f}{\sqrt{D_1}} \in F(\sqrt{D_1}).$$

Since $\sqrt{D_2}$ is in $F(\sqrt{D_2})$, it is clear that $F(\sqrt{D_1})(\sqrt{D_2})$ must be equal to $F(\sqrt{D_1})$, so that

$$[F(\sqrt{D_1},\sqrt{D_1}) : F(\sqrt{D_1})][F(\sqrt{D_1}) : F] = 1 \cdot 2 = 2,$$

as desired.

Exercise 3.101. Let F be a field of characteristic $\neq 2$. Let a, b be elements of the field F with b not a square in F. Prove that a necessary and sufficient condition for $\sqrt{a+\sqrt{b}} = \sqrt{m} + \sqrt{n}$ for some m and n in F is that $a^2 - b$ is a square in F. Use this to determine when the field $\mathbb{Q}(\sqrt{a+\sqrt{b}})$ $(a, b \in \mathbb{Q})$ is biquadratic over $\mathbb{Q}$.

Solution 3.102. ($\Longrightarrow$) First suppose that there exist elements m and n in F such that $\sqrt{a+\sqrt{b}} = \sqrt{m}+\sqrt{n}$, letting F be as given above, as a field such that the characteristic of F is not equal to 2, with a and b as elements in F. By squaring both sides of the equation

$$\sqrt{a+\sqrt{b}} = \sqrt{m} + \sqrt{n},$$

we obtain the equality whereby

$$a + \sqrt{b} = m + n + 2\sqrt{mn}.$$

Observe that since the field F is such that the characteristic of F is not equal to 2, we have that the expression $2\sqrt{mn}$ does not vanish. The vanishing of $2\sqrt{mn}$ would contradict that $\sqrt{b} \notin F$. So, we obtain the equality given below, where the expression $\sqrt{4mn}$ cannot be equal to 0:

$$a + \sqrt{b} = m + n + \sqrt{4mn}.$$

Since a, m, and n are elements in the base field F, and since $\sqrt{b}$ is not in F, we have that $\sqrt{4mn}$ is not in F. So, by considering both sides of the equality

$$a + \sqrt{b} = m + n + \sqrt{4mn}$$

in terms of an F-basis for some appropriate algebraic extension of F, we may conclude that

$$a = m + n$$

and that

$$\sqrt{b} = \sqrt{4mn},$$

with

$$b = 4mn.$$

Now, consider the expression $a^2 - b$. We have that

$$a^2 - b = (m+n)^2 - 4mn,$$

so that

$$a^2 - b = m^2 - 2mn + n^2 = (m-n)^2 = (n-m)^2$$

thus proving that $a^2 - b$ is a square with respect to the field F.

($\Longleftarrow$) Conversely, assume that $a^2 - b$ is a square with respect to the field F. So, there exists some element f in F such that

$$a^2 - b = f^2.$$

Now, letting m and n denote indeterminates in F, consider the following system of linear equations:

$$m - n = f$$
$$m + n = a.$$

It is natural to appeal to the fact that the characteristic of F is not equal to 2. Adding the equations $m - n = f$ and $m + n = a$, we find that

$$2m = f + a,$$

with $2 \in F$ as a unit in F, i.e., with $2 \in F$ as an invertible element in F. Since 2 is a unit in F, from the equality

$$2m = f + a$$

we find that

$$m = \frac{1}{2}(f + a).$$

By subtracting the equation $m - n = f$ from $m + n = a$, we have that

$$2n = a - f.$$

Again since the element $2 \in F$ is a unit in F, we have that

$$n = \frac{1}{2}(a - f).$$

So, we have shown that there exist elements m and n in F such that:

$$m - n = f$$
$$m + n = a.$$

From the equality

$$a^2 - b = f^2,$$

we have that

$$a^2 - b = (m - n)^2.$$

We thus have that

$$a^2 - b = m^2 - 2mn + n^2.$$

Equivalently,

$$a^2 - b = m^2 + 2mn + n^2 - 4mn.$$

That is,

$$a^2 - b = (m + n)^2 - 4mn.$$

But we also have that $a = m + n$, which shows that

$$b = 4mn,$$

so that

$$\sqrt{b} = \sqrt{4mn}.$$

Since a is equal to $m + n$, we have that

$$a + \sqrt{b} = m + n + 2\sqrt{mn}.$$

Equivalently,

$$a + \sqrt{b} = (\sqrt{m} + \sqrt{n})^2,$$

so that

$$\sqrt{a + \sqrt{b}} = \sqrt{m} + \sqrt{n},$$

as desired.

We thus proceed to apply the above results to determine when the field $\mathbb{Q}(\sqrt{a + \sqrt{b}})$ $(a, b \in \mathbb{Q})$ is biquadratic over $\mathbb{Q}$.

First of all, if b is a square, then we have that $a + \sqrt{b}$ is an element in $\mathbb{Q}$, so that the extension field $\mathbb{Q}(\sqrt{a + \sqrt{b}})$ in this case is an extension of $\mathbb{Q}$ of degree 2. In this trivial case, the extension $\mathbb{Q}(\sqrt{a + \sqrt{b}})$ is not biquadratic, since a biquadratic extension from a base field must be of degree 4.

Now, assume that b is not a square. Given elements x and y in $\mathbb{Q}$ such that $\sqrt{x} + \sqrt{y}$ is not in $\mathbb{Q}$, consider the field $\mathbb{Q}(\sqrt{x} + \sqrt{y})$. Since

$$(\sqrt{x} + \sqrt{y})(\sqrt{x} - \sqrt{y}) = x - y \in \mathbb{Q},$$

and since $\sqrt{x} + \sqrt{y}$ is not an element in $\mathbb{Q}$, we have that

$$\sqrt{x} - \sqrt{y} = \frac{x - y}{\sqrt{x} + \sqrt{y}} \in \mathbb{Q}\left(\sqrt{x} + \sqrt{y}\right).$$

Since $\sqrt{x} + \sqrt{y}$ and $\sqrt{x} - \sqrt{y}$ are both elements in $\mathbb{Q}\left(\sqrt{x} + \sqrt{y}\right)$, we have that $\sqrt{x}$ and $\sqrt{y}$ are both in $\mathbb{Q}\left(\sqrt{x} + \sqrt{y}\right)$, so we have that:

$$\mathbb{Q}(\sqrt{x}, \sqrt{y}) \subseteq \mathbb{Q}\left(\sqrt{x} + \sqrt{y}\right).$$

Conversely, we have that an arbitrary expression of the form

$$q_1 + q_2 \left(\sqrt{x} + \sqrt{y} \right)$$

for elements $q_1, q_2 \in \mathbb{Q}$, we have that

$$q_1 + q_2 \left(\sqrt{x} + \sqrt{y} \right) = q_1 + q_2\sqrt{x} + q_2\sqrt{y} \in \mathbb{Q}(\sqrt{x}, \sqrt{y}),$$

thus establishing the reverse inclusion whereby:

$$\mathbb{Q}(\sqrt{x}, \sqrt{y}) \supseteq \mathbb{Q} \left(\sqrt{x} + \sqrt{y} \right).$$

We have thus proven the following proposition.

Proposition 3.103. *Given elements x and y in $\mathbb{Q}$ such that $\sqrt{x} + \sqrt{y}$ is not in $\mathbb{Q}$,*

$$\mathbb{Q}(\sqrt{x}, \sqrt{y}) = \mathbb{Q} \left(\sqrt{x} + \sqrt{y} \right).$$

Now, recall that we are currently considering the case whereby b is not a square. From our previous results, we have that there exist rational numbers m and n such that

$$\sqrt{a + \sqrt{b}} = \sqrt{m} + \sqrt{n}$$

if and only if $a^2 - b$ is a square in $\mathbb{Q}$. But since we are working under the assumption that b is not a square, we have that there exist rational numbers m and n such that

$$\sqrt{a + \sqrt{b}} = \sqrt{m} + \sqrt{n}$$

if and only if there exist rational numbers m and n such that $\sqrt{m} + \sqrt{n} \notin \mathbb{Q}$ and

$$\sqrt{a + \sqrt{b}} = \sqrt{m} + \sqrt{n}.$$

So, we have that there exist rational numbers m and n such that

$$\mathbb{Q}(\sqrt{m}, \sqrt{n}) = \mathbb{Q}(\sqrt{a + \sqrt{b}})$$

if and only if $a^2 - b$ is a square in $\mathbb{Q}$. Since we are working under the assumption that b is not a square, we have that there exist non-square rational numbers m and n such that

$$\mathbb{Q}(\sqrt{m}, \sqrt{n}) = \mathbb{Q}(\sqrt{a + \sqrt{b}})$$

if and only if $a^2 - b$ is a square in $\mathbb{Q}$, in which case

$$m = \frac{1}{2} \left(a \pm \sqrt{a^2 - b} \right)$$

and

$$n = \frac{1}{2} \left(a \mp \sqrt{a^2 - b} \right).$$

So, from our results given in the previous exercise, we have that $\mathbb{Q}(\sqrt{a + \sqrt{b}})$ is a biquadratic extension of $\mathbb{Q}$ if and only if: $a^2 - b$ is a square in $\mathbb{Q}$ and $\frac{b}{4}$ is not a square in $\mathbb{Q}$. But recall that we let b be such that b is not a square in $\mathbb{Q}$. We may conclude that: $\mathbb{Q}(\sqrt{a + \sqrt{b}})$ is a biquadratic extension of $\mathbb{Q}$ if and only if: b is not a square in $\mathbb{Q}$ and $a^2 - b$ is a square in $\mathbb{Q}$.

3.11 Exercises from Section 13.3

Problem 3.104. Prove that it is impossible to construct the regular 9-gon.

Solution 3.105. We begin by observing that each interior angle within a regular 9-gon is equal to $\left(\frac{360}{9}\right)^{\circ}$. That is, each interior angle within a regular 9-gon is equal to 40°. As discussed in the class textbook, if an angle θ can be constructed using a compass and straightedge, then $\cos(\theta)$ can also be constructed. Conversely, if $\cos(\theta)$ can be constructed, then the angle θ can be constructed. The following fundamental result concerning straightedge and compass constructions is taken from the class textbook, Dummit and Foote's *Abstract Algebra*:

"**Proposition 23.** If the element $\alpha \in \mathbb{R}$ is obtained from a field $F \subset \mathbb{R}$ be a series of compass and straightedge constructions then $[F(\alpha) : F] = 2^k$ for some integer $k \geq 0$." (p. 533)

Now, by way of contradiction, suppose that it is possible to construct a regular 9-gon. In order to construct a regular 9-gon using a straightedge and compass, one would need to construct angles of the form $\frac{2\pi}{9}$. So, from our initial assumption, we have that the angle $\frac{2\pi}{9}$ is constructible. Equivalently, $\cos\left(\frac{2\pi}{9}\right)$ is constructible. By the triple angle formula for the cosine function, we find that:

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

for an input angle α. We thus have that:

$$\cos\left(\frac{2\pi}{3}\right) = 4\cos^3\left(\frac{2\pi}{9}\right) - 3\cos\left(\frac{2\pi}{9}\right).$$

Equivalently,

$$-\frac{1}{2} = 4\cos^3\left(\frac{2\pi}{9}\right) - 3\cos\left(\frac{2\pi}{9}\right).$$

So, we find that $\cos\left(\frac{2\pi}{9}\right)$ is a root of the following polynomial:

$$4x^3 - 3x + \frac{1}{2} \in \mathbb{Q}[x].$$

Equivalently, $\cos\left(\frac{2\pi}{9}\right)$ is a root of the following polynomial:

$$8x^3 - 6x + 1 \in \mathbb{Q}[x].$$

We claim that the above polynomial is irreducible over $\mathbb{Q}$. By way of contradiction, suppose that the above polynomial may be written as

$$8x^3 - 6x + 1 = (q_1 x + q_2)\left(q_3 x^2 + q_4 x + q_5\right),$$

where $q_i \in \mathbb{Q}$ for each index i. By dividing by an appropriate nonzero rational number, if necessary, we may assume without loss of generality that the degree-1 factor in the above equality is monic:

$$8x^3 - 6x + 1 = (x + q_2)\left(8x^2 + q_4 x + q_5\right).$$

In a similar fashion, we find that:

$$8x^3 - 6x + 1 = (x + q_2)\left(8x^2 + q_4 x + \frac{1}{q_2}\right).$$

Let $q_2 = \frac{a}{b}$ where a and b are integers, such that b is nonzero and $\frac{a}{b}$ is in lowest terms. Also, let $q_4 = \frac{c}{d}$, where c and d are integers, so that d is nonzero and $\frac{c}{d}$ is in lowest terms:

$$8x^3 - 6x + 1 = \left(x + \frac{a}{b}\right)\left(8x^2 + \frac{c}{d}x + \frac{b}{a}\right).$$

Equivalently,

$$8x^3 - 6x + 1 = 8x^3 + \left(\frac{8a}{b} + \frac{c}{d}\right)x^2 + \left(\frac{ac}{bd} + \frac{b}{a}\right)x + 1.$$

Since $\frac{8a}{b} + \frac{c}{d}$ vanishes, we have that $-\frac{8a}{b} = \frac{c}{d}$. Therefore,

$$8x^3 - 6x + 1 = 8x^3 + \left(\frac{-8a^2}{b^2} + \frac{b}{a}\right)x + 1.$$

That is,

$$8x^3 - 6x + 1 = 8x^3 + \left(\frac{-8a^3 + b^3}{ab^2}\right)x + 1.$$

Since $\frac{-8a^3+b^3}{ab^2}$ is equal to -6, we have that

$$-8a^3 + b^3 = -6 \cdot ab^2.$$

Therefore,

$$\left(-8a^3 + b^3\right)(\text{mod } a) \equiv \left(-6 \cdot ab^2\right)(\text{mod } a).$$

That is,

$$b^3 \equiv 0(\text{mod } a),$$

contradicting that a and b are relatively prime, as may be verified using the Fundamental Theorem of Arithmetic. So, we have thus far shown that $\cos\left(\frac{2\pi}{9}\right)$ is a root of the following irreducible element in the polynomial ring $\mathbb{Q}[x]$:

$$8x^3 - 6x + 1 \in \mathbb{Q}[x].$$

We may, accordingly, deduce that:

$$m_{\cos\left(\frac{2\pi}{9}\right),\mathbb{Q}}(x) = x^3 - \frac{3}{4}x + \frac{1}{8}.$$

Therefore,

$$\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{9}\right)\right) : \mathbb{Q}\right] = \deg m_{\cos\left(\frac{2\pi}{9}\right),\mathbb{Q}}(x) = 3.$$

But this contradicts that $\cos\left(\frac{2\pi}{9}\right)$ is constructible, according to **Proposition 23**.

Exercise 3.106. Prove that Archimedes' construction actually trisects the angle θ. [Note the isosceles triangles in (Figure 5 on page 535 of Dummit and Foote's *Abstract Algebra*) to prove that $\beta = \gamma = 2\alpha$.]

Solution 3.107. Figure 5 on page 535 of Dummit and Foote's *Abstract Algebra* will henceforth be referred to as Figure 5. With respect to this figure, let A denote the illustrated point of intersection closest to α, let B denote the illustrated point of intersection closest to β, let G denote the point of intersection closest to γ, and let T denote the point of intersection closest to θ. Also, let L and R respectively denote the left-hand and right-hand intersections of the given semi-circle and the given horiztonal line. We know that

$$\|AB\| = \|BT\|,$$

so the triangle ΔABT must be an isoceles triangle. Therefore, we may deduce that:

$$\angle BAT = \angle BTA.$$

That is,

$$\alpha = \angle BTA.$$

Therefore,

$$\alpha + \angle BTG + \theta = \angle BTA + \angle BTG + \theta.$$

Therefore,

$$\alpha + \angle BTG + \theta = 180^\circ.$$

Equivalently,

$$\alpha + (180^\circ - \beta - \gamma) + \theta = 180^\circ.$$

But since

$$\|BT\| = \|TG\|,$$

we find that $\beta = \gamma$. Therefore,

$$\alpha + (180^\circ - 2\beta) + \theta = 180^\circ.$$

We know that

$$\beta + (180^\circ - 2\alpha) = 180^\circ,$$

as is easily seen by considering the interior angles in ΔABT. We thus arrive at the equality whereby.

$$\beta = 2\alpha.$$

So, from the above equality, together with the equality whereby

$$\alpha + (180^\circ - 2\beta) + \theta = 180^\circ,$$

we observe that the equality

$$\alpha + (180^\circ - 4\alpha) + \theta = 180^\circ$$

holds. Therefore,

$$\alpha - 4\alpha + \theta = 0.$$

Therefore,

$$\theta = 3\alpha,$$

as desired.

Exercise 3.108. Prove that Conway's construction indicated in the text actually constructs $2k^{1/3}$ and $2k^{2/3}$. [One method: let (x, y) be the coordinates of the point C, a the distance from B to C and b the distance from A to D; use similar triangles to prove (a) $\frac{y}{1} = \frac{\sqrt{1-k^2}}{1+a}$, (b) $\frac{x}{a} = \frac{b+k}{1+a}$, (c) $\frac{y}{x-k} = \frac{\sqrt{1-k^2}}{3k}$, and also show that (d) $(1 - k^2) + (b + k)^2 = (1 + a)^2$; solve these equations for a and b.]

Solution 3.109. Our strategy is based on the method given above. We introduce some additional notation which is useful for our purposes. let a perpendicular line segment passing through $C = (x, y)$ intersect AD at a point P. Let the previously unlabeled vertex of the triangle illustrated in **Fig. 4** on page 535 of Dummit & Foote's *Abstract Algebra* be labeled as U.

(a) Consider the triangles ΔUBD and ΔPCD. Of course, $\angle BDU = \angle CDP$. Also, we have that $\angle CPD = \angle BUD = 90°$. We may thus deduce that $\Delta UBD \sim \Delta PCD$. Since ΔUBD and ΔPCD are similar triangles, we have that:

$$\frac{\|BD\|}{\|BU\|} = \frac{\|CD\|}{\|CP\|}.$$

Equivalently,

$$\frac{a+1}{\sqrt{1-k^2}} = \frac{1}{y},$$

with

$$\frac{\sqrt{1-k^2}}{a+1} = y,$$

as desired.

(b) Now, let Q denote the point of intersection obtained by extending a perpendicular line passing through $C = (x, y)$ to BU. Now, consider the triangles ΔBCQ and ΔBDU. Since $\angle QBC = \angle UBD$ and since $\angle BQC = \angle BUD = 90°$, we find that $\Delta BCQ \sim \Delta BDU$. So, since

$$\frac{\|QC\|}{\|BC\|} = \frac{\|UD\|}{\|BD\|}.$$

Equivalently,

$$\frac{x}{a} = \frac{k+b}{1+a},$$

as desired.

(c) Now, let R denote the previously unlabeled point of intersection given by the triangle which has two sides lengths which are respectively equal to k and $\frac{1}{3}\sqrt{1-k^2}$ and which has U and A as endpoints. Now, consider the triangles ΔUAR and ΔACP. Since

$$\angle UAR = \angle PAC$$

and since

$$\angle CPA = \angle AUR = 90°,$$

we may deduce that ΔUAR and ΔACP are similar triangles. So, since

$$\frac{\|CP\|}{\|AP\|} = \frac{\|UR\|}{\|UA\|}$$

we find that

$$\frac{y}{x-k} = \frac{\frac{1}{3}\sqrt{1-k^2}}{k},$$

so that

$$\frac{y}{x-k} = \frac{\sqrt{1-k^2}}{3k},$$

as desired.

(d) We apply the Pythagorean theorem with respect to the triangle ΔUBD. Since

$$\angle DUB = 90°$$

we have that:

$$\|UD\|^2 + \|UB\|^2 = \|BD\|^2.$$

Equivalently,

$$(k + b)^2 + (1 - k^2) = (a + 1)^2,$$

as desired.

The remainder of our solution is based on a solution given in the following link:

`https://positron0802.files.wordpress.com/2017/01/`
`abstract-algebra-dummit-foote-chapter-13-field-theory-solutions.pdf`

From (a), we have that $y = \frac{\sqrt{1-k^2}}{1+a}$, so that:

$$y(1 + a) = \sqrt{1 - k^2}. \tag{3.1}$$

From (c) we have that $\frac{y}{x-k} = \frac{\sqrt{1-k^2}}{3k}$, so that:

$$\frac{3ky}{x - k} = \sqrt{1 - k^2}. \tag{3.2}$$

So, from (3.1) and (3.2) together, we have that:

$$y(1 + a) = \frac{3ky}{x - k}. \tag{3.3}$$

So, from (3.3), we have that:

$$(1 + a)(x - k) = 3k. \tag{3.4}$$

From (b), we have that

$$\frac{x}{a} = \frac{b + k}{1 + a}.$$

Therefore,

$$x = \frac{a(b + k)}{1 + a}.$$

So, from (3.4) together with the equality $x = \frac{a(b+k)}{1+a}$, we have that:

$$\begin{aligned}
&(1 + a)\left(\frac{a(b + k)}{1 + a} - k\right) = 3k \implies \\
&a(b + k) - k(1 + a) = 3k \implies \\
&a(b + k) = 3k + k(1 + a) \implies \\
&a(b + k) = 4k + ak \implies \\
&b + k = \frac{4k + ak}{a}.
\end{aligned}$$

From (d), we have that: $(1 - k^2) + (b + k)^2 = (1 + a)^2$. So, from (d) together with the equality

$$b + k = \frac{4k + ak}{a},$$

we obtain the following:

$$\begin{aligned}
&(1-k^2)+(b+k)^2=(1+a)^2 \Longrightarrow \\
&(1-k^2)+\left(\frac{4k+ak}{a}\right)^2=(1+a)^2 \Longrightarrow \\
&a^2(1-k^2)+(4k+ak)^2=a^2(1+a)^2 \Longrightarrow \\
&a^2-a^2k^2+16k^2+8ak^2+a^2k^2=a^4+2a^3+a^2 \Longrightarrow \\
&-a^2k^2+16k^2+8ak^2+a^2k^2=a^4+2a^3 \Longrightarrow \\
&16k^2+8ak^2=a^4+2a^3 \Longrightarrow \\
&a^4+2a^3-8ak^2-16k^2=0.
\end{aligned}$$

We find that $2k^{2/3}$ is a root of the equation

$$a^4+2a^3-8ak^2-16k^2=0,$$

which shows that Conway's construction indicated in the text actually constructs $2k^{2/3}$, with $a=2k^{2/3}$. Now, recall that

$$b+k=\frac{4k+ak}{a}.$$

We thus have that

$$b=\frac{4k+(2k^{2/3})k}{(2k^{2/3})}-k.$$

This shows that

$$b=2\sqrt[3]{k}$$

may be constructed according to Conway's construction,

3.12 Exercises from Section 13.4

Exercise 3.110. Determine the splitting field and its degree over $\mathbb{Q}$ for x^4-2.

Solution 3.111. From the equality $x^4=2$, we have that $x^2=\pm\sqrt{2}$. From this latter equality, we find that the roots of $x^4-2\in\mathbb{Q}[x]$ are precisely the elements in the set

$$\{\sqrt[4]{2}, i\sqrt[4]{2}, -\sqrt[4]{2}, -i\sqrt[4]{2}\},$$

where i denotes the imaginary unit. So, it is clear that the splitting field of $x^4-2\in\mathbb{Q}[x]$ over $\mathbb{Q}$ is precisely $\mathbb{Q}(\sqrt[4]{2},i)$. Now, consider the degree of this splitting field over $\mathbb{Q}$. To compute this degree, we proceed to consider the following otwer of fields.

$$\begin{tikzcd}
\mathbb{Q}(i)(\sqrt[4]{2}) \cong \mathbb{Q}(\sqrt[4]{2})(i) \cong \mathbb{Q}(i,\sqrt[4]{2}) \cong \mathbb{Q}(\sqrt[4]{2},i) \arrow[d, dash] \\
\mathbb{Q}(i) \arrow[d, dash] \\
\mathbb{Q}
\end{tikzcd}$$

It is obvious that the minimal polynomial of the imaginary unit over $\mathbb{Q}$ is $x^2+1 \in \mathbb{Q}[x]$. Accordingly, we find that:

$$[\mathbb{Q}(i):\mathbb{Q}] = \deg\left(m_{i,\mathbb{Q}}(x)\right) = 2.$$

We thus proceed to consider the minimal polynomial of $\sqrt[4]{2}$ over the field $\mathbb{Q}(i)$. Certainly, $x = \sqrt[4]{2}$ satisfies the equality whereby $x^4 - 2 = 0$. We claim that $x^4 - 2 = 0$ is irreducible as an element in $\left(\mathbb{Q}(i)\right)[x]$. To show this, since $x^4 - 2$ splits as

$$x^4 - 2 = \left(x - \sqrt[4]{2}\right)\left(x - i\sqrt[4]{2}\right)\left(x + \sqrt[4]{2}\right)\left(x + i\sqrt[4]{2}\right),$$

if $x^4 - 2$ actually were reducible as an element in $\left(\mathbb{Q}(i)\right)[x]$, then one of the following products would have to be an element in $\left(\mathbb{Q}(i)\right)[x]$.

$$\begin{aligned}
&(x + i\sqrt[4]{2})\\
&(x + \sqrt[4]{2})\\
&(x + \sqrt[4]{2})(x + i\sqrt[4]{2})\\
&(x - i\sqrt[4]{2})\\
&(x - i\sqrt[4]{2})(x + i\sqrt[4]{2})\\
&(x - i\sqrt[4]{2})(x + \sqrt[4]{2})\\
&(x - i\sqrt[4]{2})(x + \sqrt[4]{2})(x + i\sqrt[4]{2})
\end{aligned}$$

Expand the above products as follows.

$$\begin{aligned}
&(x + i\sqrt[4]{2})\\
&(x + \sqrt[4]{2})\\
&x^2 + \sqrt[4]{2}(1+i)x + \sqrt{2}i\\
&(x - i\sqrt[4]{2})\\
&x^2 + \sqrt{2}\\
&x^2 + \sqrt[4]{2}(1-i)x - \sqrt{2}i\\
&x^3 + \sqrt[4]{2}x^2 + \sqrt{2}x + 2^{3/4}
\end{aligned}$$

But since elements in $\mathbb{Q}(i)$ are of the form $a + bi$ for $a, b \in \mathbb{Q}$, and since $\sqrt{2}$ and $\sqrt[4]{2}$ are irrational, it is clear that the above expanded products are not in $\left(\mathbb{Q}(i)\right)[x]$. Since $\sqrt[4]{2}$ is a root of $x^4 - 2$ and since $x^4 - 2$ is irreducible over the field $\mathbb{Q}(i)$, we find that the minimal polynomial of $\sqrt[4]{2}$ over $\mathbb{Q}(i)$ is precisely $x^4 - 2 \in \left(\mathbb{Q}(i)\right)[x]$, so that:

$$[\mathbb{Q}(i)(\sqrt[4]{2}):\mathbb{Q}(i)] = \deg m_{\sqrt[4]{2},\mathbb{Q}(i)}(x) = \deg\left(x^4 - 2\right).$$

We thus find that the degree sequence associated with the tower of fields given above is as indicated below.

$$\begin{tikzcd}
\mathbb{Q}(i)(\sqrt[4]{2}) \cong \mathbb{Q}(\sqrt[4]{2})(i) \cong \mathbb{Q}(i, \sqrt[4]{2}) \cong \mathbb{Q}(\sqrt[4]{2}, i) \arrow[d, dash, "4"] \\
{}
\end{tikzcd}$$

$$\begin{tikzcd}\mathbb{Q}(i) \arrow[d, dash, "2"] \\ \mathbb{Q}\end{tikzcd}$$

Therefore,

$$[\mathbb{Q}(i, \sqrt[4]{2}) : \mathbb{Q}] = [\mathbb{Q}(i, \sqrt[4]{2}) : \mathbb{Q}(i)][\mathbb{Q}(i) : \mathbb{Q}] = 4 \cdot 2 = 8.$$

We thus have that the degree of the splitting field for $x^4 - 2$ over $\mathbb{Q}$ is 8. We conclude by remarking that this computation agrees with **Proposition 26** from Dummit & Foote's *Abstract Algebra*, which states that a splitting field for a polynomial of degree m over a field $\mathbb{F}$ is of degree at most $m!$ over F, with $8 \leq 4! = 24$.

Exercise 3.112. Determine the splitting field and its degree over $\mathbb{Q}$ for $x^4 + 2$.

Solution 3.113. Consider the polynomial equation whereby $x^4 = -2$. From the equality whereby $x^4 = -2$, we obtain the equation $x^2 = \pm\sqrt{-2}$. So, we have that $x^2 = \pm i\sqrt{2}$. So, since

$$x^2 = (\pm 1) \cdot i \cdot \sqrt{2}$$

we have that

$$x = \pm\sqrt{\pm 1} \cdot \sqrt{i} \cdot \sqrt[4]{2}.$$

Equivalently,

$$x = \pm\sqrt{\pm 1} \cdot \left(\frac{1+i}{\sqrt{2}}\right) \cdot \sqrt[4]{2}.$$

So, from the above discussion, we find that the roots of the given polynomial are precisely the elements in the following set:

$$\left\{\frac{1-i}{\sqrt[4]{2}}, -\frac{1+i}{\sqrt[4]{2}}, -\frac{1-i}{\sqrt[4]{2}}, \frac{1+i}{\sqrt[4]{2}}\right\}.$$

Since

$$\frac{1-i}{\sqrt[4]{2}} + \frac{1+i}{\sqrt[4]{2}} = 2^{3/4},$$

and since

$$\frac{1-i}{\sqrt[4]{2}} - \frac{1+i}{\sqrt[4]{2}} = -i2^{3/4},$$

it is clear that the splitting field of $x^4 + 2 \in \mathbb{Q}[x]$ over $\mathbb{Q}$ is equal to:

$$\mathbb{Q}(2^{3/4}, i).$$

By repeating the argument given in Solution 3.111, we find that the degree of the splitting field of the given polynomial over $\mathbb{Q}$ is also equal to 8.

Exercise 3.114. Determine the splitting field and its degree over $\mathbb{Q}$ for $x^4 + x^2 + 1$.

Solution 3.115. Let y be such that $y = x^2$. So, we have that the given polynomial $x^4 + x^2 + 1 \in \mathbb{Q}[x]$ may be rewritten as $y^2 + y + 1$. Letting $y^2 + y + 1 = 0$, by the quadratic formula, we find that:

$$y = \frac{-1 \pm \sqrt{-3}}{2}.$$

So, we find that the roots of the polynomial $x^4 + x^2 + 1$ are given by the following expression:

$$x = \pm\sqrt{\frac{-1 \pm \sqrt{-3}}{2}}.$$

That is, the roots of the given polynomial are given by the following expression:

$$x = \pm\frac{\sqrt{-1 \pm i\sqrt{3}}}{\sqrt{2}}.$$

We focus our attention towards the following roots.

$$\alpha = \frac{\sqrt{-1 - i\sqrt{3}}}{\sqrt{2}} \qquad \beta = \frac{\sqrt{-1 + i\sqrt{3}}}{\sqrt{2}}.$$

With respect to the above notation, we have that the roots of the given polynomial are precisely $\pm\alpha$ and $\pm\beta$.

Using a trigonometric argument, it is easily seen that

$$\alpha = \frac{1}{2} - \frac{i\sqrt{3}}{2}$$

and that

$$\beta = \frac{1}{2} + \frac{i\sqrt{3}}{2}.$$

So, in this case, it is clear that the splitting field of $x^4 + x^2 + 1$ over $\mathbb{Q}$ is equal to $\mathbb{Q}(i\sqrt{3})$. Since $(i\sqrt{3})^2 = -3$, it is obvious that the degree of $\mathbb{Q}(i\sqrt{3})$ over the base field $\mathbb{Q}$ is equal to 2. That is, the splitting field of $\mathbb{Q}(i\sqrt{3})$ of the given polynomial is of degree 2 over $\mathbb{Q}$.

Exercise 3.116. Determine the splitting field and its degree over $\mathbb{Q}$ for $x^6 - 4$.

Solution 3.117. We begin by considering the roots of the given polynomial $x^6 - 4 \in \mathbb{Q}[x]$. From the equation

$$x^6 - 4 = 0$$

we find that

$$x^6 = 4,$$

which implies that

$$x^3 = \pm 2.$$

So, we see that the roots of the given polynomial consist of the solutions for

$$x^3 = 2,$$

together with the solutions for

$$x^3 = -2.$$

So, it is natural to consider the cubic roots of unity, as well as the cubic roots of -1. Through the use of a trigonometric argument, it is easily seen that the cubic roots of unity are precisely the elements in the following set:

$$\left\{1, -\frac{1}{2} + \frac{\sqrt{3}}{2}i, -\frac{1}{2} - \frac{\sqrt{3}}{2}i\right\}.$$

A symmetric argument reveals that the cubic roots of -1 consist of the elements in the following set:

$$\left\{-1, \frac{1}{2} + \frac{\sqrt{3}}{2}i, \frac{1}{2} - \frac{\sqrt{3}}{2}i\right\}.$$

So, it is clear that the roots of the given polynomial are precisely the elements in the following set.

$$\left\{\sqrt[3]{2}, \left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right)\sqrt[3]{2}, \left(-\frac{1}{2} - \frac{\sqrt{3}}{2}i\right)\sqrt[3]{2}, -\sqrt[3]{2}, \left(\frac{1}{2} + \frac{\sqrt{3}}{2}i\right)\sqrt[3]{2}, \left(\frac{1}{2} - \frac{\sqrt{3}}{2}i\right)\sqrt[3]{2}\right\}.$$

We may deduce that the splitting field of the given polynomial over $\mathbb{Q}$ is precisely:

$$\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}).$$

It is easily seen that the degree of $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$ over $\mathbb{Q}$ is 6, as may be verified by appealing to the irrationality of $\sqrt[3]{2}$, and by showing that $x^3 + 3$ is irreducible over $\mathbb{Q}(\sqrt[3]{2})$.

Exercise 3.118. Let K be a finite extension of F. Prove that K is a splitting field over F if and only if every irreducible polynomial in $F[x]$ that has a root in K splits completely in $K[x]$. [Use Theorems 8 and 27.]

Solution 3.119. Theorem 8 is formulated in the following manner in the class textbook.

"**Theorem 8.** Let $\phi: F \xrightarrow{\sim} F'$ be an isomorphism of fields. Let $p(x) \in F[x]$ be an irreducible polynomial and let $p'(x) \in F'[x]$ be the irreducible polynomial obtained by applying the map ϕ to be coefficients of $p(x)$. Let α be a root of $p(x)$ (in some extension of F) and let β be a root of $p'(x)$ (in some extension of F'). Then there is an isomorphism

$$\begin{aligned} \sigma: F(\alpha) &\xrightarrow{\sim} F'(\beta) \\ \alpha &\mapsto \beta \end{aligned}$$

mapping α to β and extending ϕ, i.e., such that σ restricted to F is the isomorphism ϕ." (p. 519)

Theorem 27 from the class textbook is given as follows.

"**Theorem 27.** Let $\phi: F \xrightarrow{\sim} F'$ be an isomorphism of fields. Let $f(x) \in F[x]$ be a polynomial and let $f'(x) \in F'[x]$ be the polynomial obtained by applying ϕ to the coefficients of $f(x)$. Let E be a splitting field for $f(x)$ over F and let E' be a splitting field for $f'(x)$ over F'. Then the isomorphism extends to an isomorphism $\sigma: E \xrightarrow{\sim} E'$, i.e., σ restricted to F is the isomorphism ϕ:

$$\begin{tikzcd}
\sigma: E \arrow[r, "\sim"] \arrow[d, dash] & E' \arrow[d, dash] \\
\phi: F \arrow[r, "\sim"] & F'
\end{tikzcd}$$

" (p. 541)

Now, to prove the biconditional statement given in the above exercise, we begin by proving the "forwards" direction for this statement, letting K and F be as given above, with K as a finite extension of F. Our solution is based on a corresponding solution given in the following link.

`https://positron0802.files.wordpress.com/2017/01/`
`abstract-algebra-dummit-foote-chapter-13-field-theory-solutions.pdf`

($\Longrightarrow$) Assume that K is a splitting field over F, letting $f(x)$ be an element in the polynomial ring $F[x]$ such that K is the splitting field of $f(x)$ over F. Let $g(x)$ be an irreducible polynomial in $F[x]$, and let α be a root of $g(x)$ such that $\alpha \in K$. Now, let β be an arbitrary root of $g(x)$. So, it remains to prove that β must be in K. Since $g(x)$ is an irreducible polynomial in $F[x]$, we have that there exists an isomorphism of the following form:

$$\begin{aligned}\sigma\colon F(\alpha) &\overset{\sim}{\to} F'(\beta)\\ \alpha &\mapsto \beta\end{aligned}$$

, Now, since K is a splitting field over F, and since and since α is a root of $g(x)$ with $\alpha \in K$, we have that $K = K(\alpha)$ is the splitting field of $f(x)$ over $F(\alpha)$. Similarly, $K(\beta)$ is the splitting field of $f(x)$ over $F(\beta)$. So, since

$$\begin{aligned}\sigma\colon F(\alpha) &\overset{\sim}{\to} F'(\beta)\\ \alpha &\mapsto \beta\end{aligned}$$

is an isomorphism of fields, by **Theorem 27**, we have that the field isomorphism σ extends to an isomorphism $\phi\colon K(\alpha) \to K(\beta)$. We thus have that

$$[K \ : \ F] = [K(\alpha) \ : \ F] = [K(\beta) \ : \ F].$$

We can conclude that $K = K(\beta)$, so that $\beta \in K$.

($\Longleftarrow$) Conversely, assume that every irreducible polynomial in $F[x]$ that has a roto in K splits completely in $K[x]$. Recall that K is a finite extension of F. We thus have that $K = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ for some $\alpha_1, \alpha_2, \ldots, \alpha_n$. For each index i, let p_i denote the minimal polynomial of α_i over F, and let $f = p_1 p_2 \cdots p_n$. Now, since each element of the form α_i is in K, from our initial assumption, we have that each polynomial of the form p_i must split completely in K. So, f splits completely in K and K is generated over F by the roots of f. So, K is the splitting field of f over F.

3.13 Exercises from Section 13.5

Exercise 3.120. Prove that the derivative D_x of a polynomial satisfies $D_x(f(x) + g(x)) = D_x(f(x)) + D_x(g(x))$ and $D_x(f(x)g(x)) = D_x(f(x))g(x) + D_x(g(x))f(x)$ for any two polynomials $f(x)$ and $g(x)$.

Solution 3.121. As above, let $f(x)$ and $g(x)$ be polynomials. Let F be a field, and let $f(x)$ and $g(x)$ be elements in the polynomial ring $F[x]$. Let these polynomials be denoted as follows, letting n and m be such that $n, m \in \mathbb{N}_0$:

$$\begin{aligned}f(x) &= a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,\\ g(x) &= b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0.\end{aligned}$$

We may assume without loss of generality that $n \geq m$, as a symmetric argument works in the case whereby $n \leq m$. Evaluate the coefficients of the expression $f(x) + g(x)$ as indicated in the following manner:

$$\begin{aligned}&f(x) + g(x) =\\ &a_n x^n \ + \ \cdots \ + \ a_{m+1} x^{m+1} \ + \ (a_m + b_m)\, x^m \ + \ \cdots \ + \ (a_1 + b_1)\, x \ + \ (a_0 + b_0)\,.\end{aligned}$$

Apply the operator D_x to both sides of the above equality:

$$\begin{aligned}&D_x\left(f(x)+g(x)\right) = \\ &a_n n x^{n-1} \; + \; \cdots \; + \; a_{m+1}(m+1)x^m \; + \; \left(a_m + b_m\right) m x^{m-1} \; + \; \cdots \; + \; \left(a_1 + b_1\right).\end{aligned}$$

Since

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

and

$$g(x) = b_n x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$$

we find that $D_x(f(x))$ and $D_x(g(x))$ may be evaluated as follows:

$$\begin{aligned}D_x(f(x)) &= a_n n x^{n-1} + a_{n-1}\left(n-1\right)x^{n-2} + \cdots + a_1, \\ D_x(g(x)) &= b_m m x^{m-1} + b_{m-1}\left(m-1\right)x^{m-2} + \cdots + b_1.\end{aligned}$$

Now, recall that we are working under the assumption that $n \geq m$. From the inequality $(n-1) \geq (m-1)$ together with the above formulas for $D_x(f(x))$ and $D_x(g(x))$, we have that $D_x(f(x)) + D_x(g(x))$ must be equal to:

$$a_n n x^{n-1} \; + \; \cdots \; + \; a_{m+1}(m+1)x^m \; + \; \left(a_m + b_m\right) m x^{m-1} \; + \; \cdots \; + \; \left(a_1 + b_1\right),$$

as desired.

It is convenient to denote $f(x)$ and $g(x)$ as follows:

$$\begin{aligned}f(x) &= \sum_{i=0}^{n} a_i x^i, \\ g(x) &= \sum_{j=0}^{m} b_j x^j.\end{aligned}$$

The coefficients in the product

$$f(x)g(x) = \left(\sum_{i=0}^{n} a_i x^i\right)\left(\sum_{j=0}^{m} b_j x^j\right)$$

may be defined using an appropriate convolution operation. For the sake of convenience, we may adopt the convention whereby a_i vanishes for $i \in \mathbb{Z}$ such that $i > n$ or $i < 0$, and we may let b_j be equal to 0 for integers j such that $j > m$ of $j < 0$. So, the above product may be denoted in terms of formal sums or generating series:

$$f(x)g(x) = \left(\sum_{i \geq 0} a_i x^i\right)\left(\sum_{j \geq 0} b_j x^j\right).$$

We thus obtain the following equality:

$$f(x)g(x) = \sum_{k=0}^{\infty}\left(\sum_{\ell=0}^{k} a_{k-\ell} b_\ell\right) x^k.$$

Therefore,

$$D_x\left(f(x)g(x)\right) = \sum_{k=0}^{\infty}\left(\sum_{\ell=0}^{k} a_{k-\ell} b_\ell\right) k x^{k-1}.$$

Similarly, since

$$D_x\left(f(x)\right) = \sum_{i=0}^{\infty} a_i i x^{i-1}$$

we have that

$$D_x\left(f(x)\right) g(x) = \left(\sum_{i=0}^{\infty} a_i i x^{i-1}\right)\left(\sum_{j=0}^{\infty} b_j x^j\right)$$

so that

$$D_x\left(f(x)\right) g(x) = \left(\sum_{i=0}^{\infty} a_{i+1}(i+1)x^i\right)\left(\sum_{j=0}^{\infty} b_j x^j\right).$$

Symmetrically,

$$f(x) D_x\left(g(x)\right) = \left(\sum_{i=0}^{\infty} a_i x^i\right)\left(\sum_{j=0}^{\infty} b_{j+1}(j+1)x^j\right).$$

So, since

$$D_x\left(f(x)\right) g(x) = \sum_{k=0}^{\infty}\left(\sum_{\ell=0}^{k} a_{\ell+1}(\ell+1)b_{k-\ell}\right)x^k$$

and since

$$f(x) D_x\left(g(x)\right) = \sum_{k=0}^{\infty}\left(\sum_{\ell=0}^{k} a_\ell b_{k-\ell-1}(k-\ell-1)\right)x^k,$$

we have that the coefficient of x^k in the sum of the above two expressions is equal to

$$\sum_{\ell=0}^{k} a_{\ell+1}(\ell+1)b_{k-\ell} + \sum_{\ell=0}^{k} a_\ell b_{k-\ell-1}(k-\ell-1).$$

The above expression is equal to:

$$\sum_{\ell=1}^{k+1} a_\ell(\ell)b_{k-\ell-1} + \sum_{\ell=0}^{k} a_\ell b_{k-\ell-1}(k-\ell-1).$$

Rewrite the above summation as follows:

$$\sum_{\ell=0}^{k+1} a_\ell(\ell)b_{k-\ell-1} + \sum_{\ell=0}^{k} a_\ell b_{k-\ell-1}(k-\ell-1).$$

The above expression is equal to:

$$\sum_{\ell=0}^{k+1} a_\ell(\ell)b_{k-\ell-1} + \sum_{\ell=0}^{k+1} a_\ell b_{k-\ell-1}(k-\ell-1).$$

The above is equal to:

$$\sum_{\ell=0}^{k+1} a_\ell b_{k-\ell-1}(k-1).$$

Rewrite the above summation as follows:

$$(k-1)\sum_{\ell=0}^{k+1} a_\ell b_{k-\ell-1}.$$

Comparing coefficients of the above form with the coefficients in

$$D_x\left(f(x)g(x)\right) = \sum_{k=0}^{\infty}\left(\sum_{\ell=0}^{k} a_{k-\ell}b_\ell\right)kx^{k-1}$$

completes our proof.

Exercise 3.122. Find all irreducible polynomials of degrees 1, 2 and 4 over $\mathbb{F}_2$ and prove that their product is $x^{16} - x$.

Solution 3.123. Trivially, degree-1 polynomials are irreducible. So, the elements x and $x + 1 = x - 1$ in $\mathbb{F}_2[x]$ are irreducible. Now, consider the degree-2 irreducible elements in $\mathbb{F}_2[x]$. The non-irreducible degree-2 elements in $\mathbb{F}_2[x]$ are:

$$\begin{aligned}
&x \cdot x = x^2,\\
&x \cdot (x+1) = x^2 + x, \text{and}\\
&(x+1) \cdot (x+1) = x^2 + 1.
\end{aligned}$$

This shows that the only polynomial of degree 2 in $\mathbb{F}_2[x]$ that is irreducible over $\mathbb{F}_2$ is $x^2 + x + 1$. Now, consider the degree-4 non-irreducible elements in $\mathbb{F}_2[x]$, which are given below.

$$\begin{aligned}
&\left(x^2\right)\left(x^2\right) = x^4\\
&\left(x^2\right)\left(x^2+1\right) = x^4 + x^2\\
&\left(x^2\right)\left(x^2+x\right) = x^4 + x^3\\
&\left(x^2\right)\left(x^2+x+1\right) = x^4 + x^3 + x^2\\
&\left(x^2+1\right)\left(x^2+1\right) = x^4 + 1\\
&\left(x^2+1\right)\left(x^2+x\right) = x^4 + x^3 + x^2 + x\\
&\left(x^2+1\right)\left(x^2+x+1\right) = x^4 + x^3 + x + 1\\
&\left(x^2+x\right)\left(x^2+x\right) = x^4 + x^2\\
&\left(x^2+x\right)\left(x^2+x+1\right) = x^4 + x\\
&\left(x^2+x+1\right)\left(x^2+x+1\right) = x^4 + x^2 + 1\\
&(x)\left(x^3\right) = x^4\\
&(x)\left(x^3+1\right) = x^4 + x\\
&(x)\left(x^3+x\right) = x^4 + x^2\\
&(x)\left(x^3+x+1\right) = x^4 + x^2 + x\\
&(x)\left(x^3+x^2\right) = x^4 + x^3\\
&(x)\left(x^3+x^2+1\right) = x^4 + x^3 + x\\
&(x)\left(x^3+x^2+x\right) = x^4 + x^3 + x^2\\
&(x)\left(x^3+x^2+x+1\right) = x^4 + x^3 + x^2 + x\\
&(x+1)\left(x^3\right) = x^4 + x^3\\
&(x+1)\left(x^3+1\right) = x^4 + x^3 + x + 1\\
&(x+1)\left(x^3+x\right) = x^4 + x^3 + x^2 + x\\
&(x+1)\left(x^3+x+1\right) = x^4 + x^3 + x^2 + 1\\
&(x+1)\left(x^3+x^2\right) = x^4 + x^2\\
&(x+1)\left(x^3+x^2+1\right) = x^4 + x^2 + x + 1\\
&(x+1)\left(x^3+x^2+x\right) = x^4 + x\\
&(x+1)\left(x^3+x^2+x+1\right) = x^4 + 1
\end{aligned}$$

So, from the above computations, we find that the only degree-4 irreducible elements in $\mathbb{F}_2[x]$ are as follows.

$$\begin{aligned}&x^4+x+1\\&x^4+x^3+1\\&x^4+x^3+x^2+x+1\end{aligned}$$

So, from the above computations, we find that the product of all irreducible polynomials of degrees 1, 2 and 4 over $\mathbb{F}_2$ is equal to the following expression.

$$x(x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1).$$

Expand the above product without reducing the resultant coefficients as elements in $\mathbb{F}_2$:

$$x^{16}+4x^{15}+8x^{14}+12x^{13}+18x^{12}+26x^{11}+32x^{10}+34x^9+34x^8+32x^7+26x^6+18x^5+12x^4+8x^3+4x^2+x.$$

Modulo 2, the above expression reduces to

$$x^{16}+x=x^{16}-x,$$

as desired.

Exercise 3.124. Prove that d divides n if and only if x^d-1 divides x^n-1. [Note that if $n=qd+r$ then $x^n-1=(x^{qd+r}-x^r)+(x^r-1)$.]

Solution 3.125. ($\Longrightarrow$) Assume that d divides n. Now, consider the following product of polynomials:

$$\left(x^d-1\right)\left(x^{n-d}+x^{n-2d}+\cdots+x^{n-(\frac{n}{d}-1)d}+1\right).$$

Expanding the above product, we obtain:

$$\begin{aligned}&x^n+x^{n-d}+\cdots+x^{2d}+x^d\\&-x^{n-d}-x^{n-2d}-\cdots-x^d-1.\end{aligned}$$

We find that the above summation telescopes, with

$$\left(x^d-1\right)\left(x^{n-d}+x^{n-2d}+\cdots+x^{n-(\frac{n}{d}-1)d}+1\right)=x^n-1,$$

which shows that x^d-1 divides x^n-1.

($\Longleftarrow$) Conversely, assume that x^d-1 divides x^n-1. Let $n=qd+r$, where q and r are elements in $\mathbb{N}_0$ such that r satisfies: $0\leq r<d$. Now, consider the following product:

$$\left(x^d-1\right)\left(x^{n-d}+x^{n-2d}+\cdots+x^{n-qd}+1\right).$$

Expanding the above product, we obtain:

$$\begin{aligned}&x^n+x^{n-d}+\cdots+x^{n-qd+d}+x^d\\&-x^{n-d}-x^{n-2d}-\cdots-x^{n-qd}-1.\end{aligned}$$

Simplifying the above summation, we find that

$$\left(x^d - 1\right)\left(x^{n-d} + x^{n-2d} + \cdots + x^{n-qd} + 1\right)$$

is equal to:

$$(x^n - 1) + \left(x^d - x^r\right).$$

But from our initial assumption that $x^d - 1$ divides $x^n - 1$ together with the equality

$$\left(x^d - 1\right)\left(x^{n-d} + x^{n-2d} + \cdots + x^{n-qd} + 1\right) = (x^n - 1) + \left(x^d - x^r\right),$$

we may deduce that $x^d - 1$ must divide $x^d - x^r$. But since $0 \leq r < d$, we may deduce that $r = 0$, so that d divides n.

3.14 Exercises from Section 13.6

Exercise 3.126. Suppose m and n are relatively prime positive integers. Let ζ_m be a primitive m^{th} root of unity and let ζ_n be a primitive n^{th} root of unity. Prove that $\zeta_m\zeta_n$ is a primitive mn^{th} root of unity.

Solution 3.127. Recall that a generator of the cyclic group of all n^{th} roots of unity is called a *primitive* n^{th} root of unity. As above, let m and n be elements in $\mathbb{N}$ such that the greatest common divisor of m and n is equal to 1. Also, let ζ_m and ζ_n be as given above. We thus have that ζ_m is a generator of the cyclic group of all m^{th} roots of unity, and we have that ζ_n is a generator of the cyclic group of all n^{th} roots of unity. Now, consider the expression $\zeta_m\zeta_n$. Since the underlying multiplicative operation of the algebraically closed field $\mathbb{C}$ is commutative, we have that:

$$(\zeta_m\zeta_n)^{mn} = \zeta_m^{mn}\zeta_n^{mn} = (\zeta_m^m)^n (\zeta_n^n)^m = 1^m \cdot 1^n = 1,$$

thus establishing that the product $\zeta_m\zeta_n$ of ζ_m and ζ_n is an $(mn)^{\text{th}}$ root of unity. We claim that $\zeta_m\zeta_n$ generates the multiplicative group consisting of the $(mn)^{\text{th}}$ roots of unity. To prove this, it suffices to prove that the order of $\zeta_m\zeta_n$ is equal to mn. For a natural number $\ell \in \mathbb{N}$, we have that

$$\zeta_m^\ell\zeta_n^\ell = (\zeta_m\zeta_n)^\ell.$$

Since ζ_m is a primitive m^{th} root of unity, we have that each power of ζ_m is an m^{th} root of unity. Also, since ζ_n is a primitive n^{th} root of unity, we have that each power of ζ_n is an n^{th} root of unity. Since m and n are relatively prime, it is easily seen that the only m^{th} root of unity which is also an n^{th} root of unity is 1, as may be verified by considering the minimal polynomial of a given m^{th} root of unity and the minimal polynomial of an arbitrary n^{th} root of unity. Conversely, the only n^{th} root of unity which is also an m^{th} root of unity is 1. So, letting $\ell \in \mathbb{N}$ be as given above, if

$$\zeta_m^\ell\zeta_n^\ell = (\zeta_m\zeta_n)^\ell = 1,$$

then since ζ_n^ℓ must be a multiplicative inverse of ζ_m^ℓ and vice-versa, we may thus deduce that

$$\zeta_m^\ell = \zeta_n^\ell = 1.$$

Since ζ_m is a primitive m^{th} root of unity, the equality $\zeta_m^\ell = 1$ implies that ℓ must be a multiple of m. A symmetric argument shows that ℓ must be a multiple of n. We have previously shown that $\zeta_n\zeta_m$ to the power of mn is equal to 1, but since

$$\zeta_m^\ell\zeta_n^\ell = (\zeta_m\zeta_n)^\ell = 1$$

implies that ℓ must be a multiple of m and a multiple of n, we have that the smallest nonzero power $k \in \mathbb{N}$ such that $\zeta_m\zeta_n$ is equal to 1 is $k = mn$. So, the order of $\zeta_m\zeta_n$ is mn, as desired.

Exercise 3.128. Let ζ_n be a primitive n^{th} root of unity and let d be a divisor of n. Prove that ζ_n^d is a primitive $(n/d)^{\text{th}}$ root of unity.

Solution 3.129. Recall that a generator of the cyclic group of all n^{th} roots of unity is called a *primitive* n^{th} root of unity. So, let ζ_n be as given above, with ζ_n as a primitive n^{th} root of unity. We thus have that ζ_n is a generator of the cyclic group of all n^{th} roots of unity, so that

$$\left\{\zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}, 1 = \zeta_n^n\right\}$$

is a multiplicative cyclic group consisting of n distinct elements, with $\zeta_n^i \neq \zeta_n^j$ for distinct natural numbers i and j which are such that $i, j \leq n$. As above, we let d be a divisor of n. We may assume without loss of generality that $d \in \mathbb{N}$. Now, consider the expression ζ_n^d, and consider the multiplicative subgroup

$$\left\langle \zeta_n^d \right\rangle \leq \left\{\zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}, 1 = \zeta_n^n\right\}$$

generated by ζ_n^d. We have that

$$\left\langle \zeta_n^d \right\rangle = \left\{\zeta_n^d, \zeta_n^{2d}, \ldots, \zeta_n^{\left(\frac{n}{d}-1\right)d}, \zeta_n^{\left(\frac{n}{d}\right)d}\right\}$$

so that

$$\left\langle \zeta_n^d \right\rangle = \left\{\zeta_n^d, \zeta_n^{2d}, \ldots, \zeta_n^{\left(\frac{n}{d}-1\right)d}, \zeta_n^{n}\right\},$$

with

$$\left\langle \zeta_n^d \right\rangle = \left\{\zeta_n^d, \zeta_n^{2d}, \ldots, \zeta_n^{\left(\frac{n}{d}-1\right)d}, 1\right\}.$$

We claim that the cyclic group of all $\left(\frac{n}{d}\right)^{\text{th}}$ roots of unity consists precisely of the elements in the underlying set of $\langle \zeta_n^d \rangle$. To show this, begin by letting γ denote an arbitrary $\left(\frac{n}{d}\right)^{\text{th}}$ root of unity. So, we find that $\gamma^{\frac{n}{d}} = 1$. From the equality $\gamma^{\frac{n}{d}} = 1$, we observe that $\gamma^n = 1$, and we find that γ is an n^{th} root of unity. But recall that ζ_n is a generator of the cyclic group of all n^{th} roots of unity. So, we observe that there must exist a natural number $i \leq n$ such that $\gamma = \zeta_n^i$. Since

$$\gamma^{\frac{n}{d}} = \zeta_n^{i\frac{n}{d}} = 1$$

we may deduce that $i\frac{n}{d}$ is an integer multiple of n, so that d evenly divides i. In other words, i must be a multiple of d, which shows that γ must be in:

$$\left\langle \zeta_n^d \right\rangle = \left\{\zeta_n^d, \zeta_n^{2d}, \ldots, \zeta_n^{\left(\frac{n}{d}-1\right)d}, 1\right\}.$$

Conversely, let j be a natural number satisfying the inequality whereby $j \leq n$, so that ζ_n^{dj} is an arbitrary elements in the following cyclic subgroup:

$$\left\langle \zeta_n^d \right\rangle = \left\{\zeta_n^d, \zeta_n^{2d}, \ldots, \zeta_n^{\left(\frac{n}{d}-1\right)d}, 1\right\}.$$

We claim that ζ_n^{dj} is an $\left(\frac{n}{d}\right)^{\text{th}}$ root of unity. This is clear, since we have that

$$\left(\zeta_n^{dj}\right)^{\frac{n}{d}} = \zeta_n^{jn} = 1,$$

as desired.

Exercise 3.130. Prove that if a field contains the n^{th} roots of unity for n odd then it also contains the $2n^{\text{th}}$ roots of unity.

Solution 3.131. Assume that a field F contains the n^{th} roots of unity for n. Now, let γ be an arbitrary $2n^{\text{th}}$ root of unity. We thus have that:

$$\gamma^{2n} = 1.$$

Equivalently,

$$\gamma^{2n} - 1 = 0.$$

Therefore,

$$(\gamma^n - 1)(\gamma^n + 1) = 0.$$

There are two cases to consider. First, suppose that $\gamma^n - 1 = 0$. Then γ is an n^{th} root of unity, so that γ is in F, as desired. Now, suppose that $\gamma^n - 1 \neq 0$. So, from the equality

$$(\gamma^n - 1)(\gamma^n + 1) = 0.$$

we have that

$$\gamma^n + 1 = 0,$$

so that

$$\gamma^n = -1.$$

Therefore,

$$-(\gamma^n) = 1.$$

But recall that n is assumed to be odd. For the sake of clarity, write $n = 2m + 1$. Since

$$-\left(\gamma^{2m+1}\right) = 1.$$

we have that

$$\left((-1)\cdot\gamma\right)^{2m+1} = 1,$$

so that

$$(-\gamma)^n = 1.$$

So, we have that $-\gamma$ is an n^{th} root of unity. But recall that we assumed that the field F contains the n^{th} roots of unity. We thus have that $-\gamma$ must be in F. But since F is a field, F must be closed under additive inverses, so that $\gamma \in F$, as desired.

Exercise 3.132. Prove that if $n = p^k m$ where p is a prime and m is relatively prime to p then there are precisely m distinct n^{th} roots of unity over a field of characteristic p.

Solution 3.133. Our solution is based on a solution given in the following link:

`https://positron0802.files.wordpress.com/2017/01/`
`abstract-algebra-dummit-foote-chapter-13-field-theory-solutions.pdf`

Let F denote a fixed field of characteristic p. The roots of the polynomial $x^n - 1$ as an element in $F[x]$ are precisely the roots of:

$$x^{p^k m} - 1 = (x^m - 1)^{p^k} \in F[x].$$

So, we thus have that the roots of unity over F are the roots of $x^m - 1$ over F. Given that p and m are relatively prime, we have that $x^m - 1$ and mx^{m-1} are relatively prime. So, we have that $x^m - 1$ has no multiple roots. Therefore, the m distinct roots of $x^m - 1$ are precisely the n^{th} roots of unity over F.

3.15 Exercises from Section 14.1

Exercise 3.134. Show that if the field K is generated over F by the elements $\alpha_1, \dots, \alpha_n$ then an automorphism σ of K fixing F is uniquely determined by $\sigma(\alpha_1)$, …, $\sigma(\alpha_n)$. In particular show that an automorphism fixes K if and only if it fixes a set of generators for K.

Solution 3.135. Assume that the field K is generated over F by the elements $\alpha_1, \dots, \alpha_n$, with:

$$K = F(\alpha_1, \dots, \alpha_n).$$

So, we have that K consists precisely of expressions of the form

$$\frac{f_1\alpha_1^{i_1}\cdots\alpha_n^{i_n} + \cdots + f_m\alpha_1^{j_1}\cdots\alpha_n^{j_n}}{g_1\alpha_1^{k_1}\cdots\alpha_n^{k_n} + \cdots + g_{m'}\alpha_1^{\ell_1}\cdots\alpha_n^{\ell_n}}$$

where f_1, f_m, g_1, etc., are in F, and where expressions of the form i_1, i_n, etc., are element in $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$, and where the above denominator is nonzero. That is, elements of K are precisely quotients of F-linear combinations of products consisting of elements in $\{\alpha_1, \dots, \alpha_n\}$ by nonzero quotients of F-linear combinations of products consisting of elements in $\{\alpha_1, \dots, \alpha_n\}$. So, letting σ be an arbitrary automorphism of K fixing F, since σ is a ring homomorphism fixing F, we have that

$$\sigma\left(\frac{f_1\alpha_1^{i_1}\cdots\alpha_n^{i_n} + \cdots + f_m\alpha_1^{j_1}\cdots\alpha_n^{j_n}}{g_1\alpha_1^{k_1}\cdots\alpha_n^{k_n} + \cdots + g_{m'}\alpha_1^{\ell_1}\cdots\alpha_n^{\ell_n}}\right)$$

must be equal to

$$\frac{f_1\sigma(\alpha_1)^{i_1}\cdots\sigma(\alpha_n)^{i_n} + \cdots + f_m\sigma(\alpha_1)^{j_1}\cdots\sigma(\alpha_n)^{j_n}}{g_1\sigma(\alpha_1)^{k_1}\cdots\sigma(\alpha_n)^{k_n} + \cdots + g_{m'}\sigma(\alpha_1)^{\ell_1}\cdots\sigma(\alpha_n)^{\ell_n}}.$$

So, the value of

$$\sigma\left(\frac{f_1\alpha_1^{i_1}\cdots\alpha_n^{i_n} + \cdots + f_m\alpha_1^{j_1}\cdots\alpha_n^{j_n}}{g_1\alpha_1^{k_1}\cdots\alpha_n^{k_n} + \cdots + g_{m'}\alpha_1^{\ell_1}\cdots\alpha_n^{\ell_n}}\right)$$

is determined by expressions of the form $\sigma(\alpha_1)$, $\sigma(\alpha_2)$, …, $\sigma(\alpha_n)$. Since an element in the domain of σ may be written so as to contain each element in $\{\alpha_1, \dots, \alpha_n\}$ in a nontrivial way, we have that the behavior of σ is precisely determined by the values of $\sigma(\alpha_1)$, $\sigma(\alpha_2)$, …, $\sigma(\alpha_n)$. Observe that the bijectivity of σ was not used with respect to the above argument.

Now, suppose that σ is an automorphism fixing K, letting K be as given above. So, $\sigma(\alpha_i)$ must be equal to α_i for each index i. Conversely, suppose that $\sigma(\alpha_i) = \alpha_i$, where σ is an automorphism on K. If we also let σ fix the elements of F, then since

$$\sigma\left(\frac{f_1\alpha_1^{i_1}\cdots\alpha_n^{i_n} + \cdots + f_m\alpha_1^{j_1}\cdots\alpha_n^{j_n}}{g_1\alpha_1^{k_1}\cdots\alpha_n^{k_n} + \cdots + g_{m'}\alpha_1^{\ell_1}\cdots\alpha_n^{\ell_n}}\right)$$

equals

$$\frac{f_1\sigma(\alpha_1)^{i_1}\cdots\sigma(\alpha_n)^{i_n} + \cdots + f_m\sigma(\alpha_1)^{j_1}\cdots\sigma(\alpha_n)^{j_n}}{g_1\sigma(\alpha_1)^{k_1}\cdots\sigma(\alpha_n)^{k_n} + \cdots + g_{m'}\sigma(\alpha_1)^{\ell_1}\cdots\sigma(\alpha_n)^{\ell_n}}.$$

we have that σ must be the identity automorphism.

Exercise 3.136. Let $G \leq \mathrm{Gal}(K/F)$ be a subgroup of the Galois group of the extensiuon K/F and suppose $\sigma_1, \dots, \sigma_k$ are generators for G. Show that the subfield E/F is fixed by G if and only if it is fixed by the generators σ_1, …, σ_k.

Solution 3.137. Consider the field extension K/F. Since the Galois group $\mathrm{Gal}(K/F)$ is presently under consideration, we have that K is Galois over F, i.e., that K/F is a Galois extension, so that the equality

$$|\mathrm{Aut}\,(K/F)| = [K\ :\ F]$$

holds. Since K/F is Galois, we have that the group $\mathrm{Aut}(K/F)$ of automorphisms of K leaving F fixed is referred to as the Galois group of K/F and is denoted as $\mathrm{Gal}(K/F)$. We remark that K/F is a finite extension. As above, we assume that σ_1, …, σ_k are generators for the subgroup $G \leq \mathrm{Gal}(K/F)$.

($\Longrightarrow$) Assume that the subfield E/F is fixed by G. Since E/F is fixed by G, we have that each element of G fixes E/F. So, in particular, generators of G fix E/F.

($\Longleftarrow$) Conversely, assume that the subfield E/F is fixed by the given generators σ_1, …, σ_k for G. Since

$$G = \langle \sigma_1, \ldots, \sigma_k \rangle,$$

we find that: given an arbitrary element $g \in G$, we may write g as

$$g = \sigma_{i_1}^{j_1} \cdots \sigma_{i_n}^{j_n}$$

for some natural number $n \in \mathbb{N}$, where

$$i_1, i_2, \ldots, i_n \in \{1, 2, \ldots, k\}$$

and

$$j_1, j_2, \ldots, j_n \in \mathbb{Z}.$$

Now, given a generator ρ in the generating set

$$\{\sigma_1, \ldots, \sigma_k\} \subseteq \mathrm{Gal}(K/F),$$

we have that ρ fixes each element in F, and we have that ρ is such that $\rho(e) = e$ for each element $e \in E$, as we are working under the assumption that the subfield E of K is fixed by G. Since

$$\forall e \in E\ \rho(e) = e$$

we have that

$$\forall e \in E\ \rho^{-1}(e) = e,$$

which shows that E/F is also fixed by ρ^{-1}. An inductive argument shows that E/F is fixed by each expression of the form ρ^z for $z \in \mathbb{Z}$. So, letting

$$g = \sigma_{i_1}^{j_1} \cdots \sigma_{i_n}^{j_n}$$

be as given above, as an arbitrary element in G, and letting $e \in E$ be arbitrary, we find that:

$$\begin{aligned} g(e) &= \sigma_{i_1}^{j_1} \cdots \sigma_{i_{n-1}}^{j_{n-1}} \sigma_{i_n}^{j_n}(e) \\ &= \sigma_{i_1}^{j_1} \cdots \sigma_{i_{n-1}}^{j_{n-1}}(e) \\ &= \sigma_{i_1}^{j_1} \cdots \sigma_{i_{n-2}}^{j_{n-2}}(e) \\ &= \cdots \\ &= e. \end{aligned}$$

Exercise 3.138. Let τ be the map $\tau: \mathbb{C} \to \mathbb{C}$ defined by $\tau(a+bi) = a - bi$ (*complex conjugation*). Prove that τ is an automorphism of $\mathbb{C}$.

Solution 3.139. Let $a, b, c, d \in \mathbb{R}$, so that $a+bi$ and $c+di$ are arbitrary elements in the field $\mathbb{C}$ of complex numbers. Consider the mapping τ evaluated at the sum of $a+bi$ and $c+di$:

$$\begin{aligned}
\tau\left(a+bi+c+di\right) &= \tau\left(a+c+bi+di\right) \\
&= \tau\left(a+c+(b+d)i\right) \\
&= a+c-(b+d)i \\
&= a+c-bi-di \\
&= a-bi+c-di \\
&= \tau\left(a+bi\right)+\tau\left(c+di\right).
\end{aligned}$$

So, we find that complex conjugation preserves addition. Now, consider the mapping τ evaluated at the product of $a+bi$ and $c+di$:

$$\begin{aligned}
\tau\left(\left(a+bi\right)\left(c+di\right)\right) &= \tau\left(ac+adi+bci-bd\right) \\
&= \tau\left(ac-bd+adi+bci\right) \\
&= \tau\left(ac-bd+(ad+bc)i\right) \\
&= ac-bd-(ad+bc)i \\
&= ac-bd-adi-bci \\
&= ac-adi-bci-bd \\
&= \left(a-bi\right)\left(c-di\right) \\
&= \tau\left(a+bi\right)\tau\left(c+di\right).
\end{aligned}$$

Also, we have that $\tau(1)$ is equal to 1, from the definition of τ. So, we find that τ is a ring homomorphism from $\mathbb{C}$ to $\mathbb{C}$. That is, τ is a field homomorphism from $\mathbb{C}$ to $\mathbb{C}$. Now, to prove that τ is an automorphism[4], we must prove that τ is bijective. Given an arbitrary element $c+di$ in the codomain $\mathbb{C}$ of τ, we have that $c-di$ maps to $c+di$ under τ, thus establishing the surjectivity of τ. Now, suppose that

$$\tau(a+bi) = \tau(c+di).$$

From the equality

$$a - bi = c - di$$

we have that

$$\mathrm{Re}(a-bi) = \mathrm{Re}(c-di)$$

and that

$$\mathrm{Im}(a-bi) = \mathrm{Im}(c-di),$$

so that a and c must be equal, and b and d must be such that $b = d$. So, we have that

$$\tau(a+bi) = \tau(c+di) \Longrightarrow a+bi = c+di,$$

as desired.

[4] See `https://en.wikipedia.org/wiki/Automorphism`.

Exercise 3.140. Determine the fixed field of complex conjugation on $\mathbb{C}$.

Solution 3.141. We begin by recalling the following proposition from the class textbook.

"**Proposition 3.** Let $H \leq \text{Aut}(K)$ be a subgroup of the group of automorphisms of K. Then the collection F of elements of K fixed by all the elements of H is a subfield of K." (p. 560)

As stated in the class textbook, "Note that it is not important in this proposition that H actually be a *subgroup* of $\text{Aut}(K)$ – the collection of elements of K fixed by all the elements of a *subset* of $\text{Aut}(K)$ is also a subfield of K." (p. 560)

Now, consider the field $\mathbb{C}$ of complex numbers, and consider the singleton set $\{\sigma\}$ consisting of the $\mathbb{C}$-automorphism given by complex conjugation. The fixed field of complex conjugation on $\mathbb{C}$ consists precisely of elements of the form

$$a + bi \in \mathbb{C}$$

such that $a, b \in \mathbb{R}$, and such that

$$a + bi = a - bi.$$

So, we find that the collection of elements of $\mathbb{C}$ fixed by the complex conjugation automorphism consists precisely of elements of the form

$$a + bi \in \mathbb{C}$$

such that a is in $\mathbb{R}$ and such that

$$\text{Im}(a + bi) = \text{Im}(a - bi) = b = -b.$$

From the above equalities, we have that the fixed field of complex conjugation on $\mathbb{C}$ is $\mathbb{R}$.

Exercise 3.142. Prove that $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ are not isomorphic.

Solution 3.143. By way of contradiction, suppose that there exists a bijective ring homomorphism ϕ from $\mathbb{Q}(\sqrt{2})$ to $\mathbb{Q}(\sqrt{3})$. Since ϕ is a bijective ring homomorphism, we have that $\phi(q) = q$ for each element q in the prime field $\mathbb{Q}$, as may be verified inductively, using equalities such as $\phi(1) = 1$, $\phi(1 + 1) = 1 + 1$, etc. Now, since $(\sqrt{2})^2 = 2$, we have that $\phi(\sqrt{2})^2 = 2$. But then $\sqrt{2}$ or $-\sqrt{2}$ would have to be in the codomain of ϕ, $\mathbb{Q}(\sqrt{3})$. That is, we would have that

$$\sqrt{2} = q_1 + q_2\sqrt{3}$$

for some elements q_1 and q_2 in $\mathbb{Q}$. If we accept that $\sqrt{\frac{2}{3}}$ is irrational, then we have that q_1 is nonzero. If we accept that $\sqrt{2}$ is irrational, we have that q_2 is nonzero. So, since

$$2 = q_1^2 + 2\sqrt{3}q_1q_2 + 3q_2^2$$

and since q_2 and q_2 are nonzero, if we accept that $\sqrt{3}$ is irrational, we arrive at a contradiction.

Exercise 3.144. Determine the automorphisms of the extension $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ explicitly.

Solution 3.145. Let σ be an automorphism of $\mathbb{Q}(\sqrt[4]{2})$ fixing $\mathbb{Q}(\sqrt{2})$. Observe that the field $\mathbb{Q}(\sqrt[4]{2})$ is the splitting field for the polynomial $x^4 - 2$ over $\mathbb{Q}$. So, we have that σ must permute the roots of $x^4 - 2$. But furthermore, σ must map $\sqrt{2}$ to $\sqrt{2}$, and must map $-\sqrt{2}$ to $-\sqrt{2}$. So, σ is either the identity automorphism, or σ maps $\sqrt[4]{2}$ to $-\sqrt[4]{2}$ and maps $-\sqrt[4]{2}$ to its additive inverse.

Exercise 3.146. Let k be a field. Show that the mapping $\phi\colon k[t] \to k[t]$ defined by $\phi(f(t)) = f(at+b)$ for fixed $a, b \in k$, $a \neq 0$ is an automorphism of $k[t]$ which is the identity on k.

Solution 3.147. Let k and ϕ be as given above, letting $a, b \in k$ be fixed. Let $f(t)$ and $g(t)$ be polynomials in the domain of ϕ. Let $f = f(t)$ be denoted as

$$f(t) = a_n t^n + a_{n-1} t^{n-1} + \cdots + a_1 t + a_0$$

and let $g = g(t)$ be denoted as

$$g(t) = b_m t^m + b_{m-1} t^{m-1} + \cdots + b_1 t + b_0.$$

We may assume without loss of generality that $n \geq m$. Let the sum of f and g be denoted as follows:

$$f(t) + g(t) = \cdots + (a_m + b_m) t^m + \cdots + (a_0 + b_0).$$

So, we have that

$$\phi(f(t) + g(t)) = \cdots + (a_m + b_m)(at+b)^m + (a_{m-1} + b_{m-1})(at+b)^{m-1} + \cdots + (a_0 + b_0).$$

Expanding each expression of the form

$$(a_i + b_i)(at+b)^i = a_i(at+b)^i + b_i(at+b)^i$$

and rearranging the resultant terms, we see that $\phi(f(t) + g(t))$ is equal to $\phi(f(t)) + \phi(g(t))$. Now, consider the product of f and g. It is convenient for our purposes to let a_i vanish for $i > n$, and to let b_i vanish for $i > m$. We thus have that

$$\left(\sum_{i=0}^{\infty} a_i t^i \right) \cdot \left(\sum_{j=0}^{\infty} b_j t^j \right) = \sum_{k=0}^{\infty} \left(\sum_{\ell=0}^{k} a_\ell b_{k-\ell} \right) t^k.$$

So, we have that

$$\phi\left(\left(\sum_{i=0}^{\infty} a_i t^i \right) \cdot \left(\sum_{j=0}^{\infty} b_j t^j \right) \right) = \sum_{k=0}^{\infty} \left(\sum_{\ell=0}^{k} a_\ell b_{k-\ell} \right) (at+b)^k.$$

Through essentially the same convolution formula, we have that this is also equal to

$$\left(\sum_{i=0}^{\infty} a_i (at+b)^i \right) \cdot \left(\sum_{j=0}^{\infty} b_j (at+b)^j \right),$$

which shows that ϕ is a ring homomorphism, since $\phi(1) = 1$. So, it remains to show that ϕ is bijective.

Let $g = g(t)$ be an arbitrary element in the codomain of ϕ. Now, consider the expression $g\left(\frac{t-b}{a}\right)$. This is a well-defined polynomial in k, since k is a field and since a is nonzero. We have that

$$\phi\left(g\left(\frac{t-b}{a} \right) \right) = g\left(\frac{at+b-b}{a} \right) = g\left(t\right),$$

thus proving the surjectivity of ϕ. So, it remains to prove that ϕ is injective. Since ϕ is a ring homomorphism, it remains to prove that the kernel of ϕ is trivial. So, it remains to prove that the following set is trivial:

$$\ker(\phi) = \left\{ f(t) \in k[t] : f(at+b) = 0 \right\}.$$

But if we let f be denoted as

$$f(t) = a_n t^n + a_{n-1} t^{n-1} + \cdots + a_1 t + a_0$$

we have that

$$f(at+b) = a_n (at+b)^n + a_{n-1}(at+b)^{n-1} + \cdots + a_1(at+b) + a_0 = 0.$$

Recall that a is nonzero. Since

$$f(at+b) = a_n (at+b)^n + a_{n-1}(at+b)^{n-1} + \cdots + a_1(at+b) + a_0 = 0,$$

by the binomial theorem, the coefficient of t^n in the expansion of the above formula would have to be equal to $a_n a$, so that a_n would have to be equal to 0, since a is nonzero. Repeating this agument inductively shows that f must be trivial, as desired.

So, we have thus far shown that ϕ is an automorphism on $k[t]$. Now, consider the behaviour of ϕ on k. We have that $\phi(f(t)) = f(at+b)$ for each element $f(t)$ in the domain of ϕ. So, for a constant polynomial c in the domain of ϕ, we have that

$$\phi(c) = c\Big|_{at+b} = c,$$

which shows that ϕ is the identity on k.

Exercise 3.148. Conversely, let ϕ be an automorphism of $k[t]$ which is the identity on k. Prove that there exist $a, b \in k$ with $a \neq 0$ such that $\phi(f(t)) = f(at+b)$ as in the previous exercise.

Solution 3.149. As above, let ϕ be an automorphism of $k[t]$ which is the identity on k. So, we have that $\phi(c) = c$ for each constant polynomial c in $k[t]$. Now, consider the mapping ϕ evaluated at the polynomial $t \in k[t]$. We have that $\phi(t)$ cannot be equal to a constant polynomial, since ϕ is bijective and since $\phi(c) = c$ for each constant polynomial c in $k[t]$. By way of contradiction, suppose that the degree of $\phi(t)$ is greater than or equal to 2. But then given a non-constant polynomial

$$f(t) = a_n t^n + a_{n-1} t^{n-1} + \cdots + a_1 t + a_0$$

in $k[t]$, we have that the degree of $\phi(f(t))$ would have to be strictly greater than n, which would mean that no element in the domain of ϕ would map to a degree-1 polynomial under ϕ, contradicting the surjectivity of ϕ. So, since the degree of $\phi(t)$ cannot be strictly less than 1 and cannot be strictly greater than 1, we may deduce that the degree of $\phi(t)$ is equal to 1, so that there exist $a, b \in k$ with $a \neq 0$ such that $\phi(t) = at + b$. So, given a non-constant polynomial

$$f(t) = a_n t^n + a_{n-1} t^{n-1} + \cdots + a_1 t + a_0$$

in $k[t]$, since ϕ is a ring homomorphism, we have that:

$$\begin{aligned}
\phi(f(t)) &= \phi(a_n t^n + a_{n-1} t^{n-1} + \cdots + a_1 t + a_0) \\
&= \phi(a_n t^n) + \phi(a_{n-1} t^{n-1}) + \cdots + \phi(a_1 t) + \phi(a_0) \\
&= \phi(a_n)\phi(t^n) + \phi(a_{n-1})\phi(t^{n-1}) + \cdots + \phi(a_1)\phi(t) + \phi(a_0) \\
&= a_n \phi(t^n) + a_{n-1}\phi(t^{n-1}) + \cdots + a_1 \phi(t) + a_0 \\
&= a_n \phi(t)^n + a_{n-1}\phi(t)^{n-1} + \cdots + a_1 \phi(t) + a_0 \\
&= a_n (at+b)^n + a_{n-1}(at+b)^{n-1} + \cdots + a_1(at+b) + a_0 \\
&= f(at+b).
\end{aligned}$$

Exercise 3.150. The following exercises determine $\mathrm{Aut}(\mathbb{R}/\mathbb{Q})$. Prove that any $\sigma \in \mathrm{Aut}(\mathbb{R}/\mathbb{Q})$ takes squares to squares and takes positive reals to positive reals. Conclude that $a < b$ implies $\sigma a < \sigma b$ for every $a, b \in \mathbb{R}$.

Solution 3.151. Let σ denote an element in $\mathrm{Aut}(\mathbb{R}/\mathbb{Q})$. Now, let $r \in \mathbb{R}$, so that r^2 is a square in $\mathbb{R}$. Since σ is a ring homomorphism, we have that

$$\sigma(r^2) = \sigma(r)^2,$$

so that σ sends squares to squares. Now, recall that σ is a field automorphism. So, we have that $\sigma(0) = 0$. Since

$$\sigma(r^2) = \sigma(r)^2,$$

for positive $s = r^2 = (\sqrt{s})^2 > 0$, we have that $\sigma(s) = \sigma(r)^2$ is positive, by bijectivity of σ, since $\sigma(0) = 0$. Now, letting a and b be elements in $\mathbb{R}$, assume that $a < b$. Equivalently, $0 < b - a$. So, since $b - a$ is positive, we have that $0 < \sigma(b - a)$. Since σ is a ring homomorphism, we have that $0 < \sigma(b) - \sigma(a)$. Therefore, $\sigma(a) < \sigma(b)$.

Exercise 3.152. Letting σ be as given above, prove that $-\frac{1}{m} < a - b < \frac{1}{m}$ implies $-\frac{1}{m} < \sigma a - \sigma b < \frac{1}{m}$ for every positive integer m. Conclude that σ is a continuous map on $\mathbb{R}$.

Solution 3.153. Letting m be a positive integer, assume that $-\frac{1}{m} < a - b < \frac{1}{m}$. So, we have that

$$-1 < ma - mb < 1.$$

First suppose that $ma - mb$ is positive. Then

$$-1 < \sigma(ma - mb) < \sigma(1),$$

from our results from Exercise 3.150. Furthermore, since σ is a field automorphism, we have that σ must map the multiplicative identity element in its domain to 1, so that

$$-1 < \sigma(ma - mb) < 1.$$

Since σ is a ring homomorphism, we have that

$$-1 < \sigma(m)\sigma(a) - \sigma(m)\sigma(b) < 1,$$

and since $\sigma(m)$ is positive from our results from Exercise 3.150, we have that

$$-\frac{1}{\sigma(m)} < \sigma(a) - \sigma(b) < \frac{1}{\sigma(m)}.$$

Now, recall that $m \in \mathbb{N}$ is a positive integer. Since σ is a field automorphism, we have that

$$\begin{aligned}\sigma(m) &= \sigma\left(\underbrace{1 + 1 + \cdots + 1}_{m\in\mathbb{N}}\right)\\ &= \underbrace{\sigma(1) + \sigma(1) + \cdots + \sigma(1)}_{m\in\mathbb{N}}\\ &= \underbrace{1 + 1 + \cdots + 1}_{m\in\mathbb{N}}\end{aligned}$$

$$= m.$$

So, since

$$-\frac{1}{\sigma(m)} < \sigma(a) - \sigma(b) < \frac{1}{\sigma(m)},$$

we have that

$$-\frac{1}{m} < \sigma a - \sigma b < \frac{1}{m},$$

as desired. So, for all $\epsilon > 0$, letting $m \in \mathbb{N}$ be such that $\frac{1}{m} < \epsilon$, and letting $\delta > 0$ be such that $\delta = \frac{1}{m}$, we have that if

$$-\delta < a - b < \delta$$

then

$$-\epsilon < \sigma a - \sigma b < \epsilon,$$

thus proving that σ is continuous on $\mathbb{R}$.

Exercise 3.154. Prove that any continuous map on $\mathbb{R}$ which is the identity on $\mathbb{Q}$ is the identity map, and hence $\mathrm{Aut}(\mathbb{R}/\mathbb{Q}) = 1$.

Solution 3.155. Let $f{:}\mathbb{R} \to \mathbb{R}$ be a continuous map which is the identity on $\mathbb{Q}$. So, we have that $f(q) = q$ for all $q \in \mathbb{Q} \subseteq \mathbb{R}$. Now, let i be an irrational number in the domain of f. We can find a rational number r which is arbitrarily close to i, and we can formalize this idea using Dedekind cuts and Cauchy sequences. So, we can construct a sequence

$$(r_1, r_2, \ldots)$$

of rational numbers such that $\lim_{j\to\infty} r_j = i$. Since f is continuous, we have that $\lim_{j\to\infty} f(r_j) = f(i) = i$, as desired. We have shown that if σ is an element in $\mathrm{Aut}(\mathbb{R}/\mathbb{Q})$, then σ must be continuous. So, given that $\sigma \in \mathrm{Aut}(\mathbb{R}/\mathbb{Q})$, we have that σ must be continuous and must be the identity on $\mathbb{Q}$, which shows that σ must be the identity on $\mathbb{R}$.

Exercise 3.156. Prove that the automorphisms of the rational function field $k(t)$ which fix k are precisely the *fractional linear transformations* determined by $t \mapsto \frac{at+b}{ct+d}$ for $a, b, c, d \in k$, $ad - bc \neq 0$ (so $f(t) \in k(t)$ maps to $f(\frac{at+b}{ct+d})$).

Solution 3.157. Suppose that σ is an automorphism of the rational function field $k(t)$ which fixes k. Consider the expression $\sigma(t)$. We know that $\sigma(\alpha) = \alpha$ for each constant α in k, and since σ is bijective, we have that $\sigma(t)$ cannot be equal to a constant in k. Now, by way of contradiction, suppose that $\sigma(t)$ is equal to a rational function of the form $\frac{p(t)}{q(t)}$ where $p(t)$ and $q(t)$ are both polynomials in $k[x]$ such that the degree of $p(t)$ is greater than or equal to 2, and such that the fraction $\frac{p(t)}{q(t)}$ is written in lowest terms. But then a rational function of the form

$$\frac{\alpha t + \beta}{\gamma t + \delta}$$

would be mapped to

$$\frac{\alpha\left(\frac{p(t)}{q(t)}\right) + \beta}{\gamma\left(\frac{p(t)}{q(t)}\right) + \delta},$$

with $\frac{p(t)}{q(t)}$ written in lowest terms, letting $\frac{\alpha\left(\frac{p(t)}{q(t)}\right)+\beta}{\gamma\left(\frac{p(t)}{q(t)}\right)+\delta}$ also be written in lowest terms. So,

$$\frac{\alpha t+\beta}{\gamma t+\delta}$$

would have to be mapped to a quotient involving a polynomial of degree at least two, in lowest terms, and a symmetric argument applies in the case whereby $q(t)$ is of degree greater than or equal to 2. More generally, a quotient of the form $\frac{r(t)}{s(t)}$ would have to be mapped to a quotient involving a polynomial of degree at least $2n$, in lowest terms, letting $r(t)$ or $s(t)$ be of degree $n \in \mathbb{N}$. But then nothing would be mapped to nonconstant quotients of polynomials of degree at most 1 by linear polynomials, contradicting the bijectivity of σ. So, from the above discussion, we have that $\sigma(t)$ must be mapped to an expression of the form $\frac{at+b}{ct+d}$, where $a, b, c, d \in k$. In order for σ to be bijective, we must have that the restriction of σ to well-defined quotients of the form

$$\frac{\alpha t+\beta}{\gamma t+\delta}$$

is bijective, from our previous discussion. By way of contradiction, suppose that $ad = bc$. From the equality $ad = bc$, we have that σ would have to map t to the following:

$$\begin{aligned}\frac{at+b}{ct+d} &= \frac{adt+bd}{d(ct+d)}\\ &= \frac{bct+bd}{d(ct+d)}\\ &= \frac{b(ct+d)}{d(ct+d)}\\ &= \frac{b}{d}.\end{aligned}$$

But this is impossible, since $\sigma(t)$ cannot be a constant in k, by bijectivity of σ.

Exercise 3.158. Determine the fixed field of the automorphism $t \mapsto t+1$ of $k(t)$.

Solution 3.159. Let $\sigma: k(t) \to k(t)$ denote the automorphism on $k(t)$ whereby $t \mapsto t+1$. Observe that each element in k is fixed by this morphsim. Now, consider the set of all elements in $k(t)$ that are fixed by this morphism. Let

$$f(t) = a_n t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0$$

be a polynomial in $k[t]$, and let

$$g(t) = b_m t^m + b_{m-1}t^{m-1} + \cdots + b_1 t + b_0$$

be a nonzero polynomial in $k[t]$, so that $\frac{f(t)}{g(t)}$ is an element in $k(t)$. Let the quotient $\frac{f(t)}{g(t)}$ be in lowest terms. Now, suppose that this element is fixed under the morphism σ given above. We thus have that

$$\frac{a_n t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0}{b_m t^m + b_{m-1}t^{m-1} + \cdots + b_1 t + b_0}$$

is equal to

$$\frac{a_n(t+1)^n + a_{n-1}(t+1)^{n-1} + \cdots + a_1(t+1) + a_0}{b_m(t+1)^m + b_{m-1}(t+1)^{m-1} + \cdots + b_1(t+1) + b_0}.$$

Expanding the numerator and the denominator of this latter rational expression using the binomial theorem, we see that this polynomial may be written as

$$\frac{f(t)+\alpha(t)}{g(t)+\beta(t)}$$

where the degree of α is strictly less than the degree of f and the degree of β is strictly less than the degree of g. So, unless f and g are both constant polynomials, it would be impossible for

$$\frac{f(t)}{g(t)}$$

to be equal to

$$\frac{f(t)+\alpha(t)}{g(t)+\beta(t)},$$

because if

$$f(t)g(t)+f(t)\beta(t)=f(t)g(t)+g(t)\alpha(t)$$

then

$$f(t)\beta(t)=g(t)\alpha(t)$$

so that

$$\frac{f(t)}{g(t)}=\frac{\alpha(t)}{\beta(t)}$$

which contradicts that f and g are in lowest terms, since the degree of α is strictly less than that of f, and the degree of β is strictly less than g. So, we have that the fixed field of the given morphism is k.

Exercise 3.160. Let K be an extension of the field F. Let $\phi\colon K\to K'$ be an isomorphism of K with a field K' which maps F to the subfield F' of K'. Prove that the map $\sigma\mapsto\phi\sigma\phi^{-1}$ defines a group isomorphism $\mathrm{Aut}(K/F)\xrightarrow{\sim}\mathrm{Aut}(K'/F')$.

Solution 3.161. Define the mapping

$$\Psi\colon\mathrm{Aut}(K/F)\to\mathrm{Aut}(K'/F')$$

so that: given an arbitrary element σ in $\mathrm{Aut}(K/F)$, $\Psi(\sigma)=\phi\sigma\phi^{-1}$, where ϕ is as given above, with $\phi\colon K\to K'$ as an isomorphism of K to K' which maps F to the subfield F' of K'. We observe that Ψ is well-defined in the sense that ϕ is invertible so that the composition $\phi\sigma\phi^{-1}$ is well-defined as a mapping from K' to K'. Furthermore, since ϕ, σ, and ϕ^{-1} are all isomorphisms, we have that $\phi\sigma\phi^{-1}$ is an isomorphism from K' to K'. That is, $\phi\sigma\phi^{-1}$ is an automorphism on K'. We claim that $\phi\sigma\phi^{-1}$ fixes F'. Since ϕ maps F to the subfield F' of K', we may deduce that ϕ^{-1} maps F' to F. Now, recall that σ is an element in $\mathrm{Aut}(K/F)$. So, we find that σ maps F to F. Again since ϕ maps F to F', we may conclude that the product $\phi\sigma\phi^{-1}$ maps F' to F'. So, we have thus far shown that the mapping Ψ given above is well-defined in the sense that $\Psi(\sigma)$ is an element in the given codomain of Ψ for each element σ in the domain of Ψ.

Now, let σ and ρ be elements in the domain of Ψ, and consider the composition $\sigma\circ\rho$:

$$\begin{aligned}\Psi(\sigma\circ\rho)&=\phi\circ\sigma\circ\rho\circ\phi^{-1}\\&=\phi\circ\sigma\circ\phi^{-1}\circ\phi\circ\rho\circ\phi^{-1}\end{aligned}$$

$$\begin{aligned} &= \left(\phi \circ \sigma \circ \phi^{-1}\right) \circ \left(\phi \circ \rho \circ \phi^{-1}\right) \\ &= \Psi(\sigma) \circ \Psi(\rho). \end{aligned}$$

So, we have that Ψ is a group homomorphism, as desired. Letting σ and ρ be as given above, we have that:

$$\begin{aligned} \Psi(\sigma) = \Psi(\rho) &\Longrightarrow \phi\sigma\phi^{-1} = \phi\rho\phi^{-1} \\ &\Longrightarrow \phi^{-1}\phi\sigma\phi^{-1} = \phi^{-1}\phi\rho\phi^{-1} \\ &\Longrightarrow \sigma\phi^{-1} = \rho\phi^{-1} \\ &\Longrightarrow \sigma\phi^{-1}\phi = \rho\phi^{-1}\phi \\ &\Longrightarrow \sigma = \rho. \end{aligned}$$

So, we have that Ψ is injective. Now, let θ be an arbitrary element in the codomain of Ψ. So, we have that θ is an automorphism on K' fixing F'. Since $\phi^{-1}\theta\phi$ is an isomorphism from K to K fixing F, we have that $\phi^{-1}\theta\phi$ is in the domain of Ψ, and we have that Ψ evaluated at $\phi^{-1}\theta\phi$ is θ.

3.16 Exercises from Section 14.2

Exercise 3.162. Determine the minimal polynomial over $\mathbb{Q}$ for the element $\sqrt{2} + \sqrt{5}$.

Solution 3.163. Let the element $\sqrt{2} + \sqrt{5}$ be denoted as $\alpha = \sqrt{2} + \sqrt{5}$. By the binomial theorem, we have that:

$$\alpha^2 = 2\sqrt{2}\sqrt{5} + 7.$$

So, we have that

$$\alpha^2 - 7 = 2\sqrt{2}\sqrt{5}.$$

That is,

$$(\alpha^2 - 7)^2 = 40.$$

So, we have that

$$\alpha^4 - 14\alpha^2 + 9 = 0.$$

So, we find that α is a root of the following degree-4 polynomial in $\mathbb{Q}[x]$:

$$x^4 - 14x^2 + 9 \in \mathbb{Q}[x].$$

Letting x^2 be denoted as γ, from the equation

$$x^4 - 14x^2 + 9 = 0$$

we have that

$$\gamma^2 - 14\gamma + 9 = 0$$

so that

$$x = \pm\sqrt{\frac{14 \pm \sqrt{160}}{2}}.$$

No root of the form

$$x = \pm\sqrt{\frac{14 \pm \sqrt{160}}{2}}$$

and no product of two distinct roots of the form

$$x = \pm\sqrt{\frac{14 \pm \sqrt{160}}{2}}$$

is rational. This shows that the minimal polynomial for $\sqrt{2} + \sqrt{5}$ over $\mathbb{Q}$ is equal to $x^4 - 14x^2 + 9$.

Exercise 3.164. Determine the minimal polynomial over $\mathbb{Q}$ for the element $1 + \sqrt[3]{2} + \sqrt[3]{4}$.

Solution 3.165. Let $1 + \sqrt[3]{2} + \sqrt[3]{4}$ be denoted as α. We thus have that

$$\alpha - 1 = \sqrt[3]{2} + \sqrt[3]{4}$$

so that

$$\alpha - 1 = \sqrt[3]{2} + (\sqrt[3]{2})^2.$$

Therefore,

$$\alpha - 1 = \sqrt[3]{2}(1 + \sqrt[3]{2}).$$

By the binomial theorem, we find that:

$$\frac{1}{2}(\alpha - 1)^3 = 2 + 3(\sqrt[3]{2})^2 + 3\sqrt[3]{2} + 1.$$

Therefore,

$$\frac{1}{2}(\alpha - 1)^3 - 3 = 3(\sqrt[3]{2})^2 + 3\sqrt[3]{2}.$$

Since $\alpha - 1 = \sqrt[3]{2} + (\sqrt[3]{2})^2$, we have that

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

That is,

$$(\alpha - 1)^3 = 6\alpha.$$

That is,

$$\alpha^3 - 3\alpha^2 - 3\alpha - 1 = 0.$$

We thus have that $1 + \sqrt[3]{2} + \sqrt[3]{4}$ is a root of the following polynomial in $\mathbb{Q}[x]$:

$$x^3 - 3x^2 - 3x - 1 \in \mathbb{Q}[x].$$

Since $x^3 - 3x^2 - 3x - 1$ is a degree-3 polynomial in $\mathbb{Q}[x]$, if this polynomial were reducible over $\mathbb{Q}$, then $x^3 - 3x^2 - 3x - 1$ would have to factor into a degree-1 polynomial in $\mathbb{Q}[x]$ and a degree-2 polynomial in $\mathbb{Q}[x]$. By the quadratic formula, we have that $1 + \sqrt[3]{2} + \sqrt[3]{4}$ cannot be a root of a quadratic element in $\mathbb{Q}[x]$, which shows that $x^3 - 3x^2 - 3x - 1$ must be irreducible as an element in $\mathbb{Q}[x]$. We may thus conclude that the monic polynomial $x^3 - 3x^2 - 3x - 1$ is the minimal polynomial over $\mathbb{Q}$ for the element $1 + \sqrt[3]{2} + \sqrt[3]{4}$.

Exercise 3.166. Determine the Galois group of $(x^2 - 2)(x^2 - 3)(x^2 - 5)$. Determine *all* the subfields of the splitting field of this polynomial.

Solution 3.167. We begin by recalling some definitions from the class textbook.

"**Definition.** Let K/F be a finite extension. Then K is said to be *Galois* over F and K/F is a *Galois* extension if $|\mathrm{Aut}(K/F)| = [K : F]$. If K/F is Galois the group of automorphisms $\mathrm{Aut}(K/F)$ is called the *Galois group of* K/F, denoted $\mathrm{Gal}(K/F)$." (p. 562)

"**Definition.** If $f(x)$ is a separable polynomial over F, then the *Galois group of* $f(x)$ *over* F is the Galois group of the splitting field of $f(x)$ over F." (p. 563)

Now, consider the given polynomial $(x^2-2)(x^2-3)(x^2-5)$ as an element in $\mathbb{Q}[x]$. This polynomial does not have any repeated roots, so $(x^2-2)(x^2-3)(x^2-5)$ is a separable polynomial over $\mathbb{Q}$. So, we have that the Galois group of $f(x) = (x^2-2)(x^2-3)(x^2-5)$ over $\mathbb{Q}$ is the Galois group of the splitting field of $f(x)$ over $\mathbb{Q}$.

Now, consider the splitting field of $f(x)$ over $\mathbb{Q}$. Since the roots of $(x^2-2)(x^2-3)(x^2-5)$ are precisely the elements in $\{\pm\sqrt{2}, \pm\sqrt{3}, \pm\sqrt{5}\}$, we have that the splitting field of $f(x)$ over $\mathbb{Q}$ is precisely $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$. So, we need to evaluate the following group of automorphisms:

$$\mathrm{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q}).$$

Now, let σ be an element in $\mathrm{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q})$. Since $(\sqrt{2})^2 = 2$, and since σ is a ring homomorphism fixing the base field $\mathbb{Q}$, we have that

$$\sigma\left((\sqrt{2})^2\right) = \left(\sigma(\sqrt{2})\right)^2 = \sigma(2) = 2.$$

So, we have that $\sigma(\sqrt{2}) \in \{\sqrt{2}, -\sqrt{2}\}$. In a similar fashion, we have that $\sigma(\sqrt{3}) \in \{\sqrt{3}, -\sqrt{3}\}$ and that $\sigma(\sqrt{5}) \in \{\sqrt{5}, -\sqrt{5}\}$. So, we obtain a total of 8 automorphisms in $\mathrm{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q})$. For a bit word w in $\{000, 001, \dots, 111\}$, letting w_i denote the i^{t} letter in w from the left, let σ_w be such that $\sigma_w(\sqrt{2}) = (\sqrt{2}, -\sqrt{2})_{w_1+1}$, $\sigma_w(\sqrt{3}) = (\sqrt{3}, -\sqrt{3})_{w_2+1}$, and $\sigma_w(\sqrt{5}) = (\sqrt{5}, -\sqrt{5})_{w_3+1}$. Given an automorphism σ in $\mathrm{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q})$, we have that $\sigma \circ \sigma$ must be the identity automorphism on $\mathrm{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q})$, since if $\sigma(\sqrt{2}) = \sqrt{2}$ then $\sigma^2(\sqrt{2}) = \sqrt{2}$, if $\sigma(\sqrt{2}) = -\sqrt{2}$ then $\sigma^2(\sqrt{2}) = \sqrt{2}$, etc. In general, if a group G is such that $g^2 = e$ for each element g in G, then G must be abelian, as may be verified by noting that for elements a and b in G, we have that $abab = e$ implies that $ba = ab$. So, we have that $\mathrm{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q})$ is an abelian group of order 8 such that σ^2 is the identity automorphism on $\mathrm{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q})$ for each element σ in $\mathrm{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q})$. So, we have that:

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}).$$

Now, consider the subgroups of $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q})$. The subgroups of this group are listed below.

$$\begin{gathered}
\{\sigma_{000}\} \\
\{\sigma_{000}, \sigma_{001}\} \\
\{\sigma_{000}, \sigma_{010}\} \\
\{\sigma_{000}, \sigma_{011}\} \\
\{\sigma_{000}, \sigma_{100}\} \\
\{\sigma_{000}, \sigma_{101}\} \\
\{\sigma_{000}, \sigma_{110}\} \\
\{\sigma_{000}, \sigma_{111}\}
\end{gathered}$$

$$\{\sigma_{000}, \sigma_{001}, \sigma_{010}, \sigma_{011}\}$$
$$\{\sigma_{000}, \sigma_{001}, \sigma_{100}, \sigma_{101}\}$$
$$\{\sigma_{000}, \sigma_{001}, \sigma_{110}, \sigma_{111}\}$$
$$\{\sigma_{000}, \sigma_{010}, \sigma_{100}, \sigma_{110}\}$$
$$\{\sigma_{000}, \sigma_{010}, \sigma_{101}, \sigma_{111}\}$$
$$\{\sigma_{000}, \sigma_{011}, \sigma_{100}, \sigma_{111}\}$$
$$\{\sigma_{000}, \sigma_{011}, \sigma_{101}, \sigma_{110}\}$$
$$\{\sigma_{000}, \sigma_{001}, \sigma_{010}, \sigma_{011}, \sigma_{100}, \sigma_{101}, \sigma_{110}, \sigma_{111}\}$$

So, it remains to determine the fixed fields corresponding to the above subgroups. Of course, the fixed field for the trivial subgroup is $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$. In general, an element in $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ is of the following form:

$$q_1 + q_2\sqrt{2} + q_3\sqrt{3} + q_4\sqrt{5} + q_5\sqrt{2}\sqrt{3} + q_6\sqrt{2}\sqrt{5} + q_7\sqrt{3}\sqrt{5} + q_8\sqrt{2}\sqrt{3}\sqrt{5}.$$

So, the fixed field for $\{\sigma_{000}, \sigma_{001}\}$ is equal to $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Similarly, the fixed field for $\{\sigma_{000}, \sigma_{010}\}$ is $\mathbb{Q}(\sqrt{2}, \sqrt{5})$.

Now, the elements in the subfield fixed by all of the elements in $\{\sigma_{000}, \sigma_{011}\}$ are precisely elements of the following form:

$$q_1 + q_2\sqrt{2} + q_7\sqrt{3}\sqrt{5} + q_8\sqrt{2}\sqrt{3}\sqrt{5}.$$

So, the subfield fixed by all of the elements in $\{\sigma_{000}, \sigma_{011}\}$ is equal to $\mathbb{Q}(\sqrt{2}, \sqrt{15})$. Similarly, the subfield field by all of the elements in $\{\sigma_{000}, \sigma_{100}\}$ is equal to $\mathbb{Q}(\sqrt{3}, \sqrt{5})$.

Now, consider the elements in the subfield fixed by all of the elements in $\{\sigma_{000}, \sigma_{101}\}$. These elements are precisely elements of the form

$$q_1 + q_3\sqrt{3} + q_6\sqrt{2}\sqrt{5} + q_8\sqrt{2}\sqrt{3}\sqrt{5}.$$

So, the subfield fixed by all of the elements in $\{\sigma_{000}, \sigma_{101}\}$ is equal to $\mathbb{Q}(\sqrt{3}, \sqrt{10})$. Similarly, the subfield fixed by all of the elements in $\{\sigma_{000}, \sigma_{110}\}$ is $\mathbb{Q}(\sqrt{5}, \sqrt{6})$. Now, consider the subfield fixed by all of the elements in $\{\sigma_{000}, \sigma_{111}\}$. An element

$$q_1 + q_2\sqrt{2} + q_3\sqrt{3} + q_4\sqrt{5} + q_5\sqrt{2}\sqrt{3} + q_6\sqrt{2}\sqrt{5} + q_7\sqrt{3}\sqrt{5} + q_8\sqrt{2}\sqrt{3}\sqrt{5}$$

in $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ is fixed by all of the elements in $\{\sigma_{000}, \sigma_{111}\}$ if and only if this element is of the form:

$$q_1 + q_5\sqrt{2}\sqrt{3} + q_6\sqrt{2}\sqrt{5} + q_7\sqrt{3}\sqrt{5},$$

for $q_1, q_5, q_6, q_7 \in \mathbb{Q}$. Now, consider the following computations.

$$\left(\sqrt{2}\sqrt{3}\right) \cdot \left(\sqrt{2}\sqrt{5}\right) = 2\sqrt{3}\sqrt{5}$$
$$\left(\sqrt{2}\sqrt{3}\right) \cdot \left(\sqrt{3}\sqrt{5}\right) = 3\sqrt{2}\sqrt{5}$$
$$\left(\sqrt{2}\sqrt{5}\right) \cdot \left(\sqrt{3}\sqrt{5}\right) = 5\sqrt{2}\sqrt{3}$$

From the above computations, we find that the subfield of $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ fixed by all of the elements in $\{\sigma_{000}, \sigma_{111}\}$ is equal to $\mathbb{Q}(\sqrt{2}\sqrt{3}, \sqrt{2}\sqrt{5}, \sqrt{3}\sqrt{5})$. So, we have thus far established the following correspondences.

Subgroup of Galois group	Fixed field
$\{\sigma_{000}\}$	$\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$
$\{\sigma_{000}, \sigma_{001}\}$	$\mathbb{Q}(\sqrt{2}, \sqrt{3})$
$\{\sigma_{000}, \sigma_{010}\}$	$\mathbb{Q}(\sqrt{2}, \sqrt{5})$
$\{\sigma_{000}, \sigma_{011}\}$	$\mathbb{Q}(\sqrt{2}, \sqrt{15})$
$\{\sigma_{000}, \sigma_{100}\}$	$\mathbb{Q}(\sqrt{3}, \sqrt{5})$
$\{\sigma_{000}, \sigma_{101}\}$	$\mathbb{Q}(\sqrt{3}, \sqrt{10})$
$\{\sigma_{000}, \sigma_{110}\}$	$\mathbb{Q}(\sqrt{5}, \sqrt{6})$
$\{\sigma_{000}, \sigma_{111}\}$	$\mathbb{Q}(\sqrt{6}, \sqrt{10}, \sqrt{15})$

Now, consider the subfield of $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ fixed by all of the elements of $\{\sigma_{000}, \sigma_{001}, \sigma_{010}, \sigma_{011}\}$. Now, recall that an element in $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ must be of the following form:

$$q_1 + q_2\sqrt{2} + q_3\sqrt{3} + q_4\sqrt{5} + q_5\sqrt{2}\sqrt{3} + q_6\sqrt{2}\sqrt{5} + q_7\sqrt{3}\sqrt{5} + q_8\sqrt{2}\sqrt{3}\sqrt{5}.$$

Elements fixed by σ_{001} must be of the following form:

$$q_1 + q_2\sqrt{2} + q_3\sqrt{3} + q_5\sqrt{2}\sqrt{3}.$$

Elements fixed by σ_{001} and σ_{010} must be of the following form:

$$q_1 + q_2\sqrt{2}.$$

Elements of this form must be fixed by σ_{011}. So, we have that the subfield fixed by the Klein four-subgroup $\{\sigma_{000}, \sigma_{001}, \sigma_{010}, \sigma_{011}\}$ is equal to $\mathbb{Q}(\sqrt{2})$. Similarly, the subfield fixed by the Klein four-subgroup $\{\sigma_{000}, \sigma_{001}, \sigma_{100}, \sigma_{101}\}$ is $\mathbb{Q}(\sqrt{3})$. Now, consider the subfield fixed by all of the morphisms in $\{\sigma_{000}, \sigma_{001}, \sigma_{110}, \sigma_{111}\}$. An element in $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ is fixed by σ_{111} if and only if it is of the form

$$q_1 + q_5\sqrt{2}\sqrt{3} + q_6\sqrt{2}\sqrt{5} + q_7\sqrt{3}\sqrt{5}.$$

So, an element in $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ is fixed by both σ_{111} and σ_{001} if and only if it is of the form

$$q_1 + q_5\sqrt{2}\sqrt{3}.$$

So, we find that the subfield fixed by all of the elements in the $\{\sigma_{000}, \sigma_{001}, \sigma_{110}, \sigma_{111}\}$ is equal to $\mathbb{Q}(\sqrt{6})$. We omit explanations for the remaining computations for this problem. All of the possible subfields are listed in the following table.

Subgroup of Galois group	Fixed field
$\{\sigma_{000}\}$	$\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$
$\{\sigma_{000}, \sigma_{001}\}$	$\mathbb{Q}(\sqrt{2}, \sqrt{3})$
$\{\sigma_{000}, \sigma_{010}\}$	$\mathbb{Q}(\sqrt{2}, \sqrt{5})$
$\{\sigma_{000}, \sigma_{011}\}$	$\mathbb{Q}(\sqrt{2}, \sqrt{15})$
$\{\sigma_{000}, \sigma_{100}\}$	$\mathbb{Q}(\sqrt{3}, \sqrt{5})$
$\{\sigma_{000}, \sigma_{101}\}$	$\mathbb{Q}(\sqrt{3}, \sqrt{10})$
$\{\sigma_{000}, \sigma_{110}\}$	$\mathbb{Q}(\sqrt{5}, \sqrt{6})$
$\{\sigma_{000}, \sigma_{111}\}$	$\mathbb{Q}(\sqrt{6}, \sqrt{10}, \sqrt{15})$
$\{\sigma_{000}, \sigma_{001}, \sigma_{010}, \sigma_{011}\}$	$\mathbb{Q}(\sqrt{2})$
$\{\sigma_{000}, \sigma_{001}, \sigma_{100}, \sigma_{101}\}$	$\mathbb{Q}(\sqrt{3})$
$\{\sigma_{000}, \sigma_{001}, \sigma_{110}, \sigma_{111}\}$	$\mathbb{Q}(\sqrt{6})$
$\{\sigma_{000}, \sigma_{010}, \sigma_{100}, \sigma_{110}\}$	$\mathbb{Q}(\sqrt{5})$
$\{\sigma_{000}, \sigma_{010}, \sigma_{101}, \sigma_{111}\}$	$\mathbb{Q}(\sqrt{10})$
$\{\sigma_{000}, \sigma_{011}, \sigma_{100}, \sigma_{111}\}$	$\mathbb{Q}(\sqrt{15})$
$\{\sigma_{000}, \sigma_{011}, \sigma_{101}, \sigma_{110}\}$	$\mathbb{Q}(\sqrt{30})$
$\{\sigma_{000}, \sigma_{001}, \sigma_{010}, \sigma_{011}, \sigma_{100}, \sigma_{101}, \sigma_{110}, \sigma_{111}\}$	$\mathbb{Q}$

Exercise 3.168. Let p be a prime. Determine the elements of the Galois group of $x^p - 2$.

Solution 3.169. Let $\sqrt[p]{2}$ denote the unique real p^{th} root of $x^p - 2$. Letting ζ_p denote a fixed primitive p^{th} root of unity, we have that the roots of $x^p - 2$ are precisely:

$$\zeta_p \sqrt[p]{2}, \zeta_p^2 \sqrt[p]{2}, \dots, \zeta_p^{p-1} \sqrt[p]{2}, \sqrt[p]{2}.$$

We thus find that $x^p - 2$ has no repeated roots, so that $x^p - 2$ is separable over $\mathbb{Q}$. The splitting field of $x^p - 2$ over $\mathbb{Q}$ is equal to:

$$\mathbb{Q}(\zeta_p, \sqrt[p]{2}).$$

Given an automorphism σ of $\mathbb{Q}(\zeta_p, \sqrt[p]{2})$ fixing $\mathbb{Q}$, we have that σ must permute the roots of $x^p - 2$. In particular, we have that the behaviour of σ is entirely determined by the values of $\sigma(\zeta_p)$ and $\sigma(\sqrt[p]{2})$. Since p is a prime, we have that there are $p - 1$ possible choices for the value of $\sigma(\zeta_p)$. There are also p choices for the value of $\sigma(\sqrt[p]{2})$. So, the Galois group for $x^p - 2$ consists of $p(p - 1)$ elements, given by $p - 1$ possible choices for the value of $\sigma(\zeta_p)$, and p choices for the value of $\sigma(\sqrt[p]{2})$.

Exercise 3.170. Prove that the Galois group of $x^p - 2$ for p a prime is isomorphic to the group of matrices $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ were $a, b \in \mathbb{F}_p$, $a \neq 0$.

Solution 3.171. Given an element ζ_p^i in $\{\zeta_p, \zeta_p^2, \dots, \zeta_p^{p-1}\}$, with $i \in \{1, 2, \dots, p-1\}$, and given an element $\zeta_p^j \sqrt[p]{2}$ in

$$\{\zeta_p \sqrt[p]{2}, \zeta_p^2 \sqrt[p]{2}, \dots, \zeta_p^{p-1} \sqrt[p]{2}, \sqrt[p]{2}\},$$

with $j \in \{0, 1, 2, \dots, p - 1\}$, let $\sigma_{i,j}$ denote the unique element in the Galois group for $x^p - 2$ mapping ζ_p to ζ_p^i, and mapping $\sqrt[p]{2}$ to $\zeta_p^j \sqrt[p]{2}$. Let the elements in $\mathbb{F}_p$ be denoted in the following manner:

$$\mathbb{F}_p = \{0, 1, \dots, p - 1\}.$$

Let Ψ denote the mapping from the Galois group of $x^p - 2$ to

$$\left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a, b \in \mathbb{F}_p, a \neq 0 \right\},$$

such that Ψ maps $\sigma_{i,j}$ to $\begin{pmatrix} i & j \\ 0 & 1 \end{pmatrix}$. We remark that this mapping is well-defined in the sense that the expression $\begin{pmatrix} i & j \\ 0 & 1 \end{pmatrix}$ is such that the index i is required to be nonzero. Now, let i_1 and i_2 be indices in $\{1, 2, \dots, p-1\}$, and let j_1 and j_2 be indices in $\{0, 1, 2, \dots, p-1\}$. Now, consider the composition $\sigma_{i_1,j_1} \circ \sigma_{i_2,j_2}$. Since σ_{i_2,j_2} maps ζ_p to $\zeta_p^{i_2}$, we have that $\sigma_{i_1,j_1} \circ \sigma_{i_2,j_2}$ maps ζ_p to $\zeta_p^{i_1 i_2 (\text{mod } p)}$. Since σ_{i_2,j_2} maps $\sqrt[p]{2}$ to $\zeta_p^{j_2} \sqrt[p]{2}$, and since σ_{i_1,j_1} is a morphism, we have that the composition $\sigma_{i_1,j_1} \circ \sigma_{i_2,j_2}$ maps $\sqrt[p]{2}$ to $\zeta_p^{(i_1 j_2 + j_1)(\text{mod } p)} \sqrt[p]{2}$. So, the mapping Ψ evaluated at the composition $\sigma_{i_1,j_1} \circ \sigma_{i_2,j_2}$ is equal to

$$\begin{pmatrix} i_1 i_2 (\text{mod } p) & (i_1 j_2 + j_1)(\text{mod } p) \\ 0 & 1 \end{pmatrix}.$$

Now, consider the matrix product $\Psi(\sigma_{i_1,j_1})\Psi(\sigma_{i_2,j_2})$, which is equal to:

$$\begin{pmatrix} i_1 & j_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} i_2 & j_2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} i_1 i_2 (\text{mod } p) & (i_1 j_2 + j_1)(\text{mod } p) \\ 0 & 1 \end{pmatrix}.$$

We thus have that Ψ is a well-defined group homomorphism from the Galois group of $x^p - 2$ to

$$\left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a, b \in \mathbb{F}_p, a \neq 0 \right\}.$$

It is obvious that Ψ is injective, since if

$$\Psi(\sigma_{i_1,j_1}) = \Psi(\sigma_{i_2,j_2})$$

then

$$\begin{pmatrix} i_1 & j_1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} i_2 & j_2 \\ 0 & 1 \end{pmatrix},$$

so tat $i_1 = i_2$ and $j_1 = j_2$. Since Ψ is an injective mapping between two sets of equal cardinality, we have that Ψ is bijective. Since Ψ is also a morpism, we thus have that Ψ is a group isomorphism, as desired.

Exercise 3.172. Let $K = \mathbb{Q}(\sqrt[8]{2}, i)$, and let $F_1 = \mathbb{Q}(i)$, $F_2 = \mathbb{Q}(\sqrt{2})$, $F_3 = \mathbb{Q}(\sqrt{-2})$. Prove that $\text{Gal}(K/F_1) \cong Z_8$, $\text{Gal}(K/F_2) = D_8$, $\text{Gal}(K/F_3) = Q_8$.

Solution 3.173. Our solution is inspired in part by a corresponding solution given in the following link.

`http://sporadic.stanford.edu/Math121/Solutions5.pdf`

Let σ be an element in $\text{Aut}(K/F_1)$. We have that the behaviour of σ is completely determined by the value of $\sigma(\sqrt[8]{2})$. Since the minimal polynomial for $\sqrt[8]{2}$ over $\mathbb{Q}(i)$ is equal to $x^8 - 2 \in \mathbb{Q}(i)[x]$, letting ζ_8 denote a primitive 8th root of unity, we have that:

$$\sigma(\sqrt[8]{2}) \in \left\{ \sqrt[8]{2}, \zeta_8 \sqrt[8]{2}, \zeta_8^2 \sqrt[8]{2}, \dots, \zeta_8^7 \sqrt[8]{2} \right\}.$$

Since there are 8 possible choices for the value of $\sigma(\sqrt[8]{2})$, we may conclude that:

$$|\mathrm{Aut}(K/F_1)| = 8.$$

Now, since

$$K = \mathbb{Q}(\sqrt[8]{2}, i) \cong \mathbb{Q}(i)(\sqrt[8]{2}),$$

we may, accordingly, identify the fields K and $\mathbb{Q}(i)(\sqrt[8]{2})$.

$$\begin{tikzcd}
\mathbb{Q}(i)(\sqrt[8]{2}) \arrow[d, dash] \\
\mathbb{Q}(i)
\end{tikzcd}$$

Since the minimal polynomial for $\sqrt[8]{2}$ over $\mathbb{Q}(i)$ is $x^8 - 2$, we thus have that:

$$[\mathbb{Q}(i)(\sqrt[8]{2}) : \mathbb{Q}(i)] = \deg m_{\sqrt[8]{2}, \mathbb{Q}(i)}(x) = 8.$$

So, since

$$[K \ : \ F_1] = |\mathrm{Aut}(K/F_1)|,$$

we find that K is a Galois extension of F_1. We also note that we have shown that the Galois group $\mathrm{Gal}(K/F_1)$ must be of order 8.

Since

$$(i+1)^2 = 2i$$

we have that

$$\sqrt{i} = \frac{i+1}{\sqrt{2}}.$$

Since

$$\left(\sqrt{i}\right)^2 = i$$

and

$$\left(\sqrt{i}\right)^4 = -1$$

and

$$\left(\sqrt{i}\right)^8 = 1,$$

it is easily seen that $\frac{i+1}{\sqrt{2}}$ is a primitive 8th root of unity. Let

$$\zeta_8 = \frac{i+1}{\sqrt{2}} = \sqrt{2}\left(\frac{i+1}{2}\right),$$

with

$$\sigma(\sqrt[8]{2}) \in \left\{\sqrt[8]{2}, \zeta_8\sqrt[8]{2}, \zeta_8^2\sqrt[8]{2}, \ldots, \zeta_8^7\sqrt[8]{2}\right\},$$

as above.

Now, let ρ denote the unique element in $\mathrm{Gal}(\mathbb{Q}(i)(\sqrt[8]{2})/\mathbb{Q}(i))$ such that:

$$\rho(\sqrt[8]{2}) = \sqrt{2}\left(\frac{i+1}{2}\right)\left(\sqrt[8]{2}\right).$$

Now, consider the following computations:

$$\begin{aligned}
\rho(\sqrt[8]{2}) &= \sqrt{2}\left(\frac{i+1}{2}\right)\left(\sqrt[8]{2}\right)\\
\rho(\rho(\sqrt[8]{2})) &= \rho(\sqrt{2})\left(\frac{i+1}{2}\right)\rho\left(\sqrt[8]{2}\right)\\
&= \left(\frac{i+1}{2}\right)\left(\rho\left(\sqrt[8]{2}\right)\right)^5\\
&= -i\sqrt[8]{2}\\
\rho(\rho(\rho(\sqrt[8]{2}))) &= \rho(-i\sqrt[8]{2})\\
&= \rho(-i)\rho(\sqrt[8]{2})\\
&= -i\rho(\sqrt[8]{2})\\
&= \sqrt{2}\left(\frac{1-i}{2}\right)\left(\sqrt[8]{2}\right)\\
\rho(\rho(\rho(\rho(\sqrt[8]{2})))) &= \rho(\sqrt{2})\left(\frac{1-i}{2}\right)\rho\left(\sqrt[8]{2}\right)\\
&= \left(\frac{1-i}{2}\right)\left(\rho\left(\sqrt[8]{2}\right)\right)^5\\
&= \left(\frac{1-i}{2}\right)\left(\sqrt{2}\left(\frac{i+1}{2}\right)\left(\sqrt[8]{2}\right)\right)^5\\
&= -\sqrt[8]{2}.
\end{aligned}$$

So, we have shown that the element ρ given above is such that the order of ρ as an element in the Galois group $\mathrm{Gal}(\mathbb{Q}(i)(\sqrt[8]{2})/\mathbb{Q}(i))$ is strictly greater than 4. So, by Lagrange's theorem, since

$$\left|\mathrm{Gal}(\mathbb{Q}(i)(\sqrt[8]{2})/\mathbb{Q}(i))\right| = 8,$$

we may deduce that the order of ρ in the Galois group $\mathrm{Gal}(\mathbb{Q}(i)(\sqrt[8]{2})/\mathbb{Q}(i))$ is equal to 8, so that $\mathrm{Gal}(\mathbb{Q}(i)(\sqrt[8]{2})/\mathbb{Q}(i))$ must be a cyclic group of order 8.

Essentially, the same kind of approach may be used to evaluate the latter two Galois group given in the above exercise. We omit the computational details involved for these latter evaluations.

3.17 Exercises From Section 14.3

Exercise 3.174. Factor $x^8 - x$ into irreducibles in $\mathbb{Z}[x]$ and in $\mathbb{F}_2[x]$.

Solution 3.175. We begin by factoring $x^8 - x$ into irreducibles in $\mathbb{Z}[x]$. The expression $x^8 - x$ may be written as $x(x^7 - 1)$. This can further be factored as

$$x(x-1)\left(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1\right).$$

From Section 13.6 of the class textbook, we have that the 7th cyclotomic polynomial $\Phi_7(x)$ is equal to

$$\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1,$$

and by Theorem 41 from Section 13.6 of the class textbook, we know that, in general, the cyclotomic polynomial $\Phi_n(x)$ is an irreducible monic polynomial in $\mathbb{Z}[x]$. So, we have that our factorization of $x^8 - x$ as

$$x(x-1)\left(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1\right).$$

is a factorization into irreducibles.

We proceed to regard $x^8 - x$ as an element in $\mathbb{F}_2[x]$, and we again consider the factorization $x^8 - x = x(x^7 - 1)$. We observe that this factorization may be rewritten in the following manner:

$$x^8 - x = x(x^7 - 1) = x(x^7 + 1).$$

Now, observe that:

$$(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)(x + 1) = x^7 + 1,$$

since coefficients are being reduced modulo 2. We thus have that:

$$x^8 - x = x(x + 1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1).$$

By way of contradiction, suppose that $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ can be factored into a product of a degree-1 polynomial and a degree-5 polynomial. Such a factorization would have to be of the following form:

$$(x + 1)(x^5 + ax^4 + bx^3 + cx^2 + dx + 1).$$

The coefficient of x^5 in the expansion of the above product is equal to $(1 + a)$. Therefore, $a = 0$:

$$(x + 1)(x^5 + bx^3 + cx^2 + dx + 1).$$

The coefficient of x^4 is equal to $b = 1$:

$$(x + 1)(x^5 + x^3 + cx^2 + dx + 1).$$

The coefficient of x^3 is equal to $1 + c$, so $c = 0$:

$$(x + 1)(x^5 + x^3 + dx + 1).$$

The coefficient of x^2 is equal to d, so $d = 1$:

$$(x + 1)(x^5 + x^3 + x + 1).$$

But if we expand the above product, we have

$$x^6 + x^5 + x^4 + x^3 + x^2 + 1,$$

and we thus have a contradiction. Now, suppose that $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ can be written as a product of a degree-2 polynomial and a degree-4 polynomial, as below:

$$(x^2 + ax + 1)(x^4 + bx^3 + cx^2 + dx + 1).$$

The coefficient of x^5 in the expansion of the above product is equal to $b + a = 1$. The coefficient of x^4 in the expansion of the above product is equal to $c + ab + 1 = 1$. So, $c + ab = 0$. Since $b + a = 1$, with $a, b \in \mathbb{F}_2$, we have that either $a = 1$ and $b = 0$, or vice-versa. So, we have that $c = 0$:

$$(x^2 + ax + 1)(x^4 + bx^3 + dx + 1).$$

The coefficient of x^3 in the expansion of the above product is $d + b = 1$. The coefficient of x^2 in the expansion of the above product is $1 + ad = 1$, so that $ad = 0$. Since $a + b = 1$, and since $d + b = 1$, we have that $d = a$. Since $ad = 0$ and since $d = a$, we can conclude that $a = d = 0$:

$$(x^2 + 1)(x^4 + bx^3 + 1).$$

Since $a + b = 1$, we have that $b = 1$:

$$(x^2 + 1)(x^4 + x^3 + 1).$$

Expanding the above product, we find that

$$(x^2 + 1)(x^4 + x^3 + 1) = x^6 + x^5 + x^4 + x^3 + x^2 + 1.$$

Finally, suppose that $x^6+x^5+x^4+x^3+x^2+x+1$ can be written as the product of two degree-3 polynomials, as below:

$$(x^3 + ax^2 + bx + 1)(x^3 + cx^2 + dx + 1).$$

The coefficient of x^5 in the expansion of the above product is equal to $c + a = 1$. The coefficient of x^4 in the expansion of the above product is equal to $d + ac + b = 1$. The coefficient of x^3 in the expansion of the above product is equal to $1 + ad + bc + 1 = 1$. The coefficient of x^2 in the expansion of the above product is equal to $a + bd + c = 1$. The coefficient of x in te expansion of the above product is $b + d = 1$. So, we arrive at the following system of equations:

$$\begin{aligned}
&b + d = 1\\
&a + bd + c = 1\\
&1 + ad + bc = 0\\
&d + ac + b = 1\\
&c + a = 1.
\end{aligned}$$

If $a = 1$, then we have that

$$\begin{aligned}
&b = 0\\
&bd = 0\\
&d = 1\\
&d + b = 1\\
&c = 0.
\end{aligned}$$

Then

$$(x^3 + x^2 + 1)(x^3 + x + 1)$$

would be equal to

$$x^6 + x^5 + x^4 + 3x^3 + x^2 + x + 1 = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1,$$

as desired. So, we have thus far shown that the expression $x^8 - x$ may be factored as follows:

$$x^8 - x = x(x + 1)(x^3 + x^2 + 1)(x^3 + x + 1).$$

If the polynomial $(x^3 + x^2 + 1)$ were reducible as an element in $\mathbb{F}_2[x]$, then we would have that:

$$(x^3 + x^2 + 1) = (x^2 + ax + 1)(x + 1).$$

Then the coefficient of x^2 would be equal to $1+a=1$, so that $a=0$. But then

$$(x^2+1)(x+1)=x^3+x^2+x+1,$$

and we arrive at a contradiction. If the polynomial (x^3+x+1) were reducible as an element in $\mathbb{F}_2[x]$, then we would have that:

$$x^3+x+1=(x^2+ax+1)(x+1).$$

The coefficient of x^2 would be $1+a=0$, so that $a=1\in\mathbb{F}_2$. But then

$$(x^2+x+1)(x+1)=x^3+1,$$

and we again arrive at a contradiction. So, we have shown that the factorization of x^8-x into irreducibles, as an element in $\mathbb{F}_2[x]$ is such that:

$$x^8-x=x(x+1)(x^3+x^2+1)(x^3+x+1).$$

If we expand

$$x^8-x=x(x+1)(x^3+x^2+1)(x^3+x+1)$$

as an element in $\mathbb{Z}[x]$, we obtain

$$x^8+2x^7+2x^6+4x^5+4x^4+2x^3+2x^2+x,$$

and this reduces to x^8-x modulo 2.

Exercise 3.176. Write out the multiplication table for $\mathbb{F}_4$ and $\mathbb{F}_8$.

Solution 3.177. In order to perform explicit computations with respect to the elements in the finite field $\mathbb{F}_4$, it is natural to let the field $\mathbb{F}_4$ be denoted as a quotient ring. As stated in the class textbook, "The importance of having irreducible polynomials at hand is that they give a representation of the finite fields $\mathbb{F}_{p^n}$ (as quotients $\mathbb{F}_p[x]/(f(x))$ for $f(x)$ irreducible of degree n) conducive to explicit computations." (p. 587) So, we begin by determining a degree-2 irreducible polynomial in $\mathbb{F}_2[x]$. Consider the polynomial x^2+x+1 as an element in $\mathbb{F}_2[x]$. By way of contradiction, suppose that this poylnomial is not irreducible in $\mathbb{F}_2[x]$. So, have that x^2+x+1 could be written as a product of two degree-1 polynomials p_1 and p_2 in $\mathbb{F}_2[x]$. Since the leading coefficient of x^2+x+1 is equal to 1, we have that the leading coefficients of both p_1 and p_2 must be equal to 1. But since the constant term of x^2+x+1 is also equal to 1, we may, accordingly, deduce that the leading term of both p_1 and p_2 is equal to 1. But since p_1 and p_2 are both degree-1 polynomials, we may deduce that

$$p_1=p_2=x+1,$$

so that

$$p_1p_2=(x+1)^2=x^2+2x+1=x^2+1,$$

which is impossible, since x^2+1 is not equal to x^2+x+1. So, we have thus far shown that:

$$\mathbb{F}_4=\mathbb{F}_2[x]/(x^2+x+1).$$

Let I denote the principal ideal $(x^2+x+1)\subseteq\mathbb{F}_2[x]$. Let the additive identity element $0+I$ be denoted as $\mathbf{0}$. Let the multiplicative identity element $1+I$ be denoted as $\mathbf{1}$. Now, consider the element

$$x+I=x+\langle x^2+x+1\rangle,$$

letting ideals be denoted using the brackets $\langle$ and $\rangle$, for the sake of clarity. Now, consider the square of this element:

$$\left(x + \langle x^2 + x + 1\rangle\right)^2 = x^2 + \langle x^2 + x + 1\rangle.$$

Since

$$x^2 + x + 1 + \langle x^2 + x + 1\rangle = 0 + \langle x^2 + x + 1\rangle,$$

we have that

$$x + 1 + \langle x^2 + x + 1\rangle = x^2 + \langle x^2 + x + 1\rangle.$$

Letting $x + I$ be denoted as $\overline{x}$, and letting

$$x + 1 + \langle x^2 + x + 1\rangle = x^2 + \langle x^2 + x + 1\rangle$$

be denoted as $\overline{x+1} = \overline{x^2}$, letting a coset of the form $\alpha + I$ be denoted as $\overline{\alpha}$, for an element α in $\mathbb{F}_2[x]$, we have that the elements in $\mathbb{F}_2[x]/\langle x^2 + x + 1\rangle$ are precisely the elements in $\{\mathbf{0}, \mathbf{1}, \overline{x}, \overline{x+1}\}$. So, using the structure endowed upon $\mathbb{F}_2[x]/\langle x^2+x+1\rangle$, we may compute the multiplication table for $\mathbb{F}_4$, as suggested as follows.

$*$	$\mathbf{0}$	$\mathbf{1}$	$\overline{x}$	$\overline{x+1}$
$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$
$\mathbf{1}$	$\mathbf{0}$	$\mathbf{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{x}$	$\mathbf{0}$	$\overline{x}$	$\overline{x+1}$	$\mathbf{1}$
$\overline{x+1}$	$\mathbf{0}$	$\overline{x+1}$	$\mathbf{1}$	$\overline{x}$

As discussed in the class textbook, the polynomial $x^3 + x + 1$ is irreducible as an element in $\mathbb{F}_2[x]$. We thus have that the field $\mathbb{F}_8$ is isomorphic to the quotient ring $\mathbb{F}_2[x]/\langle x^3 + x + 1\rangle$, so we may identify the field $\mathbb{F}_8$ with the quotient ring $\mathbb{F}_2[x]/\langle x^3 + x + 1\rangle$. Now, compute the elements in this ring:

$$\begin{aligned}
&0 + \langle x^3 + x + 1\rangle = x^3 + x + 1 + \langle x^3 + x + 1\rangle\\
&1 + \langle x^3 + x + 1\rangle = x^3 + x + \langle x^3 + x + 1\rangle\\
&x + \langle x^3 + x + 1\rangle = x^3 + 1 + \langle x^3 + x + 1\rangle\\
&x + 1 + \langle x^3 + x + 1\rangle = x^3 + \langle x^3 + x + 1\rangle\\
&x^2 + \langle x^3 + x + 1\rangle = x^3 + x^2 + x + 1 + \langle x^3 + x + 1\rangle\\
&x^2 + 1 + \langle x^3 + x + 1\rangle = x^3 + x^2 + x + \langle x^3 + x + 1\rangle\\
&x^2 + x + \langle x^3 + x + 1\rangle = x^3 + x^2 + 1 + \langle x^3 + x + 1\rangle\\
&x^2 + x + 1 + \langle x^3 + x + 1\rangle = x^3 + x^2 + \langle x^3 + x + 1\rangle
\end{aligned}$$

Using the above cosets, we may construct a multiplication table for $\mathbb{F}_8$, as indicated below. Given a coset of the form $c + \langle x^3 + x + 1\rangle$, we denote this coset as $\overline{c}$, letting c be a polynomial in $\mathbb{F}_2[x]$.

$*$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$	$\overline{x^2}$	$\overline{x^2+1}$	$\overline{x^2+x}$	$\overline{x^2+x+1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$	$\overline{x^2}$	$\overline{x^2+1}$	$\overline{x^2+x}$	$\overline{x^2+x+1}$
$\overline{x}$	$\overline{0}$	$\overline{x}$	$\overline{x^2}$	$\overline{x^2+x}$	$\overline{x+1}$	$\overline{1}$	$\overline{x^2+x+1}$	$\overline{x^2+1}$
$\overline{x+1}$	$\overline{0}$	$\overline{x+1}$	$\overline{x^2+x}$	$\overline{x^2+1}$	$\overline{x^2+x+1}$	$\overline{x^2}$	$\overline{1}$	$\overline{x}$
$\overline{x^2}$	$\overline{0}$	$\overline{x^2}$	$\overline{x+1}$	$\overline{x^2+x+1}$	$\overline{x^2+x}$	$\overline{x}$	$\overline{x^2+1}$	$\overline{1}$
$\overline{x^2+1}$	$\overline{0}$	$\overline{x^2+1}$	$\overline{1}$	$\overline{x^2}$	$\overline{x}$	$\overline{x^2+x+1}$	$\overline{x+1}$	$\overline{x^2+x}$
$\overline{x^2+x}$	$\overline{0}$	$\overline{x^2+x}$	$\overline{x^2+x+1}$	$\overline{1}$	$\overline{x^2+1}$	$\overline{x+1}$	$\overline{x}$	$\overline{x^2}$
$\overline{x^2+x+1}$	$\overline{0}$	$\overline{x^2+x+1}$	$\overline{x^2+1}$	$\overline{x}$	$\overline{1}$	$\overline{x^2+x}$	$\overline{x^2}$	$\overline{x+1}$

Exercise 3.178. Prove that an algebraically closed field must be infinite.

Solution 3.179. By way of contradiction, suppose that there exists an algebraically closed field which is finite. But finite fields must be of the form $\mathbb{F}_{p^n}$. So, suppose that $\mathbb{F}_{p^n}$ is algebraically closed, for some natural number $n \in \mathbb{N}$. We know that $\mathbb{F}_{p^{n+1}}$ properly contains $\mathbb{F}_{p^n}$, and we have that $\mathbb{F}_{p^{n+1}}$ is the splitting field for $x^{p^{n+1}} - x$ over $\mathbb{F}_p$. In other words, $\mathbb{F}_{p^{n+1}}$ contains some roots of $x^{p^{n+1}} - x$ which are not contained in $\mathbb{F}_{p^n}$, thus contradicting that $\mathbb{F}_{p^n}$ is algebraically closed.

Exercise 3.180. Construct the finite field of 16 elements and find a generator for the multiplicative group. How many generators are there?

Solution 3.181. As discussed in the class textbook, we have that

$$\mathbb{F}_{16} \cong \mathbb{F}_2[x]/\langle x^4 + x^3 + 1\rangle,$$

so we may regard the finite field $\mathbb{F}_{16}$ as being the same as the quotient ring $\mathbb{F}_2[x]/\langle x^4 + x^3 + 1\rangle$. So, we have that the following set of distinct elements is equal to the underlying set of $\mathbb{F}_2[x]/\langle x^4 + x^3 + 1\rangle$:

$$\{0+\langle x^4+x^3+1\rangle, 1+\langle x^4+x^3+1\rangle, x+\langle x^4+x^3+1\rangle, x+1+\langle x^4+x^3+1\rangle, x^2+\langle x^4+x^3+1\rangle, \ldots, x^3+x^2+x+1+\langle x^4+x^3+1\rangle\}.$$

Given a polynomial c in $\mathbb{F}_2[x]$, let the coset $c + \langle x^4 + x^3 + 1\rangle$ be denoted as $\overline{c}$. We claim that $\overline{x}$ is a generator for the underlying multiplicative group on

$$\mathbb{F}_{16} \cong \mathbb{F}_2[x]/\langle x^4 + x^3 + 1\rangle.$$

To show this, we proceed to consider the following computations.

$$\begin{aligned}
&(\overline{x})^1 = \overline{x}\\
&\overline{x} \cdot \overline{x} = \overline{x^2}\\
&\overline{x} \cdot \overline{x^2} = \overline{x^3}\\
&\overline{x} \cdot \overline{x^3} = \overline{x^3 + 1}\\
&\overline{x} \cdot (\overline{x^3 + 1}) = \overline{x^3 + x + 1}\\
&\overline{x} \cdot (\overline{x^3 + x + 1}) = \overline{x^3 + x^2 + x + 1}\\
&\overline{x} \cdot (\overline{x^3 + x^2 + x + 1}) = \overline{x^2 + x + 1}\\
&\overline{x} \cdot (\overline{x^2 + x + 1}) = \overline{x^3 + x^2 + x}\\
&\overline{x} \cdot (\overline{x^3 + x^2 + x}) = \overline{x^2 + 1}\\
&\overline{x} \cdot (\overline{x^2 + 1}) = \overline{x^3 + x}\\
&\overline{x} \cdot (\overline{x^3 + x}) = \overline{x^3 + x^2 + 1}\\
&\overline{x} \cdot (\overline{x^3 + x^2 + 1}) = \overline{x + 1}\\
&\overline{x} \cdot (\overline{x + 1}) = \overline{x^2 + x}\\
&\overline{x} \cdot (\overline{x^2 + x}) = \overline{x^3 + x^2}\\
&\overline{x} \cdot (\overline{x^3 + x^2}) = \overline{1}
\end{aligned}$$

We have shown that the order of $\overline{x}$ as an element in the underlying multiplicative group of $\mathbb{F}_{16}$ is equal to 15. So, the collection

$$\{1, \overline{x}, (\overline{x})^2, \ldots, (\overline{x})^{14}\}$$

forms a multiplicative cyclic group, and the generators of this group consist of expressions of the form $(\overline{x})^i$ where $i \in \mathbb{N}$ is such that $i \leq 14$ and such that i and 15 are relatively prime. So, the generators for this cyclic group are: $\overline{x}$, $(\overline{x})^2$, $(\overline{x})^4$, $(\overline{x})^7$, $(\overline{x})^8$, $(\overline{x})^{11}$, $(\overline{x})^{13}$, $(\overline{x})^{14}$. So, there are a total of 8 generators for the multiplicative group.

3.18 Exercises from Section 14.4

Exercise 3.182. Determine the Galois closure of the field $\mathbb{Q}(\sqrt{1+\sqrt{2}})$ over $\mathbb{Q}$.

Solution 3.183. The following is from the class textbook.

"Let E/F be any finite separable extension. Then E is contained in an extension K which is Galois over F and is minimal in the sense that in a fixed algebraic closure of K any other Galois extension of F containing E contains K." (p. 594)

As discussed in the class textbook, the Galois extension K of F containing E, as above, is referred to as the *Galois closure* of E over F.

Now, consider the given field extension $\mathbb{Q}(\sqrt{1+\sqrt{2}})$ of $\mathbb{Q}$. Letting α be equal to $\sqrt{1+\sqrt{2}}$, we have that

$$\alpha^2 = 1 + \sqrt{2}$$

so that

$$(\alpha^2 - 1)^2 = 2,$$

with

$$(\alpha^2 - 1)^2 - 2 = 0,$$

so that α is a root of $x^4 - 2x^2 - 1$. By the quadratic formula, the roots of this polynomial are:

$$\pm\sqrt{\frac{2 \pm \sqrt{8}}{2}} = \pm\sqrt{\frac{2 \pm 2\sqrt{2}}{2}} = \pm\sqrt{1 \pm \sqrt{2}}.$$

Since $x^4 - 2x^2 - 1$ is irreducible over $\mathbb{Q}$, as may be verified, we have that the minimal polynomial for α over $\mathbb{Q}$ is $x^4 - 2x^2 - 1$. Since $x^4 - 2x^2 - 1$ is also separable, we can conclude that the Galois closure of the field $\mathbb{Q}(\sqrt{1+\sqrt{2}})$ over $\mathbb{Q}$ is equal to the splitting field of $x^4 - 2x^2 - 1$ over $\mathbb{Q}$, which is equal to:

$$\mathbb{Q}(\sqrt{1+\sqrt{2}}, \sqrt{1-\sqrt{2}}).$$

Exercise 3.184. Find a primitive generator for $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ over $\mathbb{Q}$.

Solution 3.185. We begin by observing that $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ is the splitting field of the polynomial

$$(x^2 - 2)(x^2 - 3)(x^2 - 5)$$

over $\mathbb{Q}$. Since the polynomial $(x^2 - 2)(x^2 - 3)(x^2 - 5)$ is separable, we have that $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ is a splitting field of a separable polynomial over $\mathbb{Q}$, and we thus find that $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ is Galois over $\mathbb{Q}$. Now, consider the following discussion from the class textbook:

"... a primitive element for an extension can be obtained as a simple linear combination of the generators for the extension. In the case of Galois extensions it is only necessary to determine a linear combination which is not fixed by any nontrivial element of the Galois group..." (p. 595)

The element $\sqrt{2} + \sqrt{3} + \sqrt{5}$ is a linear combination of the generators in $\{\sqrt{2}, \sqrt{3}, \sqrt{5}\}$ which is not fixed by any nontrivial element of the Galois group, so we have that $\sqrt{2} + \sqrt{3} + \sqrt{5}$ is a primitive generator for $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ over the field of rational numbers.

3.19 Exercises from Section 14.5

Exercise 3.186. Determine the minimal polynomials satisfied by the primitive generators given in the text for the subfields of $\mathbb{Q}(\zeta_{13})$.

Solution 3.187. The following discussion is taken from the class textbook.

"...consider the subfields of $\mathbb{Q}(\zeta_{13})$, which correspond to the subgroups of $(\mathbb{Z}/13\mathbb{Z})^\times \cong \mathbb{Z}/12\mathbb{Z}$. A generator for this cyclic group is the automorphism $\sigma = \sigma_2$ which maps ζ_{13} to ζ_{13}^2. The nontrivial subgroups correspond to the nontrivial divisors of 12, hence are of orders 2, 3, 4, and 6 with generators σ^6, σ^4, σ^3 and σ^2, respectively. The corresponding fixed fields will be of degrees 6, 4, 3 and 2 over $\mathbb{Q}$, respectively. Generators are given by ($\zeta = \zeta_{13}$)

$$\zeta + \sigma^6\zeta = \zeta + \zeta^{2^6} = \zeta + \zeta^{-1}$$
$$\zeta + \sigma^4\zeta + \sigma^8\zeta = \zeta + \zeta^{2^4} + \zeta^{2^8} = \zeta + \zeta^3 + \zeta^9$$
$$\zeta + \sigma^3\zeta + \sigma^6\zeta + \sigma^9\zeta = \zeta + \zeta^8 + \zeta^{12} + \zeta^5$$
$$\zeta + \sigma^2\zeta + \sigma^4\zeta + \sigma^6\zeta + \sigma^8\zeta + \sigma^{10}\zeta = \zeta + \zeta^4 + \zeta^3 + \zeta^{12} + \zeta^9 + \zeta^{10}.\text{" (p. 598)}$$

Recall that $\zeta = \zeta_{13}$ denotes a primitive 13th root of unity. Write α in place of $\zeta + \zeta^{-1} = \zeta + \zeta^{12}$. We know that the degree of the minimal polynomial of α over $\mathbb{Q}$ is 6. So, let the rational coefficients a, b, c, d, e and f be such that:

$$\alpha^6 + a\alpha^5 + b\alpha^4 + c\alpha^3 + d\alpha^2 + e\alpha + f = 0.$$

Our strategy is to make use of the following equality:

$$\zeta^{12} + \zeta^{11} + \zeta^{10} + \zeta^9 + \zeta^8 + \zeta^7 + \zeta^6 + \zeta^5 + \zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = 0.$$

Expanding the equation

$$\alpha^6 + a\alpha^5 + b\alpha^4 + c\alpha^3 + d\alpha^2 + e\alpha + f = 0,$$

we have that

$$10a\zeta^{12} + 5a\zeta^{10} + a\zeta^8 + a\zeta^5 + 5a\zeta^3 + 10a\zeta + 4b\zeta^{11} + b\zeta^9 + b\zeta^4 + 4b\zeta^2 + 6b + 3c\zeta^{12} + c\zeta^{10} + c\zeta^3 + 3c\zeta + d\zeta^{11} + d\zeta^2 + 2d + e\zeta^{12} + e\zeta + 15\zeta^{11} + 6\zeta^9 + \zeta^7 + \zeta^6 + 6\zeta^4 + 15\zeta^2 + f + 20 = 0.$$

So, using the equation

$$\zeta^{12} + \zeta^{11} + \zeta^{10} + \zeta^9 + \zeta^8 + \zeta^7 + \zeta^6 + \zeta^5 + \zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = 0,$$

we obtain the following system of equations:

$$\begin{aligned} &10a + 3c + e = 1 \\ &15 + 4b + d = 1 \\ &5a + c = 1 \\ &6 + b = 1 \\ &a = 1 \\ &20 + 6b + 2d + f = 1 \end{aligned}$$

Solving for the above coefficients, we have that $a = 1$, $b = -5$, $c = -4$, $d = 6$, $e = 3$, and $f = -1$. So, the minimal polynomial for $\zeta + \zeta^{-1}$ is equal to:

$$x^6 + x^5 - 5x^4 - 4x^3 + 6x^2 + 3x - 1.$$

A similar argument can be used to show that the minimal polynomial for $\zeta+\zeta^3+\zeta^9$ is $x^4+x^3+2x^2-4x+3$; we omit details regarding the process of computing this polynomial, and the following polynomials. The minimal polynomial for $\zeta+\zeta^8+\zeta^{12}+\zeta^5$ is x^3+x^2-4x+1, and the minimal polynomial for $\zeta+\zeta^4+\zeta^3+\zeta^{12}+\zeta^9+\zeta^{10}$ is x^2+x-3.

3.20 Exercises from Section 14.6

Exercise 3.188. Show that a cubic with a multiple root has a linear factor. Is the same true for quartics?

Solution 3.189. As discussed in the class textbook, if a cubic polynomial is reducible, then it either splits into three linear factors or into a linear factor and an irreducible quadratic. So, if a cubic has a multiple root, it must have a linear factor. However, this is not, in general, true for quartics, since, for example, the degree-4 polynomial

$$(x^2-2)^2=(x^2-2)(x^2-2)$$

has multiple roots, but does not split so as to have a linear factor.

Exercise 3.190. Determine the Galois group of the following polynomial: x^3-x^2-4.

Solution 3.191. The Galois group of a separable polynomial $p(x)\in\mathbb{F}[x]$ may be defined as the Galois group of the splitting field of $p(x)$ over the field $\mathbb{F}$. We begin by observing that 2 is a root of the given polynomial, x^3-x^2-4. By considering the graph of x^3-x^2-4, we observe that x^3-x^2-4 has a unique real root, namely 2. By writing

$$x^3-x^2-4=(x-2)(x^2+ax+2)$$

for a rational coefficient $a\in\mathbb{Q}$, we have that

$$x^3-x^2-4=x^3+(a-2)x^2+(2-2a)x-4$$

we have that $a-2=-1$ and $2-2a=0$, so that $a=1$, thus yielding the following factorization:

$$x^3-x^2-4=(x-2)(x^2+x+2).$$

So, from the above factorization, we have that the roots of the given polynomial are precisely the following:

$$\alpha_1=2,\alpha_2=\frac{-1-\sqrt{-7}}{2},\alpha_3=\frac{-1+\sqrt{-7}}{2}.$$

So, since the given polynomial $p(x)=x^3-x^2-4$ has no multiple roots, we see that $p(x)=x^3-x^2-4$ is separable. Now, consider the splitting field of $p(x)=x^3-x^2-4$ over the field $\mathbb{Q}$. Since $\mathbb{Q}$ already contains $\alpha_1=2$, and since $\mathbb{Q}$ already contains $-\frac{1}{2}$, we see that the splitting field of $p(x)=x^3-x^2-4$ over $\mathbb{Q}$ is equal to $\mathbb{Q}(\sqrt{-7})$. Since $\mathbb{Q}(\sqrt{-7})$ is the splitting field of a separable polynomial, we have that $\mathbb{Q}(\sqrt{-7})$ is a Galois extension of $\mathbb{Q}$. So, it remains to compute the following group:

$$\operatorname{Aut}\left(\mathbb{Q}(\sqrt{-7})/\mathbb{Q}\right)=\operatorname{Gal}\left(\mathbb{Q}(\sqrt{-7})/\mathbb{Q}\right).$$

Let σ be an element in $\operatorname{Aut}\left(\mathbb{Q}(\sqrt{-7})/\mathbb{Q}\right)$. Since σ fixes the base field $\mathbb{Q}$, we have that the behaviour of the automorphism σ is uniquely determined by the value of $\sigma(\sqrt{-7})$. Since

$$\left(\sqrt{-7}\right)^2+7=0,$$

and since σ is a morphism, we have that

$$\left(\sigma(\sqrt{-7})\right)^2 + 7 = 0,$$

so we have that σ must map $\sqrt{-7}$ to a root of $x^2 + 7$. So, we find that the only elements in

$$\mathrm{Gal}\left(\mathbb{Q}(\sqrt{-7})/\mathbb{Q}\right)$$

are the identity automorphism σ_1 on $\mathbb{Q}(\sqrt{-7})$ and the morphism σ_2 fixing $\mathbb{Q}$ such that $\mathbb{Q}(\sqrt{-7}) = -\sqrt{-7}$. Since $\sigma_2^2 = \sigma_1$, we find that

$$\mathrm{Gal}\left(\mathbb{Q}(\sqrt{-7})/\mathbb{Q}\right) \cong \mathbb{Z}/2\mathbb{Z}.$$

Exercise 3.192. Determine the Galois group of the following polynomial: $x^3 - 2x + 4$.

Solution 3.193. We begin by observing that -2 is a root of the polynomial $x^3 - 2x + 4$. Writing

$$x^3 - 2x + 4 = (x + 2)(x^2 + ax + 2)$$

for a rational coefficient a, we have that

$$x^3 - 2x + 4 = x^3 + ax^2 + 2x + 2x^2 + 2ax + 4$$

so that

$$x^3 - 2x + 4 = x^3 + (a + 2)x^2 + (2a + 2)x + 4.$$

We thus find that $a = -2$, with:

$$x^3 - 2x + 4 = (x + 2)(x^2 - 2x + 2).$$

So, we find that the roots of $x^3 - 2x + 4$ are:

$$\alpha_1 = -2, \alpha_2 = \frac{2 - \sqrt{-4}}{2}, \alpha_3 = \frac{2 + \sqrt{-4}}{2}.$$

That is, the roots of $x^3 - 2x + 4$ are precisely:

$$\alpha_1 = -2, \alpha_2 = \frac{2 - 2i}{2}, \alpha_3 = \frac{2 + 2i}{2}.$$

For the sake of clarity, rewrite the above roots as follows:

$$\alpha_1 = -2, \alpha_2 = 1 - i, \alpha_3 = 1 + i.$$

So, we find that the splitting field of $x^3 - 2x + 4$ over $\mathbb{Q}$ is equal to $\mathbb{Q}(i)$. By repeating an argument given in the previous solution, we have that the Galois group for $x^3 - 2x + 4$ over $\mathbb{Q}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

Exercise 3.194. Determine the Galois group of the following polynomial: $x^3 - x + 1$.

Solution 3.195. We claim that $x^3 - x + 1$ is irreducible as an element in $\mathbb{Q}[x]$. By way of contradiction, suppose that there exist relatively prime integers a and $b \neq 0$ such that:

$$\left(\frac{a}{b}\right)^3 - \left(\frac{a}{b}\right) + 1 = 0.$$

So, we have that

$$a^3 = (a - b)b^2.$$

So, we have that b^2 divides a^3. But this is impossible since a and b are relatively prime, as may be verified using the Fundamental Theorem of Arithmetic. So, since $x^3 - x + 1$ has no rational roots, and since $x^3 - x + 1$ is of degree 3, we may conclude that $x^3 - x + 1$ is irreducible over $\mathbb{Q}$.

Galois groups for polynomials are only defined for separable polynomials, so it is worthwhile to check that $x^3 - x + 1$ is separable. By examining the graph of $x^3 - x + 1$, we find that $x^3 - x + 1$ has exactly one real root, which is in $(-2, -1)$. Let this real root be denoted as r. So, the only way $x^3 - x + 1$ could be non-separable would be in the situation whereby

$$x^3 - x + 1 = (x - r)(x - c)^2,$$

for some non-real complex number $c \in \mathbb{C} \setminus \mathbb{R}$. But the constant term in $(x - r)(x - c)^2$ is equal to $-rc^2 = 1$, with $c^2 = \frac{1}{-r}$, but this contradicts that c is a non-real complex number since $\frac{1}{-r}$ is positive. So, we have that $x^3 - x + 1$ is a separable polynomial.

The following discussion concerning Galois groups for cubic polynomials is taken from the class textbook:

"If the cubic polynomial $f(x)$ is irreducible then a root of $f(x)$ generates an extension of degree 3 over F, so the degree of the splitting field over F is divisible by 3. Since the Galois group is a subgroup of S_3, there are only two possibilities, namely A_3 or S_3. The Galois group is A_3 (i.e., cyclic of order 3) if and only if the discriminant... is a square." (p. 612-613)

In general, given a cubic polynomial

$$f(x) = x^3 + ax^2 + bx + c,$$

we have that the discriminant of this polynomial is

$$a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc.$$

So, we have that the discriminant of

$$x^3 + bx + c,$$

is

$$-4b^3 - 27c^2.$$

In particular, the discriminant of

$$x^3 - x + 1$$

is equal to

$$-4(-1)^3 - 27 = 4 - 27 = -23.$$

Since the given cubic polynomial $x^3 - x + 1$ is irreducible over $\mathbb{Q}$, we have that a root of $x^3 - x + 1$ generates an extension of degree 3 over $\mathbb{Q}$, so that the degree of the splitting field of $x^3 - x + 1$ over $\mathbb{Q}$ is divisible by 3. So, the corresponding Galois group is isomorphic to either S_3 or $\mathbb{Z}/3\mathbb{Z}$. Moreover, since the Galois group is A_3 if and only if the discriminant is a square, and since the discriminant of $x^3 - x + 1$ is equal to -23, we may thus conclude that the Galois group for $x^3 - x + 1$ over $\mathbb{Q}$ is isomorphic to the symmetric group S_3 of order 6.

3.21 Exercises from Section 14.7

Exercise 3.196. Use Cardano's Formulas to solve the equation $x^3 + x^2 - 2 = 0$. In particular show that the equation has the real root

$$\frac{1}{3}(\sqrt[3]{26 + 15\sqrt{3}} + \sqrt[3]{26 - 15\sqrt{3}} - 1).$$

Show directly that the roots of this cubic are $1, 1 \pm i$. Explain this by proving that

$$\sqrt[3]{26 + 15\sqrt{3}} = 2 + \sqrt{3} \quad \sqrt[3]{26 - 15\sqrt{3}} = 2 - \sqrt{3}$$

so that

$$\sqrt[3]{26 + 15\sqrt{3}} + \sqrt[3]{26 - 15\sqrt{3}} = 4.$$

Solution 3.197. We begin by briefly reviewing some preliminary material. Recall that the polynomial $f(x)$ can be solved by radicals if and only if its Galois group is a solvable group. Recall that a group G is *solvable* if there is a chain of subgroups

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_s = G$$

such that G_{i+1}/G_i is abelian for $i = 0, 1, \ldots, s-1$. So, if we consider the series $1 \trianglelefteq A_3 \trianglelefteq S_3$, we should expect that the given polynomial $x^3 + x^2 - 2$ could be solved by radicals. Given a degree-3 polynomial $f(x) = x^3 + ax^2 + bx + c$, consider the substitution $x = y - \frac{a}{3}$, yielding the polynomial

$$g(y) = y^3 + py + q,$$

where

$$p = \frac{1}{3}(3b - a^2) \qquad q = \frac{1}{27}(2a^3 - 9ab + 27c).$$

According to Cardano's formula, letting

$$A = \sqrt[3]{\frac{-27}{2}q + \frac{3}{2}\sqrt{-3D}}$$

and

$$B = \sqrt[3]{\frac{-27}{2}q - \frac{3}{2}\sqrt{-3D}},$$

where $D = -4p^3 - 27q^2$, the roots of the equation

$$g(y) = y^3 + py + q = 0$$

are

$$\alpha = \frac{A + B}{3} \qquad \beta = \frac{\rho^2 A + \rho B}{3} \qquad \gamma = \frac{\rho A + \rho^2 B}{3}$$

where $\rho = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$. Now, consider the given polynomial $x^3 + x^2 - 2 = 0$. Letting $f(x) = x^3 + x^2 - 2$, using the substitution $x = y - \frac{1}{3}$, yielding the polynomial

$$g(y) = y^3 + py + q,$$

where

$$p = -\frac{1}{3} \qquad q = -\frac{52}{27},$$

yielding the polynomial

$$g(y) = y^3 - \frac{y}{3} - \frac{52}{27}.$$

According to Cardano's formula, the roots for $g(y)$ in this case are as follows.

$$r_1 = \frac{1}{3}\left(\sqrt[3]{26 - 15\sqrt{3}} + \sqrt[3]{26 + 15\sqrt{3}}\right),$$
$$r_2 = \frac{1}{3}\left(\sqrt[3]{26 - 15\sqrt{3}}\left(-\frac{1}{2} + \frac{i\sqrt{3}}{2}\right) + \left(-\frac{1}{2} + \frac{i\sqrt{3}}{2}\right)^2 \sqrt[3]{26 + 15\sqrt{3}}\right),$$
$$r_3 = \frac{1}{3}\left(\sqrt[3]{26 - 15\sqrt{3}}\left(-\frac{1}{2} + \frac{i\sqrt{3}}{2}\right)^2 + \left(-\frac{1}{2} + \frac{i\sqrt{3}}{2}\right) \sqrt[3]{26 + 15\sqrt{3}}\right).$$

The equation

$$\sqrt[3]{26 + 15\sqrt{3}} = 2 + \sqrt{3}$$

may be verified using the binomial theorem, since

$$\left(2 + \sqrt{3}\right)^3 = 26 + 15\sqrt{3},$$

by the binomial theorem. Similarly, we have that

$$26 - 15\sqrt{3} = (2 - \sqrt{3})^3,$$

by the binomial theorem. We may use these equations to simplify the above evaluations for r_1, r_2, and r_3: $r_1 = \frac{4}{3}$, $r_2 = -\frac{2}{3} - i$, and $r_3 = -\frac{2}{3} + i$. Given the substitution $x = y - \frac{1}{3}$, we thus have that the roots of the original cubic polynomial are 1, $-1 \pm i$.

3.22 Exercises from Section 14.8

Exercise 3.198. Let p be a prime. Prove that the polynomial $x^4 + 1$ splits mod p either into two irreducible quadratics or into 4 linear factors using Corollary 41 together with the knowledge that the Galois group of this polynomial is the Klein 4-group.

Solution 3.199. Corollary 41 from the class textbook is given as follows:

Corollary 41. For any prime p not dividing the discriminant of $f(x) \in \mathbb{Z}[x]$, the Galois group of $f(x)$ over $\mathbb{Q}$ contains an element with cycle decomposition $(n_1, n_2, \ldots, n_k)$ where $n_1, n_2, \ldots, n_k$ are the degrees of the irreducible factors of $f(x)$ reduced modulo p.

As in the class textbook, we define the *discriminant* D of $x_1, x_2, \ldots, x_n$ by the equation

$$D = \prod_{i<j} (x_i - x_j)^2,$$

and we define the discriminant of a polynomial as the discriminant of the roots of the polynomial.

We proceed to consider the Galois group of the given polynomial $x^4 + 1$. From the equation $x^4 + 1 = 0$, we have that $x^4 = -1$, so that $x^2 = \pm i$, with x equal to $\pm\sqrt{\pm i}$. Since $(i+1)^2 = 2i$, we have that

$$\sqrt{i} = \frac{i+1}{\sqrt{2}}.$$

Similarly, we have that

$$\sqrt{-i} = \frac{i-1}{\sqrt{2}}.$$

So, we find that the polynomial $x^4 + 1$ is separable, so it would make sense to consider the Galois group of $x^4 + 1$.

Now, consider the splitting field of $x^4 + 1$ over $\mathbb{Q}$. This splitting field must contain

$$\sqrt{i} = \frac{i+1}{\sqrt{2}}$$

and

$$\sqrt{-i} = \frac{i-1}{\sqrt{2}},$$

and therefore must contain

$$\sqrt{i} - \sqrt{-i} = \frac{i+1}{\sqrt{2}} - \frac{i-1}{\sqrt{2}} = \frac{2}{\sqrt{2}} = \sqrt{2}.$$

Similarly, the splitting field of $x^4 + 1$ over $\mathbb{Q}$ must contain $\sqrt{2}i$. So, we see that the field $\mathbb{Q}(\sqrt{2}, i)$ is contained in the splitting field of $x^4 + 1$ over $\mathbb{Q}$. Conversely, an element in the splitting field of $x^4 + 1$ over $\mathbb{Q}$ must be in $\mathbb{Q}(\sqrt{2}, i)$, since the roots of $x^4 + 1$ are precisely $\pm\left(\frac{i+1}{\sqrt{2}}\right)$ and $\pm\left(\frac{i-1}{\sqrt{2}}\right)$.

Now, consider the Galois group of $\mathbb{Q}(\sqrt{2}, i)$ over $\mathbb{Q}$. Given an automorphism σ in this group, we have that the behaviour of σ is uniquely determined by the values of $\sigma(\sqrt{2})$ and $\sigma(i)$, with $\sigma(\sqrt{2}) \in \{\sqrt{2}, -\sqrt{2}\}$ and $\sigma(i) \in \{i, -i\}$. Since

$$\left|\mathrm{Gal}\left(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}\right)\right| = 4,$$

and since each element

$$g \in \mathrm{Gal}\left(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}\right)$$

is such that $g^2 = \mathrm{id}$, letting id denote the identity morphism in the above group, we may deduce that the Galois group of $x^4 + 1$ is isomorphic to the Klein four-group.

Now, consider the discriminant of the polynomial $x^4 + 1$. Let the roots of this polynomial be denoted as follows:

$$x_1 = \frac{i+1}{\sqrt{2}}, \qquad x_2 = -\frac{i+1}{\sqrt{2}}, \qquad x_3 = \frac{i-1}{\sqrt{2}}, \qquad x_4 = -\frac{i-1}{\sqrt{2}}.$$

We thus have that the discriminant of $x^4 + 1$ is equal to the following expression:

$$D = \prod_{i<j} (x_i - x_j)^2.$$

So, we have that:

$$D = (x_1 - x_2)^2 (x_1 - x_3)^2 (x_1 - x_4)^2 (x_2 - x_3)^2 (x_2 - x_4)^2 (x_3 - x_4)^2.$$

Computing the above expression, we have that $D = 256 = 2^8$.

Now, we can only apply **Corollary 41** with respect to primes p not dividing the discriminant of $x^4 + 1$. Since the discriminant of this polynomial is equal to $D = 256 = 2^8$, letting p be a prime, we first consider the case whereby $p = 2$. In this case, we have that

$$(x + 1)^4 \equiv (x^4 + 1)(\text{mod } 2),$$

by the binomial theorem. So, in the case whereby p is a prime number such that $p = 2$, we have that the polynomial $x^4 + 1$ splits modulo p into 4 linear factors.

Now, let p be a prime number such that $p \neq 2$. Since the discriminant D of $x^4 + 1$ is equal to $256 = 2^8$, we have that p does not divide the discriminant of $x^4 + 1$ in this case. Since the Galois group of $x^4 + 1$ over $\mathbb{Q}$ is a Klein four-subgroup of S_4, the only possible cycle decompositions are: $(2)(2)$, $(1)(1)(1)(1)$, or $(2)(1)(1)$.

By **Proposition 34** from the class textbook, we know that the Galois group of $x^4 + 1$ as an element in $\mathbb{Q}[x]$ is a subgroup of A_4 if and only if the discriminant $D \in \mathbb{Q}$ is the square of an element in $\mathbb{Q}$. But recall that the discriminant D of $x^4 + 1$ is equal to $D = 256 = 2^8$. We thus have that the Galois group of $x^4 + 1$ must be in A_4, which shows that the only possible cycle decompositions are reduced to $(2)(2)$ and the trivial cycle decomposition, as desired. Since the only possible cycle decompositions in this case are $(2)(2)$ and $(1)(1)(1)(1)$, we have that the degrees of the irreducible factors of $f(x)$ modulo p given by either the sequence $(2, 2)$ or $(1, 1, 1, 1)$.