Chapter 1

Preliminaries on Fields and Polynomials

1.1. FIELDS OF FRACTIONS

A basic relationship between the field **Q** and its subdomain **Z** with which the reader is already familiar is that every element of **Q** can be expressed as a fraction with numerator and denominator in **Z**. It is clear that such a connection can be meaningfully formulated in the more general context of an arbitrary field and a subdomain. This leads to the general concept of a field of fractions, which we shall discuss in this section.

Let A be a domain. By a **field of fractions of** A we understand a field K having A as a subdomain and such that every element of K is expressible in the form α/β with $\alpha, \beta \in A$ and $\beta \neq 0$.

It follows that if A is a domain, and if K is a field of fractions of A, then no proper subfield of K contains A, and K is a field of fraction of every intermediate domain between A and K.

In particular, a field is its only field of fractions.

The preceding definition immediately suggests the questions of existence and essential uniqueness of fields of fractions of domains. In the discussion that follows we shall see that these can be settled completely.

If a domain is given as a subdomain of a field, there is no difficulty in showing that it admits a field of fractions. In fact, we have the following result.

1.1.1. Proposition. *Let K be a field, and let A be a subdomain of K. Then the subfield of K generated by A is the only subfield of K that is a field of fractions of A; it consists of all elements of K of the form α/β with $\alpha, \beta \in A$ and $\beta \neq 0$.*

Proof. Let F denote the set of all elements of K of the form α/β with $\alpha, \beta \in A$ and $\beta \neq 0$. It is clear that $A \subseteq F$. Moreover, in view of the equalities

$$(\alpha/\beta) \pm (\gamma/\delta) = (\alpha\delta \pm \beta\gamma)/\beta\delta \quad \text{and} \quad (\alpha/\beta)(\gamma/\delta) = \alpha\gamma/\beta\delta,$$

which hold when $\alpha, \beta, \gamma, \delta \in A$ and $\beta \neq 0 \neq \delta$, we see that F is a subdomain of K. Finally, since $(\alpha/\beta)^{-1} = \beta/\alpha \in F$ whenever $\alpha, \beta \in A$ and $\alpha \neq 0 \neq \beta$, we conclude that F is a subfield of K.

It follows from its definition that F is the only subfield of K that is a field of fractions of A; and since it is contained in every subfield of K containing A, it is the subfield of K generated by A. □

The preceding proposition shows that if K is a field, and if A is a subdomain of K, we are justified in speaking of the subfield of K generated by A as **the field of fractions of A in K**.

We shall now establish the existence of a field of fractions of an arbitrary domain, without assuming *a priori* that it is contained in a field.

1.1.2. Theorem. *Every domain admits a field of fractions.*

Proof. This is an important theorem, but its proof may appear to be artificial. We shall first make some observations that may help to motivate the argument.

If K is a field, and if $\alpha, \beta, \gamma, \delta \in K$ and $\beta \neq 0 \neq \delta$, then to say that $\alpha/\beta = \gamma/\delta$ means that $\alpha\beta^{-1} = \gamma\delta^{-1}$, which in turn means that $\alpha\delta = \beta\gamma$. If the four elements $\alpha, \beta, \gamma, \delta$ belong to a subdomain A of K, we see that the equality $\alpha/\beta = \gamma/\delta$ *in* K is equivalent to the equality $\alpha\delta = \beta\gamma$ *in* A.

If we are given a domain A, then an element of a field of fractions of A is determined by a pair in $A \times (A - \{0\})$. We are led, therefore, to think of every such pair (α, β) as determining the element α/β of that field, and to take into consideration that two such pairs (α, β) and (γ, δ) determine the same element of the latter if and only if $\alpha\delta = \beta\gamma$. Note that this does *not* require A to be given as a subdomain of some field.

We can now proceed with the formal argument. It will be clear to the reader that we shall be merely imitating the familiar method of constructing $\mathbf{Q}$ from $\mathbf{Z}$. For this reason, we shall omit the tedious details required in the verification of some assertions.

Consider a domain A, and let $E = A \times (A - \{0\})$. If $(\alpha, \beta), (\gamma, \delta) \in E$, let us write $(\alpha, \beta) \sim (\gamma, \delta)$ if and only if $\alpha\delta = \beta\gamma$. It is easily verified that this defines an equivalence relation on E. Let F denote the resulting quotient set; and for each $(\alpha, \beta) \in E$, let $\langle \alpha, \beta \rangle$ denote the equivalence class in F determined by (α, β).

Now suppose that $(\alpha,\beta),(\gamma,\delta),(\bar{\alpha},\bar{\beta}),(\bar{\gamma},\bar{\delta})\in E$, and that $(\alpha,\beta)\sim(\gamma,\delta)$ and $(\bar{\alpha},\bar{\beta})\sim(\bar{\gamma},\bar{\delta})$. Then $\alpha\delta=\beta\gamma$ and $\bar{\alpha}\bar{\delta}=\bar{\beta}\bar{\gamma}$, so that

$$(\alpha\bar{\beta}+\bar{\alpha}\beta)(\delta\bar{\delta})=(\alpha\delta)(\bar{\beta}\bar{\delta})+(\bar{\alpha}\bar{\delta})(\beta\delta)$$
$$=(\beta\gamma)(\bar{\beta}\bar{\delta})+(\bar{\beta}\bar{\gamma})(\beta\delta)=(\gamma\bar{\delta}+\bar{\gamma}\delta)(\beta\bar{\beta})$$

and

$$(\alpha\bar{\alpha})(\delta\bar{\delta})=(\alpha\delta)(\bar{\alpha}\bar{\delta})=(\beta\gamma)(\bar{\beta}\bar{\gamma})=(\gamma\bar{\gamma})(\beta\bar{\beta}),$$

which implies that

$$(\alpha\bar{\beta}+\bar{\alpha}\beta,\beta\bar{\beta})\sim(\gamma\bar{\delta}+\bar{\gamma}\delta,\delta\bar{\delta})$$

and

$$(\alpha\bar{\alpha},\beta\bar{\beta})\sim(\gamma\bar{\gamma},\delta\bar{\delta}).$$

Consequently, there exist two operations in F such that

$$(\langle\alpha,\beta\rangle,\langle\bar{\alpha},\bar{\beta}\rangle)\to\langle\alpha\bar{\beta}+\bar{\alpha}\beta,\beta\bar{\beta}\rangle$$

and

$$(\langle\alpha,\beta\rangle,\langle\bar{\alpha},\bar{\beta}\rangle)\to\langle\alpha\bar{\alpha},\beta\bar{\beta}\rangle$$

for all $(\alpha,\beta),(\bar{\alpha},\bar{\beta})\in E$. Let us use, respectively, the additive and multiplicative notations for these operations; we then have

$$\langle\alpha,\beta\rangle+\langle\bar{\alpha},\bar{\beta}\rangle=\langle\alpha\bar{\beta}+\bar{\alpha}\beta,\beta\bar{\beta}\rangle$$

and

$$\langle\alpha,\beta\rangle\langle\bar{\alpha},\bar{\beta}\rangle=\langle\alpha\bar{\alpha},\beta\bar{\beta}\rangle$$

whenever $\alpha,\beta,\bar{\alpha},\bar{\beta}\in A$ and $\beta\neq0\neq\bar{\beta}$.

A tedious, but completely elementary, computation now shows that this addition and this multiplication define a field structure on F with respect to which the zero and unit elements are, respectively, $\langle0,1\rangle$ and $\langle1,1\rangle$. For all $\alpha,\beta\in A$ with $\beta\neq0$, the additive inverse of $\langle\alpha,\beta\rangle$ is $\langle-\alpha,\beta\rangle$; and for all $\alpha,\beta\in A$ with $\alpha\neq0\neq\beta$, the multiplicative inverse of $\langle\alpha,\beta\rangle$ is $\langle\beta,\alpha\rangle$.

It is readily seen that if F is provided with this field structure, the mapping $\alpha\to\langle\alpha,1\rangle$ from A to F is a monomorphism. It then follows from 0.0.1 that there exist a field K and an isomorphism u from K to F such that A is a subdomain of K and such that u extends this monomorphism from A to F.

We now claim that K is a field of fractions of A. Indeed, if $\theta\in K$, we can write $u(\theta)=\langle\alpha,\beta\rangle$ with $\alpha,\beta\in A$ and $\beta\neq0$; then

$$u(\theta)=\langle\alpha,\beta\rangle=\langle\alpha,1\rangle\langle1,\beta\rangle=\langle\alpha,1\rangle/\langle\beta,1\rangle$$
$$=u(\alpha)/u(\beta)=u(\alpha/\beta),$$

whence $\theta=\alpha/\beta$. □

The essential uniqueness of fields of fractions will be a consequence of the following fundamental result on the extendibility of monomorphisms.

1.1.3. Theorem. *Let A be a domain, and let K be a field of fractions of A. If F is a field, and if u is a monomorphism from A to F, then there exists a mapping from K to F such that $\alpha/\beta \to u(\alpha)/u(\beta)$ whenever $\alpha, \beta \in A$ and $\beta \neq 0$; and this mapping is the only monomorphism from K to F extending u.*

Proof. First note that if v is a monomorphism from K to F extending u, then

$$v(\alpha/\beta) = v(\alpha)/v(\beta) = u(\alpha)/u(\beta)$$

when $\alpha, \beta \in A$ and $\beta \neq 0$. This shows that there exists at most one monomorphism from K to F extending u, and explains why we are led to consider the possibility of defining a mapping from K to F such that $\alpha/\beta \to u(\alpha)/u(\beta)$ whenever $\alpha, \beta \in A$ and $\beta \neq 0$.

If $\alpha, \beta \in A$ and $\beta \neq 0$, then $u(\beta) \neq 0$, and hence it is meaningful to form the fraction $u(\alpha)/u(\beta)$ in F. Furthermore, if $\alpha, \beta, \gamma, \delta \in A$ and $\beta \neq 0 \neq \delta$, and if $\alpha/\beta = \gamma/\delta$, then $\alpha\delta = \beta\gamma$; therefore

$$u(\alpha)u(\delta) = u(\alpha\delta) = u(\beta\gamma) = u(\beta)u(\gamma),$$

which implies that $u(\alpha)/u(\beta) = u(\gamma)/u(\delta)$.

It follows that there exists a mapping from K to F such that $\alpha/\beta \to u(\alpha)/u(\beta)$ when $\alpha, \beta \in A$ and $\beta \neq 0$. This mapping obviously extends u; and an easy computation shows that it is a homomorphism from K to F. Consequently, it is a monomorphism from K to F extending u. □

The following two important corollaries are immediate.

1.1.4. Corollary. *Let A and B be domains, and let K and L be, respectively, fields of fractions of A and B. Then every isomorphism from A to B is uniquely extendible to an isomorphism from K to L.*

1.1.5. Corollary. *Let A be a domain, and let K and L be fields of fractions of A. Then there exists a unique A-isomorphism from K to L.*

The property of unique extendibility of monomorphisms stated in the preceding theorem actually characterizes fields of fractions (problem 1).

The second corollary shows that two fields of fractions K and L of a domain A are related in the strongest possible way. Note that the A-isomorphism from K to L "looks like" an identity mapping; for if $\alpha, \beta \in A$ and $\beta \neq 0$, it sends the fraction α/β *in* K to the fraction α/β *in* L.

Sometimes we speak of "the" field of fractions of a domain A. What is meant, of course, is that every two fields of fractions of A are being "identified" with each other by means of the A-isomorphism between them.

Note that if such "identifications" are made, then whenever A and B are domains such that A is a subdomain of B, "the" field of fractions of A is a subfield of "the" field of fractions of B.

Let K be a field, and let I be a set. Then the polynomial ring $K[X_i]_{i\in I}$ is a domain. "Its" field of fractions is denoted by $K(X_i)_{i\in I}$, and its elements are called **rational functions**. When I is nonempty and finite, we apply the same notational changes as in the case of polynomials: If $n = \mathrm{Card}(I)$ and $I = \{i_1, i_2, \ldots, i_n\}$, we write $K(X_{i_1}, X_{i_2}, \ldots, X_{i_n})$ instead of $K(X_i)_{i\in I}$. In particular, we write $K(X)$ for "the" field of fractions of $K[X]$.

PROBLEMS

1. Let K be a field, and let A be a subdomain of K. Suppose that for every field F, every monomorphism from A to F is extendible to a monomorphism from K to F. Prove that K is a field of fractions of A.
2. Let A be a domain, and let K be a field of fractions of A. Prove that if $(\theta_i)_{i\in I}$ is a finite family of elements of K, then there exist a family $(\alpha_i)_{i\in I}$ of elements of A and a $\beta \in A - \{0\}$ such that $\theta_i = \alpha_i/\beta$ for every $i \in I$.

   Give an example that shows that this assertion does not remain valid if the finiteness assumption is omitted.
3. Let A be a domain, let K be a field of fractions of A, and let I be a set. Show that $K(X_i)_{i\in I}$ is a field of fractions of $A[X_i]_{i\in I}$.
4. Let A be a domain, let $\mathscr{P}$ be a prime ideal of A, and let K be a field of fractions of A. Let R denote the subset of K consisting of the fractions α/β with $\alpha \in A$ and $\beta \in A - \mathscr{P}$; and let $\mathscr{M}$ denote the subset of K consisting of the fractions α/β with $\alpha \in \mathscr{P}$ and $\beta \in A - \mathscr{P}$. Verify the following assertions:
   a. R is an intermediate domain between A and K.
   b. $\mathscr{M}$ is the only maximal ideal of R.
   c. $\mathscr{P} = A \cap \mathscr{M}$.
   d. There exists a monomorphism from $A/\mathscr{P}$ to $R/\mathscr{M}$ such that $\alpha + \mathscr{P} \to \alpha + \mathscr{M}$ for every $\alpha \in A$.
   e. If F is a field of fractions of $A/\mathscr{P}$, then the monomorphism from F to $R/\mathscr{M}$ extending the monomorphism described in assertion d is an isomorphism.
5. Let A be a factorial domain, and let K be a field of fractions of A. Prove that every element of K that is a zero of a monic polynomial in $A[X]$ belongs to A.

1.2. THE CHARACTERISTIC

Let A be a domain. We know that there exists a unique homomorphism $\mathbf{Z}$ to A. The kernel of this homomorphism is a prime ideal of $\mathbf{Z}$; its nonnegative generator is called the **characteristic of** A and is denoted by $\mathrm{Char}(A)$. There

are two possibilities for Char(A): It is either 0 or a prime, according as the homomorphism from $\mathbf{Z}$ to A is or is not injective.

Let us recall that, given a domain A and an integer n, it is customary to denote by the same symbol n the element of A assigned to the integer n by the homomorphism from $\mathbf{Z}$ to A.

When A has prime characteristic p, we have to keep in mind that distinct integers may represent a single element of A. In fact, if m and n are integers, the equality $m = n$ holds in A if and only if $m \equiv n \pmod{p}$, since each of these conditions expresses the fact that $m - n$ belongs to the kernel of the homomorphism from $\mathbf{Z}$ to A. In particular, if n is an integer, then the equality $n = 0$ holds in A if and only if $p \mid n$.

This mild notational ambiguity, which should not cause confusion, does not occur when A has characteristic 0. In this case, we can simply regard $\mathbf{Z}$ as a subdomain of A; in other words, $\mathbf{Z}$ can be "identified" with its image in A.

The following examples show that there exist fields of every possible characteristic.

1.2.1. Examples

a. Every domain admitting $\mathbf{Z}$ as a subdomain has characteristic 0.

This is obvious: If A is such a domain, then the homomorphism from $\mathbf{Z}$ to A is the inclusion mapping $i_{\mathbf{Z} \to A}$, which is injective.

b. If p is a prime, then the field $\mathbf{Z}/p$ has characteristic p.

Indeed, the homomorphism from $\mathbf{Z}$ to $\mathbf{Z}/p$ is the natural projection, which has $p\mathbf{Z}$ as its kernel. □

We shall now derive the basic properties of the characteristic.

1.2.2. Proposition. *Let A be a domain. Then the following conditions are equivalent*:

(a) Char(A) = 0.
(b) $\mathbf{Z}$ *is embeddable in* A.
(c) *The image of* $\mathbf{Z}$ *in* A *is not a field.*

Proof. Let u denote the homomorphism from $\mathbf{Z}$ to A. To prove the equivalence of (a) and (b), we need only note that $\mathbf{Z}$ is embeddable in A if and only if u is injective, hence if and only if Char(A) = 0.

Since $\mathbf{Z}/\mathrm{Ker}(u)$ and $\mathrm{Im}(u)$ are isomorphic, to say that $\mathrm{Im}(u)$ is a field means that $\mathbf{Z}/\mathrm{Ker}(u)$ is a field, which in turn means that $\mathrm{Ker}(u)$ is nonnull. This shows that (a) and (c) are equivalent. □

1.2.3. Corollary. *If K is a field, then* Char(K) = 0 *if and only if* $\mathbf{Q}$ *is embeddable in K.*

Proof. Since $\mathbf{Q}$ is a field of fractions of $\mathbf{Z}$, we know from 1.1.3 that the embeddability of $\mathbf{Z}$ in K is equivalent to that of $\mathbf{Q}$ in K. □

1.2.4. Corollary. *Every finite field has prime characteristic.*

Proof. By the preceding corollary, a field of characteristic 0 contains a subfield equipotent to $\mathbf{Q}$, and hence it is not finite. □

1.2.5. Proposition. *Let A be a domain, and let p be a prime. Then the following conditions are equivalent*:

(a) $\mathrm{Char}(A) = p$.
(b) *The equality* $p = 0$ *holds in* A.
(c) $\mathbf{Z}/p$ *is embeddable in* A.
(d) *The image of* $\mathbf{Z}$ *in* A *and* $\mathbf{Z}/p$ *are isomorphic.*

Proof. As in the proof of proposition 1.2.2, let u denote the homomorphism from $\mathbf{Z}$ to A.

We already know that (a) implies (b). To verify the opposite implication, note that if the equality $p = 0$ holds in A, then $\mathrm{Char}(A) \neq 0$ and $\mathrm{Char}(A) | p$, whence $\mathrm{Char}(A) = p$. Thus, (a) and (b) are equivalent.

To prove that (a) implies (d), suppose that $\mathrm{Char}(A) = p$. Then $\mathrm{Ker}(u) = p\mathbf{Z}$, and hence $\mathbf{Z}/\mathrm{Ker}(u) = \mathbf{Z}/p$. Since $\mathbf{Z}/\mathrm{Ker}(u)$ and $\mathrm{Im}(u)$ are isomorphic, it follows that $\mathrm{Im}(u)$ and $\mathbf{Z}/p$ are isomorphic.

It is obvious that (d) implies (c). For if $\mathbf{Z}/p$ is isomorphic to the subring $\mathrm{Im}(u)$ of A, then it is embeddable in A.

To conclude, we now show that (c) implies (a). Suppose that $\mathbf{Z}/p$ is embeddable in A, and choose a monomorphism v from $\mathbf{Z}/p$ to A. If w denotes the natural projection from $\mathbf{Z}$ to $\mathbf{Z}/p$, it is clear that $u = v \circ w$. Furthermore, since v is injective, we have

$$\mathrm{Ker}(u) = \mathrm{Ker}(v \circ w) = \mathrm{Ker}(w) = p\mathbf{Z},$$

whence $\mathrm{Char}(A) = p$. □

1.2.6. Proposition. *If A and B are domains such that A is embeddable in B, then* $\mathrm{Char}(A) = \mathrm{Char}(B)$.

Proof. Since every ring that is embeddable in A is embeddable in B, this follows at once from 1.2.2 and 1.2.5. □

In regard to 1.2.4, it should be noted that there exist infinite fields of every possible characteristic. For if K is a field and I is a nonempty set, then the field $K(X_i)_{i \in I}$ of rational functions is infinite; and by 1.2.6, it has the same characteristic as K.

Given a domain A and a positive integer n, the mapping $\alpha \to \alpha^n$ from A to A is usually of very limited interest, because it does not have good *additive* properties.

It is known that some beginners in algebra, with complete disregard for the classical binomial theorem, are quite prepared to accept the validity of the equality

$$(\alpha \pm \beta)^n = \alpha^n \pm \beta^n.$$

As a consequence, they reach a number of interesting conclusions.

The "freshman's dream", as the illusion just described is sometimes called, actually contains an element of truth: It will be shown presently that the equality

$$(\alpha \pm \beta)^{p^n} = \alpha^{p^n} \pm \beta^{p^n}$$

holds in domains of prime characteristic p. This will exemplify one of the fundamental differences between fields of characteristic 0 and fields of prime characteristic.

Let A be a domain of prime characteristic p. The mapping $\alpha \to \alpha^p$ from A to A is called the **Frobenius mapping of** A.

The following theorem explains why the Frobenius mapping is of interest in the theory of fields.

1.2.7. Theorem. *If A is a domain of prime characteristic, then the Frobenius mapping of A is an injective endomorphism.*

Proof. Let us put $p = \mathrm{Char}(A)$. Since the conditions $\alpha \in A$ and $\alpha^p = 0$ imply that $\alpha = 0$, we need only prove that the Frobenius mapping of A is an endomorphism; and to do this, it suffices to verify that

$$(\alpha + \beta)^p = \alpha^p + \beta^p$$

for all $\alpha, \beta \in A$.

Let $1 \leq k \leq p-1$; since

$$p \nmid k!, \quad p \nmid (p-k)!, \quad \text{and} \quad p \mid p!,$$

and since

$$p! = k!(p-k)!\binom{p}{k},$$

we conclude next that $p \mid \binom{p}{k}$, and hence the equality $\binom{p}{k} = 0$ holds in A.

Now it is easy to complete the proof. For if $\alpha, \beta \in A$, then

$$(\alpha+\beta)^p = \sum_{k=0}^{p} \binom{p}{k} \alpha^{p-k}\beta^k$$

$$= \alpha^p + \sum_{k=1}^{p-1} \binom{p}{k} \alpha^{p-k}\beta^k + \beta^p = \alpha^p + \beta^p,$$

which is what was needed. □

1.2.8. Corollary. *If A is a domain of prime characteristic p, and if n is a nonnegative integer, then the mapping $\alpha \to \alpha^{p^n}$ from A to A is an injective endomorphism.*

Proof. This is obvious: If $n = 0$, the mapping in question is i_A; and if $n > 0$, it is the nth iterate of the Frobenius mapping of A. □

1.2.9. Example. Let A be a domain of prime characteristic p, If $\alpha \in A$ and if n is a nonnegative integer, then the polynomial $X^{p^n} - \alpha$ in $A[X]$ admits at most one zero in A.

For if β and γ are zeros of $X^{p^n} - \alpha$ in A, then

$$\beta^{p^n} = \alpha = \gamma^{p^n},$$

and the preceding corollary shows that $\beta = \gamma$. □

PROBLEMS

1. Let p be a prime. Use the fact that $\mathrm{Char}(\mathbf{Z}/p) = p$ in order to prove that
$$n^p \equiv n \pmod{p}$$
for every integer n. (This result is known as **Fermat's little theorem**.)
2. Let p be a prime. Verify that 1 and $p-1$ are the zeros of $X^2 - 1$ in $\mathbf{Z}/p$, and then prove that
$$(p-1)! \equiv -1 \pmod{p}.$$
(This result is known as **Wilson's theorem**.)
3. Let A be a domain of prime characteristic p. Show that
$$(\alpha - \beta)^{p-1} = \sum_{k=0}^{p-1} \alpha^{p-1-k}\beta^k$$
for all $\alpha, \beta \in A$.
4. Let A and B be domains. Show that if A has prime characteristic and if there exists a homomorphism from A to B, then $\mathrm{Char}(A) = \mathrm{Char}(B)$.
5. Give an example of two fields of characteristic 0 neither of which is embeddable in the other.
6. Let A be a domain. Prove the following assertions:
   a. $\mathrm{Char}(A) = 2$ if and only if $-\alpha = \alpha$ for every $\alpha \in A$.
   b. If A^* is embeddable in A^+, then $\mathrm{Char}(A) = 2$.
   c. A^* and A^+ are not isomorphic.
7. Let K be a field such that $\mathrm{Char}(K) \neq 2$, and let u be a mapping from K to K such that $u(1) = 1$, $u(\alpha + \beta) = u(\alpha) + u(\beta)$ for all $\alpha, \beta \in K$, and $u(\alpha)u(1/\alpha) = 1$ for all $\alpha \in K^*$. Show that u is an endomorphism.

1.3. PERFECT FIELDS AND PRIME FIELDS

The two special types of field appearing in the title of this section arise naturally in connection with the characteristic.

In general, the Frobenius mapping of a domain of prime characteristic is not an automorphism, because it may fail to be surjective (problem 1). On the other hand, there exist domains of prime characteristic for which the Frobenius mapping reduces to the identity mapping (problem 2).

We say that a field is **perfect** when either it has characteristic 0 or it has prime characteristic and its Frobenius mapping is an automorphism.

If K is a field of prime characteristic p, the symbol K^p will be used to denote the image of the Frobenius mapping of K. Thus, K^p is the subfield of K consisting of the elements of K that admit pth roots in K; and the mapping $\alpha \to \alpha^p$ from K to K^p is an isomorphism.

It follows that a field K of prime characteristic p is perfect if and only if $K^p = K$, hence if and only if every element of K admits a pth root in K.

The same comments made in the proof of 1.2.8 can now be used in order to prove the following proposition.

1.3.1. Proposition. *If K is a perfect field of prime characteristic p, and if n is a nonnegative integer, then the mapping $\alpha \to \alpha^{p^n}$ from K to K is an automorphism.*

As the next proposition shows, there exist perfect fields of every possible prime characteristic.

1.3.2. Proposition. *Every finite field is perfect.*

Proof. We have already seen that every finite field has prime characteristic; and since every injective mapping from a finite set to itself is bijective, the Frobenius mapping of every finite field is an automorphism. □

It can also be shown that there exist fields that are not perfect of every possible prime characteristic (problem 1).

One of the important properties of field extensions that we shall study in detail is that of separability. It will be seen that perfect fields can be described as the fields that do not admit inseparable extensions.

We say that a field is **prime** when it is its only subfield. Equivalently, a field is prime when it possesses no proper subfields.

It is not difficult to determine the prime fields. In fact, we have the following result.

1.3.3. Proposition. *A field of characteristic 0 is prime if and only if it is isomorphic to $\mathbf{Q}$; and a field of prime characteristic p is prime if and only if it is isomorphic to $\mathbf{Z}/p$.*