

Notes on the book: *Patrick Morandi, Field and Galois Theory*

Meng-Gen Tsai
plover@gmail.com

August 29, 2021

Contents

I. Galois Theory	3
§1. Field Extensions	3
Problem 1.1.	3
Problem 1.2.	3
Problem 1.3.	4
Problem 1.4.	4
Problem 1.5.	5
Problem 1.9.	6
Problem 1.11.	6
Problem 1.12.	7
Problem 1.16.	7
Problem 1.23.	8
Problem 1.24.	8
Problem 1.25.	9
§2. Automorphisms	9
Problem 2.1.	9
Problem 2.2.	10
Problem 2.4.	10
II. Some Galois Extensions	12
§10. Hilbert Theorem 90 and Group Cohomology	12
Supplement.	12
Problem 10.1.	14
Problem 10.2.	16
Supplement.	17
Problem 10.3.	18
Problem 10.4.	18
Problem 10.5.	19

Problem 10.6.	20
Problem 10.7.	20

I. Galois Theory

§1. Field Extensions

Problem 1.1.

Let K be a field extension of F . By defining scalar multiplication for $\alpha \in F$ and $a \in K$ by $\alpha \cdot a = \alpha a$, the multiplication in K , show that K is an F -vector space.

Proof.

(1) K is an additive group.

(2) Show that $(\alpha\beta) \cdot a = \alpha \cdot (\beta \cdot a)$ for $\alpha, \beta \in F$ and $a \in K$. In fact,

$$\begin{aligned}(\alpha\beta) \cdot a &= \alpha\beta a \in K, \\ \alpha \cdot (\beta \cdot a) &= \alpha\beta a \in K.\end{aligned}$$

(3) Show that $(\alpha + \beta) \cdot a = \alpha \cdot a + \beta \cdot a$ for $\alpha, \beta \in F$ and $a \in K$.

$$\begin{aligned}(\alpha + \beta) \cdot a &= (\alpha + \beta)a \\ &= \alpha a + \beta a \in K, \\ \alpha \cdot a + \beta \cdot a &= \alpha a + \beta a \in K.\end{aligned}$$

(4) Show that $\alpha \cdot (a + b) = \alpha \cdot a + \alpha \cdot b$ for $\alpha \in F$ and $a, b \in K$.

$$\begin{aligned}\alpha \cdot (a + b) &= \alpha(a + b) \\ &= \alpha a + \alpha b \in K, \\ \alpha \cdot a + \alpha \cdot b &= \alpha a + \alpha b \in K.\end{aligned}$$

(5) Show that $1 \cdot a = a$ for $a \in K$. $1 \cdot a = 1a = a \in K$.

By (1) to (5), K is an F -vector space. \square

Problem 1.2.

If K is a field extension of F , prove that $[K : F] = 1$ if and only if $K = F$.

Proof.

(1) $[K : F] = 1 \iff K = F$. Take a basis $\{1\}$ for K as an F -vector space.

- (2) $[K : F] = 1 \implies K = F$. Take a basis $\{a\}$ for K as an F -vector space where $a \in K$. Since $1 \in K$ as an F -vector space, there exists $\alpha \in F$ such that $1 = \alpha a$. $a = \alpha^{-1} \in F$, or $K \subseteq F$, or $K = F$.

□

Problem 1.3.

Let K be a field extension of F , and let $a \in K$. Show that the evaluation map $ev_a : F[x] \rightarrow K$ given by $ev_a(f(x)) = f(a)$ is a ring and F -vector space homomorphism. (Such a map is called an F -algebra homomorphism.)

Proof.

- (1) ev_a is a ring homomorphism.

$$(a) \quad ev_a(f(x) + g(x)) = f(a) + g(a) = ev_a(f(x)) + ev_a(g(x)).$$

$$(b) \quad ev_a(f(x)g(x)) = g(a)f(a) = ev_a(g(x))ev_a(f(x)).$$

$$(c) \quad ev_a(1) = 1.$$

- (2) ev_a is an F -vector space homomorphism.

$$(a) \quad ev_a(f(x) + g(x)) = f(a) + g(a) = ev_a(f(x)) + ev_a(g(x)).$$

$$(b) \quad \text{Given } c \in F, ev_a(cf(x)) = cf(a) = c ev_a(f(x)).$$

□

Problem 1.4.

Prove Proposition 1.9: Let K be a field extension of F and let $a_1, \dots, a_n \in K$. Then

$$F[a_1, \dots, a_n] = \{f(a_1, \dots, a_n) : f \in F[x_1, \dots, x_n]\}$$

and

$$F(a_1, \dots, a_n) = \left\{ \frac{f(a_1, \dots, a_n)}{g(a_1, \dots, a_n)} : f, g \in F[x_1, \dots, x_n], g(a_1, \dots, a_n) \neq 0 \right\},$$

so $F(a_1, \dots, a_n)$ is the quotient field of $F[x_1, \dots, x_n]$.

Proof (Proposition 1.8).

- (1) The evaluation map $ev_{(a_1, \dots, a_n)} : F[x_1, \dots, x_n] \rightarrow K$ has image

$$\{f(a_1, \dots, a_n) : f \in F[x_1, \dots, x_n]\},$$

so this set is a subring of K .

(2) If R is a subring of K that contains F and a_1, \dots, a_n , then

$$f(a_1, \dots, a_n) \in R$$

for any $f(x_1, \dots, x_n) \in F[x_1, \dots, x_n]$ by closure of addition and multiplication.

(3) So $\{f(a_1, \dots, a_n) : f \in F[x_1, \dots, x_n]\}$ is contained in all subrings of K that contains F and a_1, \dots, a_n . Hence

$$F[a_1, \dots, a_n] = \{f(a_1, \dots, a_n) : f \in F[x_1, \dots, x_n]\}.$$

(4) The quotient field of $F[a_1, \dots, a_n]$ is then the set

$$\left\{ \frac{f(a_1, \dots, a_n)}{g(a_1, \dots, a_n)} : f, g \in F[x_1, \dots, x_n], g(a_1, \dots, a_n) \neq 0 \right\}.$$

It is clearly is contained in any subfield of K that contains $F[a_1, \dots, a_n]$; hence, it is equal to $F(a_1, \dots, a_n)$.

□

Problem 1.5.

Show that $\mathbb{Q}(\sqrt{5}, \sqrt{7}) = \mathbb{Q}(\sqrt{5} + \sqrt{7})$.

Proof.

(1) $\mathbb{Q}(\sqrt{5}, \sqrt{7}) \supseteq \mathbb{Q}(\sqrt{5} + \sqrt{7})$ since $\sqrt{5} + \sqrt{7} \in \mathbb{Q}(\sqrt{5}, \sqrt{7})$.

(2)

$$\begin{aligned} (\sqrt{7} + \sqrt{5})^{-1} &= \frac{1}{\sqrt{7} + \sqrt{5}} \\ &= \frac{\sqrt{7} - \sqrt{5}}{(\sqrt{7} + \sqrt{5})(\sqrt{7} - \sqrt{5})} \\ &= \frac{\sqrt{7} - \sqrt{5}}{2} \in \mathbb{Q}(\sqrt{5} + \sqrt{7}), \end{aligned}$$

Or $\sqrt{7} - \sqrt{5} \in \mathbb{Q}(\sqrt{5} + \sqrt{7})$. Thus

$$\begin{aligned} \sqrt{7} &= \frac{1}{2} \cdot ((\sqrt{7} + \sqrt{5}) + (\sqrt{7} - \sqrt{5})) \in \mathbb{Q}(\sqrt{5} + \sqrt{7}), \\ \sqrt{5} &= \frac{1}{2} \cdot ((\sqrt{7} + \sqrt{5}) - (\sqrt{7} - \sqrt{5})) \in \mathbb{Q}(\sqrt{5} + \sqrt{7}). \end{aligned}$$

Thus, $\mathbb{Q}(\sqrt{5}, \sqrt{7}) \subseteq \mathbb{Q}(\sqrt{5} + \sqrt{7})$.

By (1)(2), $\mathbb{Q}(\sqrt{5}, \sqrt{7}) = \mathbb{Q}(\sqrt{5} + \sqrt{7})$. □

Problem 1.9.

If K is an extension of F such that $[K : F]$ is prime, show that there are no intermediate fields between K and F .

Proof. Let L be any field such that $F \subseteq L \subseteq K$. By Proposition 1.20,

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

Since $[K : F]$ is prime, $[K : L] = 1$ or $[L : F] = 1$. By Problem 1.2, $L = K$ or $L = F$, or there are no intermediate fields between K and F . \square

Problem 1.11.

If K is an algebraic extension of F and if R is a subring of K with $F \subseteq R \subseteq K$, show that R is a field.

Proof.

- (1) R is a domain since R is contained in a field K . To show R is a field, it suffices to show that every nonzero element $\alpha \in R$ has an inverse in R .
- (2) Since $\alpha \in R \subseteq K$ is algebraic over F , there is a minimal polynomial

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

such that $f(\alpha) = 0$, where each $b_i \in F$ and $b_0 \neq 0$ by the minimality of f .

- (3) Note that

$$\begin{aligned} f(\alpha) &= 0 \\ \iff b_n \alpha^n + b_{n-1} \alpha^{n-1} + \cdots + b_0 &= 0 \\ \iff b_n \alpha^n + b_{n-1} \alpha^{n-1} + \cdots + b_1 \alpha &= -b_0 \\ \iff \alpha(b_n \alpha^{n-1} + b_{n-1} \alpha^{n-2} + \cdots + b_1) &= -b_0 \\ \iff \alpha \underbrace{((-b_0)^{-1} b_n \alpha^{n-1} + (-b_0)^{-1} b_{n-1} \alpha^{n-2} + \cdots + (-b_0)^{-1} b_1)}_{:=\alpha'} &= 1. \end{aligned}$$

Hence $\alpha' \in F[\alpha] \subseteq R$. Therefore α' is the inverse of α in R .

\square

Problem 1.12.

Show that $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ are not isomorphic as fields but are isomorphic as vector spaces over \mathbb{Q} .

Proof.

- (1) Show that $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ are not isomorphic as fields. (Reductio ad absurdum) If $\varphi : \mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{Q}(\sqrt{3})$ were an isomorphism as fields, then φ is an identity map on \mathbb{Q} , and

$$\begin{aligned}\varphi(\sqrt{2}) &= a + b\sqrt{3} \text{ for some } a, b \in \mathbb{Q} \\ \implies \varphi(\sqrt{2})\varphi(\sqrt{2}) &= (a + b\sqrt{3})^2 \\ \implies \varphi(\sqrt{2}\sqrt{2}) &= (a + b\sqrt{3})^2 \\ \implies \varphi(2) &= a^2 + 3b^2 + 2ab\sqrt{3} \\ \implies 2 &= a^2 + 3b^2 + 2ab\sqrt{3}.\end{aligned}$$

If $2ab \neq 0$, then $\sqrt{3} = \frac{2-a^2-3b^2}{2ab} \in \mathbb{Q}$, which is absurd. Hence $2ab = 0$.

- (a) $a = 0$. Write $b = \frac{m}{n} \in \mathbb{Q}$ where $m, n \in \mathbb{Z}$ and $(m, n) = 1$. Hence

$$2n^2 = 3m^2.$$

So $2 \mid 3m^2$, $2 \mid m^2$, $2 \mid m$. So $4 \mid 2n^2$, $2 \mid n^2$, $2 \mid n$. Hence $2 \mid (m, n)$, contrary to the assumption that $(m, n) = 1$.

- (b) $b = 0$. $2 = a^2$. Write $a = \frac{m}{n} \in \mathbb{Q}$ where $m, n \in \mathbb{Z}$ and $(m, n) = 1$. Similar to the argument in (a), we will reach a contradiction.

By (a)(b), no such isomorphism φ , that is, $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ are not isomorphic as fields.

- (2) Show that $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ are isomorphic as \mathbb{Q} -vector spaces. $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$. There is a natural map $\varphi : \mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{Q}(\sqrt{3})$ defined by $\varphi(a + b\sqrt{2}) = a + b\sqrt{3}$. Clearly φ is well-defined, linear, injective and surjective.

□

Problem 1.16.

Let \mathbb{A} be the algebraic closure of \mathbb{Q} in \mathbb{C} . Prove that $[\mathbb{A} : \mathbb{Q}] = \infty$.

Proof (Example 1.16). By Example 1.16, $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$. Therefore,

$$[\mathbb{A} : \mathbb{Q}] = [\mathbb{A} : \mathbb{Q}(\sqrt[n]{2})][\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = [\mathbb{A} : \mathbb{Q}(\sqrt[n]{2})]n$$

for arbitrary $n \in \mathbb{Z}^+$. Hence $[\mathbb{A} : \mathbb{Q}] = \infty$. \square

Proof (Example 1.16). Given a prime number p . By Example 1.16, $[\mathbb{Q}(\rho) : \mathbb{Q}] = p - 1$ where $\rho = \exp(2\pi i/p)$. Therefore,

$$[\mathbb{A} : \mathbb{Q}] = [\mathbb{A} : \mathbb{Q}(\rho)][\mathbb{Q}(\rho) : \mathbb{Q}] = [\mathbb{A} : \mathbb{Q}(\rho)](p - 1)$$

for arbitrary prime p . Hence $[\mathbb{A} : \mathbb{Q}] = \infty$. \square

Problem 1.23.

Recall that the characteristic of a ring R with identity is the smallest positive integer n for which $n \cdot 1 = 0$, if such an n exists, or else the characteristic is 0. Let R be a ring with identity. Define $\varphi : \mathbb{Z} \rightarrow R$ by $\varphi(n) = n \cdot 1$, where 1 is the identity of R . Show that φ is a ring homomorphism and that $\ker(\varphi) = m\mathbb{Z}$ for a unique nonnegative integer m , and show that m is the characteristic of R .

Proof.

(1) φ is a ring homomorphism.

$$(a) \quad \varphi(a+b) = \varphi(a) + \varphi(b). \quad \varphi(a+b) = (a+b) \cdot 1 = a \cdot 1 + b \cdot 1 = \varphi(a) + \varphi(b).$$

$$(b) \quad \varphi(ab) = \varphi(a)\varphi(b). \quad \varphi(ab) = (ab) \cdot 1 = (a \cdot 1)(b \cdot 1) = \varphi(a)\varphi(b) \text{ since } 1 \times 1 = 1. \text{ (Here } \times \text{ is the multiplication operator of } R\text{.)}$$

(2) $\ker(\varphi) = m\mathbb{Z}$ for a unique nonnegative integer m . Since $\ker(\varphi)$ is an ideal of a PID \mathbb{Z} , there is a unique nonnegative integer m such that $\ker(\varphi) = m\mathbb{Z}$.

(3) m is the characteristic of R . There are only two possible cases, $\text{char}(R) = 0$ or else $\text{char}(R) > 0$.

$$(a) \quad \text{char}(R) = 0. \quad \ker(\varphi) = 0. \quad \text{Thus } m = 0 = \text{char}(R).$$

$$(b) \quad \text{char}(R) = n > 0. \quad n \in \ker(\varphi), \text{ so } m > 0 \text{ and } m \mid n. \text{ By the minimality of } n, \quad m = n = \text{char}(R).$$

\square

Problem 1.24.

For any positive integer n , give an example of a ring of characteristic n .

Proof. The ring $\mathbb{Z}/n\mathbb{Z}$. \square

Problem 1.25.

If R is an integral domain, show that either $\text{char}(R) = 0$ or $\text{char}(R)$ is prime.

Proof.

- (1) 1 has infinite order. $\text{char}(R) = 0$. (Nothing to do.)
- (2) 1 has finite order n . Want to show n is prime. If $n = ab$ where $a, b \in \mathbb{Z}^+$, then

$$0 = n \cdot 1 = (a \cdot 1)(b \cdot 1).$$

Since R is an integral domain, $a \cdot 1 = 0$ or $b \cdot 1 = 0$. By the minimality of n , $a \geq n$ or $b \geq n$. $a = n$ or $b = n$. That is, n is prime.

□

§2. Automorphisms**Problem 2.1.**

Show that the only automorphism of \mathbb{Q} is the identity.

Proof. Given any $\sigma \in \text{Aut}(\mathbb{Q})$.

- (1) Show that $\sigma(1) = 1$. Since $1^2 = 1$, $\sigma(1)\sigma(1) = \sigma(1)$. $\sigma(1) = 0$ or 1 . There are only two possible cases.

- (a) Assume that $\sigma(1) = 0$. So

$$\sigma(a) = \sigma(a \cdot 1) = \sigma(a) \cdot \sigma(1) = \sigma(a) \cdot 0 = 0$$

for any $a \in \mathbb{Q}$. That is, $\sigma = 0 \in \text{Aut}(\mathbb{Q})$, which is absurd.

- (b) Therefore, $\sigma(1) = 1$.

- (2) Show that $\sigma(n) = n$ for all $n \in \mathbb{Z}^+$. Write $n = 1 + 1 + \cdots + 1$ (n times 1). Applying the additivity of σ , we have

$$\sigma(n) = \sigma(1) + \sigma(1) + \cdots + \sigma(1) = 1 + 1 + \cdots + 1 = n.$$

(Might use induction on n to eliminate \cdots symbols.)

- (3) Show that $\sigma(n) = n$ for all $n \in \mathbb{Z}$. By the additivity of σ , $\sigma(-n) = -\sigma(n) = -n$ for $n \geq 0$. The result is established.

For any $a = \frac{n}{m} \in \mathbb{Q}$ ($m, n \in \mathbb{Z}$, $n \neq 0$), applying the multiplication of σ on $am = n$, that is, $\sigma(a)\sigma(m) = \sigma(n)$. By (3), we have $\sigma(a)m = n$, or

$$\sigma(a) = \frac{m}{n} = a$$

provided $n \neq 0$, or σ is the identity. \square

Problem 2.2.

Show that the only automorphism of \mathbb{R} is the identity. (Hint: If σ is an automorphism, show that $\sigma|_{\mathbb{Q}} = \text{id}$, and if $a > 0$, then $\sigma(a) > 0$. It is an interesting fact that there are infinitely many automorphisms of \mathbb{C} , even though $[\mathbb{C} : \mathbb{R}] = 2$. Why is this fact not a contradiction to this problem?)

Proof (Hint). Given any $\sigma \in \text{Aut}(\mathbb{R})$.

- (1) Apply the same argument in Problem 2.1, we have $\sigma|_{\mathbb{Q}} = \text{id}$. Notice that $\sigma(a) \neq 0$ for any $a \neq 0$.
- (2) Show that $\sigma(a) > 0$ if $a > 0$. Given any $a > 0$. Write $a = \sqrt{a}\sqrt{a}$ (well-defined) and then apply σ on the both sides,

$$\sigma(a) = \sigma(\sqrt{a})\sigma(\sqrt{a}) = \sigma(\sqrt{a})^2 > 0$$

(since $\sqrt{a} \neq 0$ and thus $\sigma(\sqrt{a})$ cannot be zero).

- (3) Show that $\sigma(a) > \sigma(b)$ if $a > b$. It is a corollary to (2) by applying σ on $a - b > 0$. ($\sigma(a - b) > 0$, or $\sigma(a) - \sigma(b) > 0$, or $\sigma(a) > \sigma(b)$.)
- (4) For any real number $x \in \mathbb{R}$, choose two sequences $\{p_n\}, \{q_n\}$ of rational numbers such that $p_n < x < q_n$ and $p_n, q_n \rightarrow x$ as $n \rightarrow \infty$. Take σ on the inequality, $\sigma(p_n) < \sigma(x) < \sigma(q_n)$. So $p_n < \sigma(x) < q_n$ since $\sigma|_{\mathbb{Q}} = \text{id}$. Let $n \rightarrow \infty$, we get $x \leq \sigma(x) \leq x$, or $\sigma(x) = x$.

\square

Supplement. Automorphisms of the Complex Numbers. by Paul B. Yale (Pomona College) [Link].

Problem 2.4.

Let B be an integral domain with quotient field F . If $\sigma : B \rightarrow B$ is a ring automorphism, show that σ induces a ring automorphism $\sigma' : F \rightarrow F$ defined by $\sigma'(a/b) = \sigma(a)/\sigma(b)$ if $a, b \in B$ with $b \neq 0$.

Proof.

(1) Show that σ' is well-defined.

- (a) $\sigma' : F \rightarrow F$ is defined. $\sigma(a), \sigma(b) \in B$ since σ is a homomorphism.
 $\sigma(b) \neq 0$ since $b \neq 0$ and σ is a one-on-one homomorphism.
- (b) σ' is independent of the representation of $a/b \in F$. Suppose $a/b = c/d$ where $a, b, c, d \in B$ and $b, d \neq 0$. Hence,

$$\begin{aligned}
 a/b = c/d &\iff ad = bc \\
 &\iff \sigma(ad) = \sigma(bc) \\
 &\iff \sigma(a)\sigma(d) = \sigma(b)\sigma(c) \quad (\sigma: \text{homomorphism}) \\
 &\iff \sigma(a)/\sigma(d) = \sigma(c)/\sigma(b) \quad (\sigma(b), \sigma(d) \neq 0) \\
 &\iff \sigma'(a/b) = \sigma'(c/d).
 \end{aligned}$$

(2) Show that σ' is a ring homomorphism.

- (a) Show that $\sigma'(a/b + c/d) = \sigma'(a/b) + \sigma'(c/d)$.

$$\begin{aligned}
 \sigma'(a/b + c/d) &= \sigma'((ad + bc)/(bd)) \\
 &= \sigma(ad + bc)/\sigma(bd) \\
 &= (\sigma(a)\sigma(d) + \sigma(b)\sigma(c))/(\sigma(b)\sigma(d)) \quad (\sigma: \text{homomorphism}) \\
 &= \sigma(a)/\sigma(b) + \sigma(c)/\sigma(d) \\
 &= \sigma'(a/b) + \sigma'(c/d).
 \end{aligned}$$

- (b) Show that $\sigma'(a/b \cdot c/d) = \sigma'(a/b) \cdot \sigma'(c/d)$.

$$\begin{aligned}
 \sigma'(a/b \cdot c/d) &= \sigma'((ac)/(bd)) \\
 &= \sigma(ac)/\sigma(bd) \\
 &= (\sigma(a)\sigma(c))/(\sigma(b)\sigma(d)) \quad (\sigma: \text{homomorphism}) \\
 &= \sigma(a)/\sigma(b) \cdot \sigma(c)/\sigma(d) \\
 &= \sigma'(a/b) \cdot \sigma'(c/d).
 \end{aligned}$$

(3) Show that σ' is injective.

$$\begin{aligned}
 \sigma'(a/b) = 0 &\iff \sigma(a)/\sigma(b) = 0 \\
 &\iff \sigma(a) = 0 \\
 &\iff a = 0 \quad (\sigma: \text{injective}) \\
 &\iff a/b = 0/b = 0 \in F
 \end{aligned}$$

(4) Show that σ' is a surjective. Given any $c/d \in F$, want to show there is $a/b \in F$ such that $\sigma'(a/b) = c/d$.

$$\begin{aligned}
 c/d \in F &\implies c, d \in B \\
 &\implies \exists a, b \in B \text{ such that } \sigma(a) = c, \sigma(b) = d \quad (\sigma: \text{surjective}) \\
 &\implies \exists a, b \in B \text{ such that } \sigma(a)/\sigma(b) = c/d \\
 &\implies \exists a, b \in B \text{ such that } \sigma'(a/b) = c/d.
 \end{aligned}$$

II. Some Galois Extensions

§10. Hilbert Theorem 90 and Group Cohomology

Supplement.

- (1) Corollary 10.4 (Cohomological Hilbert Theorem 90). Let K be a cyclic Galois extension of F . Then $H^1(\text{Gal}(K/F), K^\times) = 0$.
- (2) (*Exercise 10.24 in the textbook: Rudin, Principles of Mathematical Analysis, 3rd edition.*) Let $\omega = \sum a_i(\mathbf{x})dx_i$ be a 1-form of class C'' in a convex open set $E \subseteq \mathbb{R}^n$. Assume $d\omega = 0$ and prove that ω is exact in E . Hence the first de Rham cohomology $H_{\text{dR}}^1(E) = 0$.
- (3) $H_{\text{dR}}^1(E) = 0$ if E is simply connected. (The converse is not true.)
- (4) (*Exercise 10.21 in the textbook: Rudin, Principles of Mathematical Analysis, 3rd edition.*) Consider the 1-form

$$\eta = \frac{xdy - ydx}{x^2 + y^2}$$

in $\mathbb{R}^2 - \{\mathbf{0}\}$.

- (a) Carry out the computation that leads to

$$\int_{\gamma} \eta = 2\pi \neq 0,$$

and prove that $d\eta = 0$.

- (b) Let $\gamma(t) = (r \cos t, r \sin t)$, for some $r > 0$, and let Γ be a C'' -curve in $\mathbb{R}^2 - \{\mathbf{0}\}$, with parameter interval $[0, 2\pi]$, with $\Gamma(0) = \Gamma(2\pi)$, such that the intervals $[\gamma(t), \Gamma(t)]$ do not contain $\mathbf{0}$ for any $t \in [0, 2\pi]$. Prove that

$$\int_{\Gamma} \eta = 2\pi.$$

- (c) Take $\Gamma(t) = (a \cos t, b \sin t)$ where $a > 0$, $b > 0$ are fixed. Show that

$$\int_0^{2\pi} \frac{ab}{a^2 \cos^2 t + b^2 \sin^2 t} dt = 2\pi.$$

- (d) Show that

$$\eta = d\left(\arctan \frac{y}{x}\right)$$

in any convex open set in which $x \neq 0$, and that

$$\eta = d \left(-\arctan \frac{x}{y} \right)$$

in any convex open set in which $y \neq 0$. Explain why this justifies the notation $\eta = d\theta$, in spite of the fact that η is not exact in $\mathbb{R}^2 - \{0\}$.

- (5) (Exercise 10.22 in the textbook: Rudin, *Principles of Mathematical Analysis*, 3rd edition.) Define ζ in $\mathbb{R}^3 - \{0\}$ by

$$\zeta = \frac{xdy \wedge dz + ydz \wedge dx + zdx \wedge dy}{r^3}$$

where $r = (x^2 + y^2 + z^2)^{\frac{1}{2}}$, let D be the rectangle given by $0 \leq u \leq \pi$, $0 \leq v \leq 2\pi$, and let Σ be the 2-surface in \mathbb{R}^3 , with parameter domain D , given by

$$x = \sin u \cos v, \quad y = \sin u \sin v, \quad z = \cos u.$$

- (a) Prove that $d\zeta = 0$ in $\mathbb{R}^3 - \{0\}$.
 (b) Let S denote the restriction of Σ to a parameter domain $E \subseteq D$. Prove that

$$\int_S \zeta = \int_E \sin u \, du \, dv = A(S),$$

where A denotes area, as in Section 10.46. Note that this contains

$$\int_{\Sigma} \zeta = \int_D \sin u \, du \, dv = 4\pi \neq 0$$

as a special case.

- (c) Suppose g, h_1, h_2, h_3 , are C'' -functions on $[0, 1]$, $g > 0$. Let $(x, y, z) = \Phi(s, t)$ define a 2-surface Φ , with parameter domain I^2 , by

$$x = g(t)h_1(s), \quad y = g(t)h_2(s), \quad z = g(t)h_3(s).$$

Prove that

$$\int_{\Phi} \zeta = 0.$$

Note the shape of the range of Φ : For fixed s , $\Phi(s, t)$ runs over an interval on a line through 0 . The range of Φ thus lies in a “cone” with vertex at the origin.

- (d) Let E be a closed rectangle in D , with edges parallel to those of D . Suppose $f \in C''(D)$, $f > 0$. Let Ω be the 2-surface with parameter domain E , defined by

$$\Omega(u, v) = f(u, v)\Sigma(u, v).$$

Define S as in (b) and prove that

$$\int_{\Omega} \zeta = \int_S \zeta = A(S).$$

(e) Put $\lambda = -\frac{z}{r}\eta$, where

$$\eta = \frac{xdy - ydx}{x^2 + y^2}.$$

Then λ is a 1-form in the open set $V \subseteq \mathbb{R}^3$ in which $x^2 + y^2 > 0$. Show that ζ is exact in V by showing that

$$\zeta = d\lambda.$$

(f) Is ζ exact in the complement of every line through the origin?

- (6) (Exercise 10.23 in the textbook: Rudin, Principles of Mathematical Analysis, 3rd edition.) Fix n . Define $r_k = (x_1^2 + \cdots + x_k^2)^{\frac{1}{2}}$ for $1 \leq k \leq n$, let E_k be the set of all $\mathbf{x} \in \mathbb{R}^n$ at which $r_k > 0$, and let ω_k be the $(k-1)$ -form defined in E_k by

$$\omega_k = (r_k)^{-k} \sum_{i=1}^k (-1)^{i-1} x_i dx_1 \wedge \cdots \wedge \widehat{dx_i} \wedge \cdots \wedge dx_k$$

Note that $\omega_2 = \eta$, $\omega_3 = \zeta$ in the terminology of Exercise 10.21 and Exercise 10.22. Note also that

$$E_1 \subseteq E_2 \subseteq \cdots \subseteq E_n = \mathbb{R}^n.$$

(a) Prove that $d\omega_k = 0$ in E_k .

(b) For $k = 2, \dots, n$, prove that ω_k is exact in E_{k-1} , by showing that

$$\omega_k = d(f_k \omega_{k-1}) = df_k \wedge \omega_{k-1}$$

where $f_k(\mathbf{x}) = (-1)^k g_k \left(\frac{x_k}{r_k} \right)$ where

$$g_k(t) = \int_{-1}^t (1 - s^2)^{\frac{k-3}{2}} ds \quad (-1 < t < 1).$$

(c) Is ω_n exact in E_n ?

- (7) $H_{\text{dR}}^{n-1}(\mathbb{R}^n - \{\mathbf{0}\}) = \mathbb{R}^1$. (Compare to (5)(6)(7).)

Problem 10.1.

Let M be a G -module. Show that the boundary map $\delta_n : C^n(G, M) \rightarrow C^{n+1}(G, M)$ defined in this section is a homomorphism.

Proof.

(1) δ_n is defined by

$$\begin{aligned}\delta_n(f)(\sigma_1, \dots, \sigma_{n+1}) &= \sigma_1 f(\sigma_2, \dots, \sigma_{n+1}) \\ &\quad + \sum_{i=1}^n (-1)^i f(\sigma_1, \dots, \sigma_i \sigma_{i+1}, \dots, \sigma_{n+1}) \\ &\quad + (-1)^{n+1} f(\sigma_1, \dots, \sigma_n)\end{aligned}$$

if $n > 0$. If $n = 0$, then the map $\delta_0 : M = C^0(G, M) \rightarrow C^1(G, M)$ is defined by $\delta_0(m)(\sigma) = \sigma m - m$.

(2) It suffices to show that $\delta_n(f+g) = \delta_n(f) + \delta_n(g)$ for all n and all n -cochains f and g .

(3) If $n = 0$, then

$$\begin{aligned}\delta_0(f+g)(\sigma) &= \sigma(f+g) - (f+g) \\ &= \sigma f + \sigma g - f - g && (M: G\text{-module}) \\ &= (\sigma f - f) + (\sigma g - g) && (M: \text{abelian group}) \\ &= \delta_0(f) + \delta_0(g).\end{aligned}$$

(4) If $n \geq 1$, then

$$\begin{aligned}&\delta_n(f+g)(\sigma) \\ &= \sigma_1(f+g)(\sigma_2, \dots, \sigma_{n+1}) + \sum_{i=1}^n (-1)^i (f+g)(\sigma_1, \dots, \sigma_i \sigma_{i+1}, \dots, \sigma_{n+1}) \\ &\quad + (-1)^{n+1} (f+g)(\sigma_1, \dots, \sigma_n) \\ &= \sigma_1 f(\sigma_2, \dots, \sigma_{n+1}) + \sigma_1 g(\sigma_2, \dots, \sigma_{n+1}) \\ &\quad + \sum_{i=1}^n (-1)^i f(\sigma_1, \dots, \sigma_i \sigma_{i+1}, \dots, \sigma_{n+1}) \\ &\quad + \sum_{i=1}^n (-1)^i g(\sigma_1, \dots, \sigma_i \sigma_{i+1}, \dots, \sigma_{n+1}) \\ &\quad + (-1)^{n+1} f(\sigma_1, \dots, \sigma_n) + (-1)^{n+1} g(\sigma_1, \dots, \sigma_n) \\ &= \left\{ \sigma_1 f(\sigma_2, \dots, \sigma_{n+1}) + \sum_{i=1}^n (-1)^i f(\sigma_1, \dots, \sigma_i \sigma_{i+1}, \dots, \sigma_{n+1}) \right. \\ &\quad \left. + (-1)^{n+1} f(\sigma_1, \dots, \sigma_n) \right\} + \left\{ \sigma_1 g(\sigma_2, \dots, \sigma_{n+1}) \right. \\ &\quad \left. + \sum_{i=1}^n (-1)^i g(\sigma_1, \dots, \sigma_i \sigma_{i+1}, \dots, \sigma_{n+1}) + (-1)^{n+1} g(\sigma_1, \dots, \sigma_n) \right\} \\ &= \delta_n(f)(\sigma) + \delta_n(g)(\sigma).\end{aligned}$$

(Here note that $C^n(G, M)$ is an abelian group).

□

Problem 10.2.

With notation as in the previous problem, show that $\delta_{n+1} \circ \delta_n$ is the zero map.

Proof.

(1) If $n = 0$, then

$$\begin{aligned} (\delta_1 \circ \delta_0)(f)(\sigma_1, \sigma_2) &= \delta_1(\delta_0(f))(\sigma_1, \sigma_2) \\ &= \sigma_1 \delta_0(f)(\sigma_2) - \delta_0(f)(\sigma_1 \sigma_2) + \delta_0(f)(\sigma_1) \\ &= \sigma_1(\sigma_2 f - f) - (\sigma_1 \sigma_2 f - f) + (\sigma_1 f - f) \\ &= 0. \end{aligned}$$

(2) If $n \geq 1$, then we write

$$\begin{aligned} &(\delta_{n+1} \circ \delta_n)(f)(\sigma_1, \dots, \sigma_{n+2}) \\ &= \delta_{n+1}(\delta_n(f))(\sigma_1, \dots, \sigma_{n+2}) \\ &= \underbrace{\sigma_1 \delta_n(f)(\sigma_2, \dots, \sigma_{n+2})}_{\text{Part (3)}} \\ &\quad + \underbrace{\sum_{j=1}^{n+1} (-1)^j \delta_n(f)(\sigma_1, \dots, \sigma_j \sigma_{j+1}, \dots, \sigma_{n+2})}_{\text{Parts (4)(5)(6)}} \\ &\quad + \underbrace{(-1)^{n+2} \delta_n(f)(\sigma_1, \dots, \sigma_{n+1})}_{\text{Part (7)}}. \end{aligned}$$

(3) The first term is

$$\begin{aligned} &\sigma_1 \delta_n(f)(\sigma_2, \dots, \sigma_{n+2}) \\ &= \sigma_1 \sigma_2 f(\sigma_3, \dots, \sigma_{n+2}) \\ &\quad + \sum_{i=1}^n (-1)^i \sigma_1 f(\sigma_2, \dots, \sigma_{i+1} \sigma_{i+2}, \dots, \sigma_{n+2}) \\ &\quad + (-1)^{n+1} \sigma_1 f(\sigma_2, \dots, \sigma_{n+1}). \end{aligned}$$

(4) The first term ($j = 1$) in the summation is

$$\begin{aligned} &(-1)^1 \delta_n(f)(\sigma_1 \sigma_2, \dots, \sigma_{n+2}) \\ &= -\sigma_1 \sigma_2 f(\sigma_3, \dots, \sigma_{n+2}) \\ &\quad + f(\sigma_1 \sigma_2 \sigma_3, \dots, \sigma_{n+2}) - \sum_{i=2}^n (-1)^i f(\sigma_1 \sigma_2, \dots, \sigma_{i+1} \sigma_{i+2}, \dots, \sigma_{n+2}) \\ &\quad - (-1)^{n+1} f(\sigma_1 \sigma_2, \dots, \sigma_{n+1}) \end{aligned}$$

(5) The j th term for $2 \leq j \leq n$ in the summation is

$$\begin{aligned}
& (-1)^j \delta_n(f)(\sigma_1, \dots, \sigma_j \sigma_{j+1}, \dots, \sigma_{n+2}) \\
&= (-1)^j \sigma_1 f(\sigma_2, \dots, \sigma_j \sigma_{j+1}, \dots, \sigma_{n+2}) \\
&\quad + (-1)^j \sum_{i=1}^{j-2} (-1)^i f(\sigma_1, \dots, \sigma_i \sigma_{i+1}, \dots, \sigma_j \sigma_{j+1}, \dots, \sigma_{n+2}) \\
&\quad + (-1)^j (-1)^{j-1} f(\sigma_1, \dots, \sigma_{j-1} \sigma_j \sigma_{j+1}, \dots, \sigma_{n+2}) \\
&\quad + (-1)^j (-1)^j f(\sigma_1, \dots, \sigma_j \sigma_{j+1} \sigma_{j+2}, \dots, \sigma_{n+2}) \\
&\quad + (-1)^j \sum_{i=j+1}^n (-1)^i f(\sigma_1, \dots, \sigma_j \sigma_{j+1}, \dots, \sigma_{i+1} \sigma_{i+2}, \dots, \sigma_{n+2}) \\
&\quad + (-1)^j (-1)^{n+1} f(\sigma_1, \dots, \sigma_j \sigma_{j+1}, \dots, \sigma_{n+1}).
\end{aligned}$$

(6) The last term ($j = n + 1$) in the summation is

$$\begin{aligned}
& (-1)^{n+1} \delta_n(f)(\sigma_1, \dots, \sigma_n, \sigma_{n+1} \sigma_{n+2}) \\
&= (-1)^{n+1} \sigma_1 f(\sigma_2, \dots, \sigma_{n+1} \sigma_{n+2}) \\
&\quad + (-1)^{n+1} \sum_{i=1}^{n-1} (-1)^i f(\sigma_1, \dots, \sigma_i \sigma_{i+1}, \dots, \sigma_{n+1} \sigma_{n+2}) \\
&\quad + (-1)^{n+1} (-1)^n f(\sigma_1, \dots, \sigma_n \sigma_{n+1} \sigma_{n+2}) \\
&\quad + (-1)^{n+1} (-1)^{n+1} f(\sigma_1, \dots, \sigma_n).
\end{aligned}$$

(7) The last term is

$$\begin{aligned}
& (-1)^{n+2} \delta_n(f)(\sigma_1, \dots, \sigma_{n+1}) \\
&= (-1)^{n+2} \sigma_1 f(\sigma_2, \dots, \sigma_{n+1}) \\
&\quad + (-1)^{n+2} \sum_{i=1}^n (-1)^i f(\sigma_1, \dots, \sigma_i \sigma_{i+1}, \dots, \sigma_{n+1}) \\
&\quad + (-1)^{n+2} (-1)^{n+1} f(\sigma_1, \dots, \sigma_n).
\end{aligned}$$

(8) Hence we have $(\delta_{n+1} \circ \delta_n)(f)(\sigma_1, \dots, \sigma_{n+2}) = 0$.

□

Supplement.

- (1) (Theorem 10.20 in the textbook: *Rudin, Principles of Mathematical Analysis*, 3rd edition.) If ω is a k -form of class \mathcal{C}'' in some open set $E \subseteq \mathbb{R}^n$, then $d^2\omega = 0$.

- (2) (Exercise 10.16 in the textbook: Rudin, *Principles of Mathematical Analysis*, 3rd edition.) If $k \geq 2$ and $\sigma = [\mathbf{p}_0, \mathbf{p}_1, \dots, \mathbf{p}_k]$ is an oriented affine k -simplex, prove that $\partial^2 \sigma = 0$, directly from the definition of the boundary operator ∂ . Deduce from this that $\partial^2 \Psi = 0$ for every chain Ψ .

Problem 10.3.

Let M be a G -module, and let $f \in Z^2(G, M)$. Show that $f(1, 1) = f(1, \sigma) = \sigma^{-1}f(\sigma, 1)$ for all $\sigma \in G$.

Proof.

- (1) $f \in Z^2(G, M)$ if and only if $\delta_2(f) = 0$. So

$$\begin{aligned} \delta_2(f)(\sigma_1, \sigma_2, \sigma_3) &= \sigma_1 f(\sigma_2, \sigma_3) - f(\sigma_1 \sigma_2, \sigma_3) + f(\sigma_1, \sigma_2 \sigma_3) - f(\sigma_1, \sigma_2) \\ &= 0. \end{aligned}$$

for any $\sigma_1 \sigma_2, \sigma_3 \in G$.

- (2) Take $\sigma_1 = \sigma_2 = 1$ and $\sigma_3 = \sigma$ to get

$$f(1, \sigma) - f(1, \sigma) + f(1, \sigma) - f(1, 1) = 0.$$

So $f(1, 1) = f(1, \sigma)$.

- (3) Take $\sigma_1 = \sigma$ and $\sigma_2 = \sigma_3 = 1$ to get

$$\sigma f(1, 1) - f(\sigma, 1) + f(\sigma, 1) - f(\sigma, 1) = 0.$$

So $\sigma f(1, 1) = f(\sigma, 1)$ or $f(1, 1) = \sigma^{-1}f(\sigma, 1)$.

□

Problem 10.4.

If E is a group with an abelian normal subgroup M , and if $G = E/M$, show that the action of G on M given by $\sigma m = eme^{-1}$ if $eM = \sigma$ is well-defined and makes M into a G -module.

Proof.

- (1) Show that $G \times M \rightarrow M$ defined by $\sigma m = eme^{-1}$ is independent of the choice of the coset representation of $\sigma = eM$. Suppose $\sigma = e_1 M = e_2 M$. $e_2 = e_1 m_1$ for some $m_1 \in M$.

(2) Therefore

$$e_2 m e_2^{-1} = (e_1 m_1) m (e_1 m_1)^{-1} = e_1 m_1 m m_1^{-1} e_1^{-1} = e_1 m e_1^{-1}.$$

Here $(e_1 m_1)^{-1} = m_1^{-1} e_1^{-1}$ holds in a group E and $m_1 m m_1^{-1} = m$ since M is an abelian group.

(3) Show that M is a G -module where $G \times M \rightarrow M$ is defined by $\sigma m = e m e^{-1}$.

(a) Show that $1m = m$. $1m = 1m1^{-1} = m$ where $1 = 1M \in G = E/M$.

(b) Show that $\sigma(\tau m) = (\sigma\tau)m$. Write $\sigma = e_\sigma M$ and $\tau = e_\tau M$. Hence $\sigma\tau = e_\sigma e_\tau M$ and

$$\begin{aligned} \sigma(\tau m) &= \sigma(e_\tau m e_\tau^{-1}) \\ &= e_\sigma (e_\tau m e_\tau^{-1}) e_\sigma^{-1} \\ &= (e_\sigma e_\tau) m (e_\sigma e_\tau)^{-1} \\ &= (\sigma\tau)m. \end{aligned}$$

(c) Show that $\sigma(m_1 + m_2) = \sigma m_1 + \sigma m_2$.

$$\begin{aligned} \sigma(m_1 + m_2) &= e(m_1 + m_2)e^{-1} \\ &= e m_1 e^{-1} + e m_2 e^{-1} \\ &= \sigma m_1 + \sigma m_2 \end{aligned}$$

where $\sigma = eM$ for some $e \in E$.

□

Problem 10.5.

With E , M , G as in the previous problem, if e_σ is a coset representative of σ , show that the function defined by $f(\sigma, \tau) = e_\sigma e_\tau e_{\sigma\tau}^{-1}$ is a 2-cocycle.

Proof. It suffices to show that $\delta_2(f)(\sigma, \tau, v) = 0$ for any $\sigma, \tau, v \in G$. That is,

$$\begin{aligned} &\delta_2(f)(\sigma, \tau, v) \\ &= \sigma f(\tau, v) f(\sigma\tau, v)^{-1} f(\sigma, \tau v) f(\sigma, \tau)^{-1} \\ &= \sigma f(\tau, v) f(\sigma, \tau v) f(\sigma\tau, v)^{-1} f(\sigma, \tau)^{-1} \quad (M: \text{abelian}) \\ &= \sigma (e_\tau e_v e_{\tau v}^{-1}) (e_\sigma e_{\tau v} e_{\sigma\tau v}^{-1}) (e_{\sigma\tau} e_v e_{\sigma\tau v}^{-1})^{-1} (e_\sigma e_\tau e_{\sigma\tau}^{-1})^{-1} \\ &= (e_\sigma e_\tau e_v e_{\tau v}^{-1} e_\sigma^{-1}) (e_\sigma e_{\tau v} e_{\sigma\tau v}^{-1}) (e_{\sigma\tau v} e_v^{-1} e_{\sigma\tau}^{-1}) (e_{\sigma\tau} e_\tau^{-1} e_\sigma^{-1}) \\ &= 1. \end{aligned}$$

□

Problem 10.6.

Suppose that M is a G -module. For each $\sigma \in G$, let $m_\sigma \in M$. Show that the cochain f defined by $f(\sigma, \tau) = m_\sigma + \sigma m_\tau - m_{\sigma\tau}$ is a coboundary.

Proof.

- (1) To show f is a 2-coboundary, it suffices to show that there is a $g \in C^1(G, M)$ such that $f = \delta_1(g)$.
- (2) Actually, we can define $g : G \rightarrow M$ by $\sigma \mapsto m_\sigma$. So

$$\delta_1(g)(\sigma, \tau) = \sigma g(\tau) - g(\sigma\tau) + g(\sigma) = \sigma m_\tau - m_{\sigma\tau} + m_\sigma = f(\sigma, \tau)$$

for all $\sigma, \tau \in G$. Hence $f \in B^2(G, M)$.

□

Problem 10.7.

If M is a G -module and $f \in Z^2(G, M)$, show that $E_f = M \times G$ with multiplication defined by

$$(m, \sigma)(n, \tau) = (m \cdot \sigma n \cdot f(\sigma, \tau), \sigma\tau)$$

makes E_f into a group.

Proof.

- (1) The multiplication is a binary operation on E_f .
- (2) (Associativity) Show that

$$((m, \sigma)(n, \tau))(k, v) = (m, \sigma)((n, \tau)(k, v)).$$

for all $(m, \sigma), (n, \tau), (k, v)$. Note that

$$\begin{aligned} ((m, \sigma)(n, \tau))(k, v) &= (m \cdot \sigma n \cdot f(\sigma, \tau), \sigma\tau)(k, v) \\ &= (m \cdot \sigma n \cdot f(\sigma, \tau) \cdot \sigma\tau k \cdot f(\sigma\tau, v), \sigma\tau v) \\ &= (m \cdot \sigma n \cdot \sigma\tau k \cdot f(\sigma, \tau) \cdot f(\sigma\tau, v), \sigma\tau v) \end{aligned}$$

and

$$\begin{aligned} (m, \sigma)((n, \tau)(k, v)) &= (m, \sigma)(n \cdot \tau k \cdot f(\tau, v), \tau v) \\ &= (m \cdot \sigma(n \cdot \tau k \cdot f(\tau, v)) \cdot f(\sigma, \tau v), \sigma\tau v) \\ &= (m \cdot \sigma n \cdot \sigma\tau k \cdot \underbrace{\sigma f(\tau, v) \cdot f(\sigma, \tau v)}_{=f(\sigma, \tau) \cdot f(\sigma\tau, v)}, \sigma\tau v) \end{aligned}$$

(since $f \in Z^2(G, M)$).

- (3) (Identity element) *Show that there exists an element*

$$1 := (f(1, 1)^{-1}, 1) \in E_f$$

such that $1(m, \sigma) = (m, \sigma)1 = (m, \sigma)$ for every $(m, \sigma) \in E_f$. Same as Problem 10.3. Note that

$$\begin{aligned} (m, \sigma)(f(1, 1)^{-1}, 1) &= (m \cdot \underbrace{\sigma f(1, 1)^{-1}}_{=\sigma^{-1}f(\sigma, 1)^{-1}} \cdot f(\sigma, 1), \sigma) \\ &= (m \cdot \sigma(\sigma^{-1}f(\sigma, 1)^{-1}) \cdot f(\sigma, 1), \sigma) \\ &= (m \cdot (\sigma\sigma^{-1})f(\sigma, 1)^{-1} \cdot f(\sigma, 1), \sigma) \\ &= (m, \sigma) \end{aligned}$$

and

$$\begin{aligned} (f(1, 1)^{-1}, 1)(m, \sigma) &= (f(1, 1)^{-1} \cdot m \cdot f(1, \sigma), \sigma) \\ &= (f(1, \sigma)^{-1} \cdot m \cdot f(1, \sigma), \sigma) \\ &= (m, \sigma). \end{aligned}$$

- (4) *Note.* To find the identity element, we need to find (n, τ) such that $(m, \sigma)(n, \tau) = (m, \sigma)$. So

$$(m, \sigma)(n, \tau) = (m \cdot \sigma n \cdot f(\sigma, \tau), \sigma\tau) = (m, \sigma)$$

implies that $\tau = 1 \in G$ and thus $m \cdot \sigma n \cdot f(\sigma, 1) = m$. Hence

$$n = \sigma^{-1}f(\sigma, 1)^{-1} = (\sigma^{-1}f(\sigma, 1))^{-1} = f(1, 1)^{-1}$$

(in the multiplicative notation).

- (5) (Inverse element) *Show that for each $(m, \sigma) \in E_f$, there exists an element*

$$(n, \tau) := (\sigma^{-1} \{f(\sigma, \sigma^{-1})^{-1} \cdot m^{-1} \cdot f(1, 1)^{-1}\}, \sigma^{-1}) \in E_f$$

such that $(m, \sigma)(n, \tau) = (n, \tau)(m, \sigma) = 1$, where 1 is the identity element in E_f . (To find the inverse element, we might apply the same argument in part (4).) A direct calculation with the fact that $f \in Z^2(G, M)$ gives

$$\begin{aligned} &(m, \sigma) (\sigma^{-1} \{f(\sigma, \sigma^{-1})^{-1} \cdot m^{-1} \cdot f(1, 1)^{-1}\}, \sigma^{-1}) \\ &= (m \cdot \sigma (\sigma^{-1} \{f(\sigma, \sigma^{-1})^{-1} \cdot m^{-1} \cdot f(1, 1)^{-1}\}) \cdot f(\sigma, \sigma^{-1}), 1) \\ &= (m \cdot f(\sigma, \sigma^{-1})^{-1} \cdot m^{-1} \cdot f(1, 1)^{-1} \cdot f(\sigma, \sigma^{-1}), 1) \\ &= (f(1, 1)^{-1}, 1) \end{aligned}$$

and

$$\begin{aligned}
& (\sigma^{-1} \{f(\sigma, \sigma^{-1})^{-1} \cdot m^{-1} \cdot f(1, 1)^{-1}\}, \sigma^{-1}) (m, \sigma) \\
&= (\sigma^{-1} \{f(\sigma, \sigma^{-1})^{-1} \cdot m^{-1} \cdot f(1, 1)^{-1}\} \cdot \sigma^{-1} m \cdot f(\sigma^{-1}, \sigma), 1) \\
&= (\sigma^{-1} f(\sigma, \sigma^{-1})^{-1} \cdot f(\sigma^{-1}, \sigma) \cdot \sigma^{-1} f(1, 1)^{-1}, 1) \\
&= (f(1, 1)^{-1} \cdot \underbrace{\sigma^{-1} f(1, 1) \cdot \sigma^{-1} f(1, 1)^{-1}}_{=1}, 1) \\
&= (f(1, 1)^{-1}, 1).
\end{aligned}$$

Here we take $(\sigma_1, \sigma_2, \sigma_3) \mapsto (\sigma^{-1}, \sigma, \sigma^{-1})$ in part (1) of the proof of Problem 10.3 to get

$$\begin{aligned}
\sigma^{-1} f(\sigma, \sigma^{-1})^{-1} \cdot f(\sigma^{-1}, \sigma) &= f(1, \sigma^{-1})^{-1} \cdot f(\sigma^{-1}, 1) \\
&= f(1, 1)^{-1} \cdot \sigma^{-1} f(1, 1).
\end{aligned}$$

□