

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

Meng-Gen Tsai  
 plover@gmail.com

July 21, 2021

## Contents

<b>Chapter I: Galois Theory</b>	<b>2</b>
§I.1: Field Extensions . . . . .	2
Problem I.1.1. . . . .	2
Problem I.1.2. . . . .	2
Problem I.1.3. . . . .	3
Problem I.1.4. . . . .	3
Problem I.1.5. . . . .	4
Problem I.1.9. . . . .	5
Problem I.1.11. . . . .	5
Problem I.1.12. . . . .	6
Problem I.1.16. . . . .	6
Problem I.1.23. . . . .	7
Problem I.1.24. . . . .	7
Problem I.1.25. . . . .	8
§I.2: Automorphisms . . . . .	8
Problem I.2.1. . . . .	8
Problem I.2.2. . . . .	9
Problem I.2.4. . . . .	9

# Chapter I: Galois Theory

## §I.1: Field Extensions

### Problem I.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 I.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 I.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 I.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 I.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 I.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 I.1.2,  $L = K$  or  $L = F$ , or there are no intermediate fields between  $K$  and  $F$ .  $\square$

**Problem I.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  $\alpha'$  is the inverse of  $\alpha$  in  $R$ .

$\square$

**Problem I.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  $\varphi$  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  $\varphi$ , 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  $\varphi$  is well-defined, linear, injective and surjective.

□

**Problem I.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 I.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  $\varphi$  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)  $\varphi$  is a ring homomorphism.

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

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

(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 I.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 I.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.

□

## §I.2: Automorphisms

**Problem I.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  $\sigma$ , 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  $\sigma$ ,  $\sigma(-n) = -\sigma(n) = -n$  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  $\sigma$  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  $\sigma$  is the identity.  $\square$

### Problem I.2.2.

*Show that the only automorphism of  $\mathbb{R}$  is the identity. (Hint: If  $\sigma$  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 I.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  $\sigma$  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  $\sigma$  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  $\sigma$  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 I.2.4.

*Let  $B$  be an integral domain with quotient field  $F$ . If  $\sigma : B \rightarrow B$  is a ring automorphism, show that  $\sigma$  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  $\sigma'$  is well-defined.

- (a)  $\sigma' : F \rightarrow F$  is defined.  $\sigma(a), \sigma(b) \in B$  since  $\sigma$  is a homomorphism.  
 $\sigma(b) \neq 0$  since  $b \neq 0$  and  $\sigma$  is a one-on-one homomorphism.
- (b)  $\sigma'$  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  $\sigma'$  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  $\sigma'$  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  $\sigma'$  is a surjective. Given any  $c/d \in F$ , want to show there is  $a/b \in F$  such that  $\sigma'(a/b) = c/d$ .

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