

§48 Field Extensions

We recall a technical term from Example 39.2(f).

48.1 Definition: Let E be a field and let K be a nonempty subset of E . If K itself is a field under the operations defined on E , then K is called a *subfield of E* . In this case, E is called an *extension field of K* , or simply an *extension of K* .

We write E/K to denote that E is an extension of K , and speak of the field extension E/K . Confusion with a factor group or a factor space is not likely. We will frequently employ Hasse diagrams (see §21) for field extensions. For example, the picture



will mean that K is a subfield of E .

As in the case of subgroups, subrings and subspaces, we have a subfield criterion.

48.2 Lemma (Subfield criterion): *Let E be a field and K a nonempty subset of E . Then K is a subfield of E if and only if*

- (i) $a + b \in K$,
- (ii) $-b \in K$,
- (iii) $ab \in K$,
- (iv) $b^{-1} \in K$ (in case $b \neq 0$)

for all $a, b \in K$.

Proof: A field is a ring in which the nonzero elements form a commutative group under multiplication (see the remarks after Definition 29.13). Thus E is a ring of this type, and K is a subfield of E if and only if K is a

subring of E such that the nonzero elements in K form a commutative group under multiplication. Certainly, every subgroup of $E^\times = E \setminus \{0\}$ is commutative. Thus K is a subfield of E if and only if K is a subring of E and $K \setminus \{0\}$ is a subgroup of E^\times . Now K is a subring of E if and only if (i),(ii),(iii) hold and $K \setminus \{0\}$ is a subgroup of E^\times if and only if

$$(iii)' \quad ab \in K \setminus \{0\} \text{ for all } a, b \in K \setminus \{0\}$$

and (iv) hold. Since $K \subseteq E$ and the field E has no zero divisors, (iii)' is weaker than (iii), and we conclude that K is a subfield of E if and only if (i),(ii),(iii),(iv) hold. \square

From now on, we will write $\frac{1}{b}$ (or $1/b$) for the inverse b^{-1} of a nonzero element in a field. Likewise, we will write $\frac{a}{b}$ or (a/b) for the product $ab^{-1} = b^{-1}a$ of two elements a, b^{-1} in a field (assuming $b \neq 0$). It follows from Lemma 48.2 that, whenever K is a subfield of E and $a, b \in K$, then

$$a + b, a - b, ab, \frac{a}{b}$$

belong to K , it being assumed $b \neq 0$ in the last case. A subfield of E is therefore a nonempty subset of E that is closed under addition, subtraction, multiplication and division (by nonzero elements).

48.3 Examples: (a) \mathbb{R} is an extension of \mathbb{Q} , and \mathbb{C} is an extension of \mathbb{Q} . Also \mathbb{R} is a subfield of \mathbb{C} .

(b) If K is any field and x an indeterminate over K , then K is a subfield of $K(x)$ (provided we identify, as usual, an element a of K with the rational function $\frac{a}{1}$, where the numerator and denominator are elements of $K \subseteq K[x]$). Similarly K is a subfield of $K(x, y)$, where y is another indeterminate over K .

(c) Let $\mathbb{Q}(i) := \{x + yi \in \mathbb{C} : x, y \in \mathbb{Q}\} \subseteq \mathbb{C}$. For any a, b in $\mathbb{Q}(i)$, say $a = x + yi$ and $b = z + ui$ with $x, y, z, u \in \mathbb{Q}$, we have

- (i) $a + b = (x + z) + (y + u)i \in \mathbb{Q}(i)$,
- (ii) $-b = (-z) + (-u)i \in \mathbb{Q}(i)$,

$$(iii) ab = (xz - yu) + (xu + yz)i \in \mathbb{Q}(i),$$

$$(iv) b^{-1} = \frac{z}{z^2 + u^2} + \frac{-u}{z^2 + u^2} i \in \mathbb{Q}(i), \text{ provided } b = z + ui \neq$$

$$0 + 0i = 0.$$

So $\mathbb{Q}(i)$ is a subfield of \mathbb{C} . It is in fact the field of fractions of $\mathbb{Z}[i]$, and is called the *gaussian field*.

(d) $\mathbb{Q}(\sqrt{2}) := \{x + y\sqrt{2} \in \mathbb{R} : x, y \in \mathbb{Q}\}$ is a subfield of \mathbb{R} . Indeed, for any a, b in $\mathbb{Q}(i)$, say $a = x + y\sqrt{2}$ and $b = z + u\sqrt{2}$ with $x, y, z, u \in \mathbb{Q}$, we have

$$(i) a + b = (x + z) + (y + u)\sqrt{2} \in \mathbb{Q}(\sqrt{2}),$$

$$(ii) -b = (-z) + (-u)\sqrt{2} \in \mathbb{Q}(\sqrt{2}),$$

$$(iii) ab = (xz + 2yu) + (xu + yz)\sqrt{2} \in \mathbb{Q}(\sqrt{2}),$$

$$(iv) b^{-1} = \frac{z}{z^2 - 2u^2} + \frac{-u}{z^2 - 2u^2} \sqrt{2} \in \mathbb{Q}(\sqrt{2}), \text{ provided } b =$$

$z + u\sqrt{2} \neq 0 + 0\sqrt{2} = 0$. Here we use the fact that $\sqrt{2} \in \mathbb{R}$ is an irrational number (Example 35.11) so that $z^2 - 2u^2 \neq 0$ if z and u are nonzero rational numbers.

(e) Let $L = \{x + y\sqrt[3]{2} \in \mathbb{R} : x, y \in \mathbb{Q}\} \subseteq \mathbb{R}$. Then L is not a subfield of \mathbb{R} since, for example $\sqrt[3]{2} \in L$ but $\sqrt[3]{2} \cdot \sqrt[3]{2} \notin L$ (why?) On the other hand,

$$\mathbb{Q}(\sqrt[3]{2}) := \{x + y\sqrt[3]{2} + z\sqrt[3]{4} \in \mathbb{R} : x, y, z \in \mathbb{Q}\} = \{x + y\sqrt[3]{2} + z(\sqrt[3]{2})^2 \in \mathbb{R} : x, y, z \in \mathbb{Q}\}$$

is a subfield of \mathbb{R} . The proof of $b \in \mathbb{Q}(\sqrt[3]{2}) \setminus \{0\} \implies 1/b \in \mathbb{Q}(\sqrt[3]{2})$ is left to the reader.

(f) Let K be a field and let K_i ($i \in I$) be a family of subfields of K . Then $\bigcap_{i \in I} K_i$ is a subfield of K , for the closure properties in Lemma 48.2 hold for $\bigcap_{i \in I} K_i$ if they hold for each of the K_i .

From the last example, we infer that the intersection of *all* subfields of a field K is a subfield of K . Note that the intersection is taken over a nonempty set, since at least K is a subfield of K .

48.4 Definition: Let K be a field. The intersection of all subfields of K is called the *prime subfield of K* .

Thus every subfield of K contains (is an extension of) the prime subfield of K . We want to describe the elements in the prime subfield of K . Let P denote the prime subfield of K . In order to distinguish clearly between the integer $1 \in \mathbb{Z}$ and the identity element of K , we will denote in this discussion the identity element of K as e . We know $0 \in P$, $e \in P$ and $0 \neq e$ because P is a field. Now P is a group under addition, so $e + e = 2e$, $2e + e = 3e$, $3e + e = 4e$, ... are elements of P , and also $-e$, $-2e$, $-3e$, $-4e$,

Hence $\dots, -4e, -3e, -2e, -e, 0, e, 2e, 3e, 4e, \dots$

all belong to P : we have $\{me \in K: m \in \mathbb{Z}\} \subseteq P$. Moreover, P is closed under division (by nonzero elements), and so $P_0 := \{me/ne \in K: m, n \in \mathbb{Z}\}$ is a subset of P . It is natural to expect that P_0 is a subfield of K (and thus $P_0 = P$): for any $me/ne, re/se \in P_0$ with $m, n, r, s \in \mathbb{Z}$, we presumably have

- (i) $\frac{me}{ne} + \frac{re}{se} = \frac{(ms + rn)e}{(ns)e} \in P_0$,
- (ii) $-\frac{re}{se} = \frac{(-r)e}{se} \in P_0$,
- (iii) $\frac{me}{ne} \frac{re}{se} = \frac{(mr)e}{(ns)e} \in P_0$,
- (iv) $\frac{1}{\frac{re}{se}} = \frac{se}{re} \in P_0$, provided $\frac{re}{se} \neq 0$, i.e., $re \neq 0$.

These are in fact true, but care must be exercised in justifying (i),(ii),(iii), (iv). This is done in the next theorem which states that P is isomorphic either to \mathbb{Q} or to \mathbb{Z}_p for some prime number p .

48.5 Theorem: *The prime subfield of any field K is isomorphic to \mathbb{Q} or to \mathbb{Z}_p for some prime number p (ring isomorphism).*

Proof: Let e be the identity of K and let P be the prime subfield of K . Then $1e = e \neq 0 \neq -e = -1e$. We distinguish two cases, according as there does or does not exist an integer $n \in \mathbb{Z} \setminus \{0\}$ satisfying $ne = 0$.

Case 1. Assume there is a nonzero integer n such that $ne = 0$. Then there are natural numbers k with $ke = 0$. Let p be the smallest natural number such that $pe = 0$. We claim that the mapping

$$\begin{aligned} \varphi: \mathbb{Z} &\rightarrow P \\ n &\rightarrow ne \end{aligned}$$

is a ring homomorphism, that p is a prime number and that $P \cong \mathbb{Z}_p$.

For any $m, n \in \mathbb{Z}$, we have $(m + n)\varphi = (m + n)e = me + ne$ (this is not distributivity!) and $(mn)\varphi = (mn)e = (me)(ne) = m\varphi \cdot n\varphi$ (here $(mn)e = (me)(ne)$ is distributivity!), so φ is a ring homomorphism.

If p were composite, say $p = rs$ with $r, s \in \mathbb{N}$, $1 < r < p$, $1 < s < p$, then $0 = pe = (rs)e = (re)(se)$ would yield, since the field K has no zero divisors, that $re = 0$ or $se = 0$, contradicting the definition of p as the *smallest* natural number satisfying $pe = 0$. So p is a prime number.

To prove $P \cong \mathbb{Z}_p$, we will find $\text{Ker } \varphi$. From $pe = 0$, we have $p \in \text{Ker } \varphi$, so $pn \in \text{Ker } \varphi$ for all $n \in \mathbb{Z}$ (because $\text{Ker } \varphi$ is an ideal of \mathbb{Z}) and $p\mathbb{Z} \subseteq \text{Ker } \varphi$. On the other hand, if $m \in \text{Ker } \varphi$, we divide m by p to get $m = qp + r$, with $q, r \in \mathbb{Z}$ and $0 \leq r < p$. This gives $0 = me = (qp + r)e = (qp)e + re = 0 + re$. As $0 \leq r < p$, this forces $r = 0$, which means $m = qp$ and $m \in p\mathbb{Z}$. So we get $\text{Ker } \varphi \subseteq p\mathbb{Z}$. Therefore $\text{Ker } \varphi = p\mathbb{Z}$. [A more conceptual argument: $\text{Ker } \varphi$ is an ideal of \mathbb{Z} and \mathbb{Z} is a principal ideal domain, so $\text{Ker } \varphi = d\mathbb{Z}$ for some $d \in \mathbb{Z}$. We have $d \neq 0$ in Case 1. From $pe = 0$ we get $p \in \text{Ker } \varphi = d\mathbb{Z}$, so $d|p$. But p is a prime number, so $d = \mp 1$ or $d = \mp p$. The possibility $d = \mp 1$ is excluded, because $\mp 1e = \mp e \neq 0$. Hence $d = \mp p$ and $\text{Ker } \varphi = d\mathbb{Z} = \mp p\mathbb{Z} = p\mathbb{Z}$.]

Thus $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z} = \mathbb{Z}/\text{Ker } \varphi \cong \text{Im } \varphi \subseteq P$ and $\text{Im } \varphi$, being a ring isomorphic to \mathbb{Z}_p , is a field. So $\text{Im } \varphi$ is a subfield of K , therefore $P \subseteq \text{Im } \varphi$. This yields $P = \text{Im } \varphi$ and $\mathbb{Z}_p \cong P$, as claimed.

Case 2. Assume there is no nonzero integer n such that $ne = 0$. We claim that the mapping

$$\begin{aligned} \psi: \mathbb{Q} &\rightarrow P \\ m/n &\rightarrow me/ne \end{aligned}$$

is a ring homomorphism and that $P \cong \mathbb{Q}$.

First we show that ψ is well defined. If $\frac{m}{n} = \frac{m'}{n'} \in \mathbb{Q}$ with $m, n, m', n' \in \mathbb{Z}$ ($n \neq 0 \neq n'$), then $mn' = m'n$ in \mathbb{Z} , so $(mn')e = (m'n)e$ in P , thus $(me)(n'e) = (m'e)(ne)$ in P . Multiplying both sides of this equation by $\frac{1}{ne} \frac{1}{n'e} \in P$, we obtain $\frac{me}{ne} = \frac{m'e}{n'e}$. So ψ is well defined.

ψ is a ring homomorphism: for all $\frac{m}{n}, \frac{r}{s} \in \mathbb{Q}$ with $m, n, r, s \in \mathbb{Z}$, $n \neq 0 \neq s$,

$$\text{we have } \left(\frac{m}{n} + \frac{r}{s}\right)\psi = \left(\frac{ms + rn}{ns}\right)\psi = \frac{(ms + rn)e}{(ns)e} = \frac{(ms)e + (rn)e}{ne \cdot se}$$

$$= \frac{(me)(se) + (re)(ne)}{ne \cdot se} = \frac{me}{ne} + \frac{re}{se} = \frac{m}{n} \psi + \frac{r}{s} \psi$$

$$\text{and } \left(\frac{m}{n} \frac{r}{s} \right) \psi = \frac{mr}{ns} \psi = \frac{(mr)e}{(ns)e} = \frac{(me)(re)}{(ne)(se)} = \frac{me}{ne} \frac{re}{se} = \frac{m}{n} \psi \frac{r}{s} \psi$$

Since we assume that $me \neq 0$ for $m \in \mathbb{Z} \setminus \{0\}$ in Case 2, we obtain $\text{Ker } \psi = \left\{ \frac{m}{n} \in \mathbb{Q} : \frac{me}{ne} = 0 \in K \right\} = \left\{ \frac{m}{n} \in \mathbb{Q} : me = 0 \in K \right\} = \left\{ \frac{m}{n} \in \mathbb{Q} : m = 0 \in \mathbb{Z} \right\} = \{0\}$, so $\mathbb{Q} \cong \mathbb{Q}/\{0\} = \mathbb{Q}/\text{Ker } \psi \cong \text{Im } \psi \subseteq P$ and $\text{Im } \psi$, being a ring isomorphic to \mathbb{Q} , is a field. So $\text{Im } \psi$ is a subfield of K , therefore $P \subseteq \text{Im } \psi$. This yields $P = \text{Im } \psi$ and $\mathbb{Q} \cong P$, as claimed. \square

48.6 Definition: Let K be a field and let e be the identity element of K . If there are nonzero integers n such that $ne = 0$, and if p is the smallest natural number such that $pe = 0$, then K is said to be a *field of characteristic p* and p is called the *characteristic of K* . If there is no nonzero integer n such that $ne = 0$, then K is said to be a *field of characteristic 0*, and 0 is called the *characteristic of K* .

Equivalently, K is of characteristic p or 0 according as its prime subfield is isomorphic to \mathbb{Z}_p or to \mathbb{Q} . We write $\text{char } K = p$ and $\text{char } K = 0$ in these respective cases. For example, $\text{char } \mathbb{Z}_p = p$ and $\text{char } \mathbb{Q}(i) = \text{char } \mathbb{Q}(\sqrt{2}) = \text{char } \mathbb{R} = \text{char } \mathbb{C} = 0$. We will usually identify \mathbb{Z}_p or \mathbb{Q} with the prime subfield of K , as the case may be. In particular, we will write 1 instead of e for the identity element of K . Thus K will be considered to be an extension of \mathbb{Z}_p or \mathbb{Q} .

We remark that, if K is a field of characteristic p , then $pa = 0$ for any element a of K . This follows from

$pa = a + a + \cdots + a = 1a + 1a + \cdots + 1a = (1 + 1 + \cdots + 1)a = (p1)a = 0a = 0$, the sums having p terms. This result will be used in the sequel without explicit mention.

We make two conventions. Henceforward, we will write \mathbb{F}_p in place of \mathbb{Z}_p . This will always remind us that \mathbb{F}_p is a field (p prime). Secondly, we shall drop the bars in the elements of \mathbb{F}_p , as we have already done on several

occasions. For example, we will write 2 instead of $\bar{2} \in \mathbb{F}_5$. A notation such as "2" is therefore ambiguous: it stands for the integer $2 \in \mathbb{Z}$, as well as $\bar{2} \in \mathbb{F}_2$, as well as $\bar{2} \in \mathbb{F}_3$, as well as $\bar{2} \in \mathbb{F}_5$, etc. It will be clear from the context, however, which meaning is accorded to "2". The ambiguity is therefore harmless.

We proceed to discuss field homomorphisms.

48.7 Lemma: *If K is a field, then K and $\{0\}$ are the only ideals of K .*

Proof: If A is an ideal of K and $A \neq \{0\}$, there is an $a \in A$, $a \neq 0$. Then a has an inverse $\frac{1}{a}$ in K and $\frac{1}{a}a = 1 \in A$, because A is an ideal. Then we get $b = b \cdot 1 \in A$ for all $b \in K$, so $K \subseteq A$ and $A = K$.

□

48.8 Lemma: *If K_1 and K_2 are fields and $\varphi: K_1 \rightarrow K_2$ is a ring homomorphism, then either $a\varphi = 0$ for all $a \in K_1$ or φ is one-to-one.*

Proof: $\text{Ker } \varphi$ is an ideal of K_1 , so either $\text{Ker } \varphi = K_1$ or $\text{Ker } \varphi = \{0\}$ by Lemma 48.7. In these respective cases, either $a\varphi = 0$ for all $a \in K_1$ or φ is one-to-one. □

When we deal with fields and ring homomorphisms from a field to another, we naturally want to disregard the uninteresting ring homomorphism that maps every element of its domain to the zero element of the other field. Any other ring homomorphism is one-to-one by Lemma 48.8. This leads us to the following definition.

48.9 Definition: If K_1 and K_2 are fields and $\varphi: K_1 \rightarrow K_2$ is a one-to-one ring homomorphism, then φ will be called a *field homomorphism*. If φ is a field homomorphism onto K_2 , then φ will be called a *field isomorphism*. A field isomorphism from K onto the same field K will be called a (*field*) *automorphism of K* .

If $\varphi: K_1 \rightarrow K_2$ is a field isomorphism, then φ is a homomorphism of additive groups, so $0_{K_1}\varphi = 0_{K_2}$, and also $\text{Ker } \varphi = \{0_{K_1}\}$, where 0_{K_1} and 0_{K_2} are the zero elements of the fields K_1, K_2 , respectively. Thus $\varphi_{K_1 \setminus \{0\}}$ is a one-to-one mapping from $K_1 \setminus \{0\}$ onto $K_2 \setminus \{0\}$. In addition, $(ab)\varphi = a\varphi \cdot b\varphi$ for all a, b in K_1 , so $(ab)\varphi = a\varphi \cdot b\varphi$ for all $a, b \in K_1 \setminus \{0\}$ and therefore $\varphi_{K_1^\times}: K_1^\times \rightarrow K_2^\times$ is a one-to-one homomorphism of groups onto K_2^\times : we have $K_1^\times \cong K_2^\times$. In particular, $(1_{K_1})\varphi = 1_{K_2}$, where 1_{K_1} and 1_{K_2} are the identities of the fields K_1, K_2 , respectively.

48.10 Lemma: *Let K_1, K_2, K_3 be fields.*

(1) *If $\varphi: K_1 \rightarrow K_2$ and $\psi: K_2 \rightarrow K_3$ are field homomorphisms, then $\varphi\psi: K_1 \rightarrow K_3$ is a field homomorphism.*

(2) *If $\varphi: K_1 \rightarrow K_2$ and $\psi: K_2 \rightarrow K_3$ are field isomorphisms, then $\varphi\psi: K_1 \rightarrow K_3$ is a field isomorphism.*

(3) *If $\varphi: K_1 \rightarrow K_2$ is a field isomorphism, then $\varphi^{-1}: K_2 \rightarrow K_1$ is a field isomorphism.*

Proof: (1) $\varphi\psi$ is a ring homomorphism by Lemma 30.16(1) and one-to-one by Theorem 3.11(2).

(2) $\varphi\psi$ is a field homomorphism by part (1) and onto by Theorem 3.11(1).

(3) φ^{-1} is a ring homomorphism by Lemma 30.16(2) and one-to-one by Theorem 3.17(1). □

A field homomorphism $\varphi: K_1 \rightarrow K_2$ can be characterized as a one-to-one function such that

$$(a + b)\varphi = a\varphi + b\varphi, \quad (a - b)\varphi = a\varphi - b\varphi, \quad (ab)\varphi = a\varphi \cdot b\varphi, \quad \frac{a}{b}\varphi = \frac{a\varphi}{b\varphi}$$

for all $a, b \in K_1$ ($b \neq 0$ in the division). Let us consider some examples.

48.11 Examples: (a) The conjugation mapping $\varphi: \mathbb{C} \rightarrow \mathbb{C}$ is an automorphism of \mathbb{C} , because

$$\begin{array}{l} x \rightarrow \bar{x} \\ \overline{x + y} = \bar{x} + \bar{y}, \quad \overline{x - y} = \bar{x} - \bar{y}, \quad \overline{xy} = \bar{x} \cdot \bar{y}, \quad \overline{x/y} = \bar{x}/\bar{y} \end{array}$$

for any $x, y \in \mathbb{C}$.

(b) The mapping $\varphi: \mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{Q}(\sqrt{2})$ is an automorphism of $\mathbb{Q}(\sqrt{2})$ because

$$a + b\sqrt{2} \rightarrow a - b\sqrt{2}$$

$$\begin{aligned} ((a + b\sqrt{2}) + (c + d\sqrt{2}))\varphi &= ((a + c) + (b + d)\sqrt{2})\varphi = (a + c) - (b + d)\sqrt{2} \\ &= (a - b\sqrt{2}) + (c - d\sqrt{2}) = (a + b\sqrt{2})\varphi + (c + d\sqrt{2})\varphi, \end{aligned}$$

$$\begin{aligned} ((a + b\sqrt{2})(c + d\sqrt{2}))\varphi &= ((ac + 2bd) + (ad + bc)\sqrt{2})\varphi \\ &= (ac + 2bd) - (ad + bc)\sqrt{2} = (ac + 2(-b)(-d)) + (a(-d) + (-b)c)\sqrt{2} \\ &= (a - b\sqrt{2})(c - d\sqrt{2}) = (a + b\sqrt{2})\varphi(c + d\sqrt{2})\varphi \end{aligned}$$

for all $a + b\sqrt{2}, c + d\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, where $a, b, c, d \in \mathbb{Q}$, so that φ is a ring homomorphism and, because of $1\varphi = (1 + 0\sqrt{2})\varphi = 1 - 0\sqrt{2} = 1 \neq 0$, the kernel of φ is not K and φ is therefore one-to-one.

(c) Let K be a field and x an indeterminate over K . Then the mapping

$$\begin{array}{l} \varphi: K(x) \rightarrow K(x) \\ \frac{p(x)}{q(x)} \rightarrow \frac{p(x^2)}{q(x^2)} \end{array}$$

is a field homomorphism. Note that $\text{Im } \varphi \subset K(x)$. Thus $K(x)$ is isomorphic to a proper subset of itself (namely to $\text{Im } \varphi$).

Let E/K be a field extension. Then E is an additive group and

$$\begin{aligned} a(x + y) &= ax + ay \\ (a + b)x &= ax + bx \\ (ab)x &= a(bx) \\ 1x &= x \end{aligned}$$

for all $x, y \in E$ and for all $a, b \in K$ (in fact for all $a, b \in E$, but we do not need this now). Hence E is a vector space over K , as we have already noted in Example 39.2(h). Studying both the field and the vector space structure of E will be very useful. In particular, the dimension of E over K will play an important role.

48.12 Definition: Let E/K be a field extension. The dimension of E over K is called the *degree of E over K* , or the *degree of the extension E/K* .

It will prove convenient to write $|E:K|$ instead of $\dim_K E$ for the degree of E over K . The field E is said to be a *finite dimensional extension* or an *infinite dimensional extension of K* according as $|E:K|$ is finite or infinite. Most authors use the term "finite extension" for a finite dimensional extension.

An important fact in the theory of fields is that a finite dimensional extension of a finite dimensional extension is a finite dimensional extension, and that the degrees behave multiplicatively. More exactly, we have the

48.13 Theorem: Let F/E and E/K be field extensions of finite degrees $|F:E|$ and $|E:K|$. Then F/K is a finite dimensional extension. In fact

$$|F:K| = |F:E| |E:K|$$

and furthermore if $\{f_1, f_2, \dots, f_r\}$ is an E -basis of F and $\{e_1, e_2, \dots, e_s\}$ a K -basis of E , then $\{f_i e_j : i = 1, 2, \dots, r; j = 1, 2, \dots, s\}$ is a K -basis of F .

Proof: If K is a subfield of E and E is a subfield of F , then certainly K is a subfield of F . Thus F is an extension of K .

Now the claim about the degree. Put $|F:E| = r$ and $|E:K| = s$ for brevity. We are to prove that the dimension of F over K is equal to rs . Let $\{f_1, f_2, \dots, f_r\}$ be an E -basis of F and $\{e_1, e_2, \dots, e_s\}$ a K -basis of E . We are to find a K -basis of F having exactly rs elements. The most natural thing to do is to consider the rs products $f_i e_j$. We contend that $\{f_i e_j : i = 1, 2, \dots, r; j = 1, 2, \dots, s\}$ is a K -basis of F .

First we show that $\{f_i e_j\}$ spans F over K . Indeed, let f be an arbitrary element of F . Then

$$f = b_1 f_1 + b_2 f_2 + \dots + b_r f_r$$

for some $b_1, b_2, \dots, b_r \in E$, because $\{f_i : i = 1, 2, \dots, r\}$ spans F over E ; and for each i ,

$$b_i = a_{i1} e_1 + a_{i2} e_2 + \dots + a_{is} e_s$$

for some $a_{i1}, a_{i2}, \dots, a_{is} \in K$, because $\{e_j : j = 1, 2, \dots, s\}$ spans E over K . Hence

$$f = \sum_{i=1}^r b_i f_i = \sum_{i=1}^r \left(\sum_{j=1}^s a_{ij} e_j \right) f_i = \sum_{i,j} a_{ij} (e_j f_i)$$

is a linear combination of $e_j f_i = f_i e_j$ over K . Thus $\{f_i e_j\}$ spans F over K .

Furthermore, $\{f_i e_j\}$ is linearly independent over K . Indeed, if b_{ij} are elements of K such that

$$\sum_{i,j} b_{ij} f_i e_j = 0$$

then
$$\sum_{i=1}^r \left(\sum_{j=1}^s b_{ij} e_j \right) f_i = 0,$$

where $\sum_{j=1}^s b_{ij} e_j \in E$ for each i . Since $\{f_i : i = 1, 2, \dots, r\}$ is linearly independent over E , we have $\sum_{j=1}^s b_{ij} e_j = 0$ for each i . Since $\{e_j : j = 1, 2, \dots, s\}$ is linearly independent over E , we obtain $b_{ij} = 0$ for each ij . Hence $\{f_i e_j\}$ is linearly independent over K .

Thus $\{f_i e_j\}$ is a K -basis of F and $|F:K| = rs = |F:E| |E:K|$. □

It follows from Theorem 48.13 by induction that

$$|K_n:K_1| = |K_n:K_{n-1}| |K_{n-1}:K_{n-2}| \dots |K_2:K_1|$$

whenever $K_n/K_{n-1}, K_{n-1}/K_{n-2}, \dots, K_2/K_1$ are finite dimensional field extensions. In fact, Theorem 48.13 and its generalization is true for infinite dimensional extensions, too, but we will not need this.

48.14 Lemma: *Let F/E and E/K be field extensions. If $|F:K|$ is finite, then $|F:E|$ and $|E:K|$ are both finite. In fact, both of them are divisors of $|F:K|$ and $|F:K| = |F:E| |E:K|$.*

Proof: Let $n = |F:K|$ and let $\{f_i : i = 1, 2, \dots, n\}$ be a basis of F over K . Then $\{f_i : i = 1, 2, \dots, n\}$ spans F over E and so $|F:E| \leq n$ by Steinitz' replacement theorem. Thus $|F:E|$ is finite.

Now the finiteness of $|E:K|$. If E were infinite dimensional over K , there would be $n + 1$ K -linearly independent elements of E , so there would be

$n + 1$ K -linearly independent elements of F , contradicting $|F:K| = n$. Thus $|E:K|$ is finite.

We now obtain $n = |F:K| = |F:E| |E:K|$ from Theorem 48.13. In particular, $|F:E|$ and $|E:K|$ divide n .

□

Exercises

1. Let E be a field and $K \subseteq E$. Show that K is a subfield of E if and only if K is a subgroup of E and $K \setminus \{0\}$ is a subgroup of $E \setminus \{0\}$.
2. Let p be prime. Is \mathbb{Z}_{p^2} an extension of \mathbb{Z}_p ? Is \mathbb{Z}_{p^3} an extension of \mathbb{Z}_{p^2} ?
3. Prove that $\mathbb{Q}(\omega) = \{x + y\omega : x, y \in \mathbb{Q}\}$ and $\mathbb{Q}(\sqrt{5}i) = \{x + y\sqrt{5}i : x, y \in \mathbb{Q}\}$ are subfields of \mathbb{C} .
4. Let K be a field and let $\text{Aut}(K)$ be the set of all field automorphisms of K . Show that $\text{Aut}(K)$ is a group under composition.
5. Find all automorphisms of \mathbb{Q} , \mathbb{F}_p , $\mathbb{Q}(i)$, $\mathbb{Q}(\omega)$, $\mathbb{Q}(\sqrt{5}i)$, $\mathbb{Q}(\sqrt[3]{2})$ (see Ex.3).
6. Find three nonisomorphic infinite fields of characteristic $p \neq 0$.
7. Find the degrees of the following extensions: \mathbb{C}/\mathbb{R} , $\mathbb{C}/\mathbb{Q}(i)$, $\mathbb{Q}(i)/\mathbb{Q}$, \mathbb{R}/\mathbb{Q} , $\mathbb{F}(x)/\mathbb{F}$.
8. Show that $\mathbb{Q}(\sqrt{2}, i) := \{a + b\sqrt{2} + ci + d\sqrt{2}i : a, b, c, d \in \mathbb{Q}\}$ is an extension field of both $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{2})$. Find $|\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}|$ by two different methods.
9. Prove or disprove: If E/K_1 and E/K_2 are finite dimensional field extensions, then $E/(K_1 \cap K_2)$ is finite dimensional, too.
10. Let K be a field and e the identity element of K . Show that $\text{char } K = 0$ or p according as the subring of K generated by e is isomorphic to \mathbb{Z} or to \mathbb{Z}_p .
11. Find the prime subfields of the fields in §29, Ex. 8.

12. Let K be a field of characteristic $p \neq 0$. Prove that $\varphi: K \rightarrow K$ is a field homomorphism.
 $a \rightarrow a^p$