# PROLOGUE

O glücklich, wer noch hoffen kann,
Aus diesem Meer des Irrtums aufzutauchen!
Was man nicht weiss, das eben brauchte man,
Und was man weiss, kann man nicht brauchen.
Goethe, *Faust I*

One of the principal aims of this book is to describe some methods of constructing skew fields. The case most studied so far is that of skew fields finite-dimensional over their centres. But a finite-dimensional $k$-algebra, where $k$ is a commutative field, is a field whenever it has no zero-divisors. On the one hand this enormously simplifies their study, while on the other hand it puts many constructions out of bounds (because they produce infinite-dimensional algebras). The study of fields that are not necessarily finite-dimensional over their centres is still in its early stages, and the methods needed here are not very closely related to those used on finite-dimensional algebras – the relation between these subjects is rather like the relation between finite and infinite groups.

There are some ways of obtaining a field directly, for example Schur's lemma tells us that the endomorphism ring of a simple module is a field, and the coordinatization theorem shows that when we coordinatize a Desarguesian plane, the coordinates lie in a field. But these methods are not very explicit, and we shall have no more to say about them. For us the usual way to construct a field is to take a suitable ring and embed it in a field. What is to be understood by 'suitable' will transpire later.

There are five methods of interest to us; they are

(1) Ore's method (Ch. 1),
(2) The method of power series (Ch. 2),
(3) Inverse limits of Ore domains (Ch. 2),

(4) A general criterion (Ch. 4),
(5) An application of the specialization lemma (Ch. 6).

As a test ring we shall use the free algebra on a set $X$ over a commutative field $k$, written $k\langle X\rangle$. All five methods can be used on $k\langle X\rangle$, and each has its pros and cons. (1) is particularly simple, but not in any way canonical, (2) and (3) provide a convenient normal form, while (4) gives, at least in principle, a complete survey over all possible embeddings, indeed over all homomorphisms of our ring into fields. Finally (5) applies only to free algebras, where it gives an easy existence proof of the universal field of fractions.

The main applications are to the construction of the field coproduct, which shows that the class of skew fields possesses the amalgamation property and allows a form of HNN-construction. The consequences are described here, but it is clear that the existing range of constructions is still rather limited, mainly because a good specialization theory is still lacking (see 8.8 below). One would hope that the present work will offer encouragement to others working towards that goal.

# 1

# Rings and their fields of fractions

Fields, especially skew fields, are generally constructed as the field of fractions of some ring, but of course not every ring has a field of fractions and for a given ring it may be quite difficult to decide if a field of fractions exists. While a full discussion of this question is left to Ch. 4, for the moment we shall bring some general observations on the kind of conditions to expect (mainly quasi-identities) in 1.2 and give some necessary conditions relating to the rank of free modules in 1.4, as well as some sufficient conditions. On the one hand there is the Ore condition in 1.3, generalizing the commutative case; on the other hand and perhaps less familiar, we have the trivializability of relations, leading to semifirs in 1.6, which include free algebras and coproducts of fields, as we shall see in Ch. 5. Some general relations between matrices over rings, and the applications to the factorization of elements over principal ideal domains (needed later) are described in 1.5.

Although readers will have met fields before, a formal definition is given in 1.1 and is contrasted there with the definition of near fields, which however will not occupy us further. The final section 1.7 deals with the matrix functor and its left adjoint, the matrix reduction functor, which will be of use later in constructing counter-examples.

## 1.1 Fields, skew fields and near fields

By a *field* we understand a set $K$ with two binary operations, *addition*, denoted by a plus sign: $+$, and *multiplication*, denoted by a cross, $\times$, a dot, $\cdot$, or simply by juxtaposition, with two distinguished elements, zero: 0 and one: 1, such that

(i) $K$ is a group under addition, with 0 as neutral element,

(ii) $1 \neq 0$ and $K^\times = K\backslash\{0\}$ is a group under multiplication, with 1 as neutral element,

(iii) the two operations are related by the *distributive laws*:

$$x(y + z) = xy + xz, (x + y)z = xz + yz \text{ for all } x, y, z \in K.$$

The groups $K$ in (i) and $K^\times$ in (ii) are the *additive group* and the *multiplicative group* of $K$ respectively.

Our first observation is that the additive group is always abelian. For, using first the left and then the right distributive law, we have

$$(x + 1)(y + 1) = (x + 1)y + (x + 1)\cdot 1 = xy + y + x + 1,$$

while an expansion on the other side gives

$$(x + 1)(y + 1) = x(y + 1) + 1\cdot(y + 1) = xy + x + y + 1.$$

Equating the results and cancelling $xy$ on the left and 1 on the right, we find that $y + x = x + y$, as claimed.

If the multiplicative group of $K$ is abelian, $K$ is a *commutative field*; when commutativity is not assumed, $K$ is called a *skew field* or also a *division ring*. Since skew fields form the topic of this book, we shall use the term 'field' to mean 'not necessarily commutative field' and only occasionally add 'skew', when emphasis is needed.

Let $K$ be a field. Any *subfield* of $K$ (i.e. a subset of $K$ admitting all the operations of $K$) contains 1 and hence the subfield generated by 1. This least subfield, often denoted by $\Pi$, is called the *prime subfield* of $K$. It is either the rational field $\mathbf{Q}$ or $\mathbf{Z}/p$, the integers mod $p$, for some prime $p$. Accordingly $K$ is said to have *characteristic* 0 or $p$; this characteristic is also written char $K$.

Given a field $K$ and a subset $X$ of $K$, the *centralizer* of $X$ in $K$ is defined as the set

$$\mathcal{C}_K(X) = \{y \in K | xy = yx \text{ for all } x \in X\}.$$

This set is easily seen to be a subfield of $K$. In the special case $X = K$ we obtain the *centre* $C$ of $K$:

$$C = \{y \in K | xy = yx \text{ for all } x \in K\}.$$

Clearly the centre is a commutative subfield containing the prime subfield $\Pi$.

Just as rings arise naturally as the endomorphism sets of abelian groups, or more generally, of modules, i.e. groups with operators, so fields arise as endomorphism sets of simple modules. Their importance stems from the fact that linear algebra, first developed over the real

numbers, can be carried out over any field. This applies even to skew fields, as long as we do not try to form determinants. In fact there is a form of determinant over skew fields, the Dieudonné determinant, but this will play only a limited role here. The main difference is that whereas the structure of commutative fields is fairly well known since the fundamental paper of Steinitz [10], information on skew fields is much more fragmentary. The theory is best developed for fields finite-dimensional over their centres (division algebras), but we shall mainly be concerned with fields infinite-dimensional over their centres, where a full classification is not to be expected.

It is a natural question to ask what can be said about endomorphism sets of non-abelian groups. Let $G$ be a group written multiplicatively and consider the set $\mathcal{M}(G)$ of all mappings preserving 1 of $G$ into itself. On $\mathcal{M}(G)$ we have two operations, the multiplication arising by composition of mappings and addition arising from the group operation:

$$x(\alpha\beta) = (x\alpha)\beta,\ x(\alpha + \beta) = x\alpha \cdot x\beta \text{ for all } x \in G,\ \alpha, \beta \in \mathcal{M}(G).$$

It follows that the left distributive law holds,

$$\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma, \quad \alpha, \beta, \gamma \in \mathcal{M}(G),$$

but the right distributive law fails to hold in general. In fact we have

$$(\alpha + \beta)\gamma = \alpha\gamma + \beta\gamma$$

for all $\alpha, \beta \in \mathcal{M}(G)$ only when $\gamma$ is an endomorphism of $G$. However, if we restrict ourselves to endomorphisms we no longer have an addition, because the sum of two endomorphisms need not be an endomorphism. Thus $\mathcal{M}(G)$ fails to be a ring only in that it lacks the right distributive law (except for the vestige $0\alpha = 0$) and the commutativity of addition. It forms an example of a *near ring*; a subring whose non-zero elements all have inverses is a *near field*. Near fields have been used in the study of permutation groups, in geometry, as the rings coordinatizing certain translation planes and in the classification of finite subgroups of skew fields (see Amitsur [55] and for the results, 3.9 below), but they will not occupy us further in this volume. For a detailed account of near fields see Wähling [87].

In any field $K$ the addition can be expressed in terms of the multiplication $xy$ and the operation $x + 1$. For we clearly have

$$x + y = \begin{cases} (xy^{-1} + 1)y & \text{if } y \neq 0, \\ x & \text{if } y = 0. \end{cases}$$

This observation leads to a definition of fields which emphasizes the multiplicative structure. Let $G$ be any group, written multiplicatively; by

the *group with* 0 on $G$ we understand the set $G_0 = G \cup \{0\}$ with multiplication $xy$ as in $G$ for $x, y \neq 0$, while $x0 = 0x = 0$ for all $x \in G_0$.

LEMMA 1.1.1. *Let $G$ be a group and $G_0$ the group with 0 on $G$. Suppose that $\sigma: G_0 \to G_0$ is a map such that $e\sigma = 0$ for some $e \in G$ and further,*

(i) $0\sigma = 1$, *where 1 is the neutral element of $G$,*
(ii) $(y^{-1}xy)\sigma = y^{-1} \cdot x\sigma \cdot y$ *for all $x, y \in G$,*
(iii) $[(xy^{-1})\sigma \cdot y]\sigma = ([x\sigma \cdot y^{-1}]\sigma)y$ *for all $x \in G_0$, $y \in G$.*

*Then $G_0$ is a field with respect to its multiplication and the addition*

$$x + y = \begin{cases} (xy^{-1})\sigma \cdot y & \text{if } y \neq 0, \\ x & \text{if } y = 0. \end{cases} \tag{1}$$

*Proof.* By (1), $x + 0 = x$, $0 + x = (0x^{-1})\sigma \cdot x = 1 \cdot x = x$ for $x \neq 0$. Now with the help of (1), (iii) may be written as

$$(x + y)\sigma = x\sigma + y.$$

Further, (1) shows that $x\sigma = x + 1$, hence

$$(x + y) + 1 = (x + 1) + y. \tag{2}$$

Now the definition (1) shows that for $yz \neq 0$,

$$xz + yz = [(xz(yz)^{-1})\sigma]yz = (xy^{-1} \cdot \sigma)yz = (x + y)z,$$

hence

$$(x + y)z = xz + yz. \tag{3}$$

This has been shown to hold for $y, z \neq 0$. If $z = 0$, both sides reduce to 0, while for $y = 0$, both become $xz$, so (3) holds identically in $G_0$.

Next we have to prove

$$z(x + y) = zx + zy. \tag{4}$$

If one of $x, y, z$ is 0, this is clear; otherwise we have by (ii),

$$\begin{aligned} zx + zy = (zx \cdot y^{-1}z^{-1})\sigma \cdot zy &= z(xy^{-1}\sigma)z^{-1} \cdot zy \\ &= z(xy^{-1}\sigma)y \\ &= z(x + y) \end{aligned}$$

and (4) follows.

Next we have, by (2),

$$(xz^{-1} + yz^{-1}) + 1 = (xz^{-1} + 1) + yz^{-1};$$

multiplying on the right by $z$ and using (3) twice, we find

$$(x + y) + z = (x + z) + y, \tag{5}$$

at least when $z \neq 0$, but for $z = 0$ it holds trivially. Taking $x = 0$, we find that $y + z = z + y$, hence addition is commutative and so (5) can be rewritten to give the associative law:

$$(x + y) + z = x + (y + z).$$

Finally, for $x \neq 0$, we have

$$ex + x = (ex \cdot x^{-1})\sigma \cdot x = 0 \cdot x = 0.$$

Thus $x$ has the additive inverse $ex$, and this is true even when $x = 0$ and $e0 = 0$. This shows $G_0$ to be a group under addition, with neutral element 0. In particular, $e$ is the additive inverse of 1 and writing $-1$ for $e$, we obtain the usual notation for a field. ■

**Exercises**

1. Show that every near field with fewer than nine elements is a field (for a near field on nine elements, see Ex. 4).

2. Show that if in Lemma 1.1, (ii) is omitted, we obtain a near field.

3. Let $K$ be any field with a subgroup $P$ of index 2 in $K^\times$ and with an automorphism of order 2, $x \mapsto x'$, mapping $P$ into itself. Define a new multiplication on $K$ by the rule

$$x \circ y = \begin{cases} xy & \text{if } x \in P, \\ xy' & \text{if } x \notin P. \end{cases}$$

Verify that $K$ with this multiplication is a near field which is not a field.

4. (Dickson [05]) Apply Ex. 3 to construct a near field on any field of $p^2$ elements, where $p$ is an odd prime.

5. (Ferrero [68]) Let $\Gamma$ be an additive group with a group $G$ acting on it by fix-point-free automorphisms (i.e. $\alpha g = \alpha$ for $\alpha \in \Gamma$, $g \in G$ implies $\alpha = 0$ or $g = 1$). Let $\Delta_i$ $(i \in I)$ be a family of orbits $\neq \{0\}$ in $\Gamma$, with representatives $\delta_i$ and on $\Gamma$ define a multiplication by putting $\alpha \circ \beta = \beta g_\alpha$ if $\alpha \in \Delta_i$ and $g_\alpha$ is the unique element of $G$ satisfying $\delta_i g_\alpha = \alpha$; otherwise, i.e. if $\alpha \notin \Delta_i$ for all $i$, put $\alpha \circ \beta = 0$. Verify that except for lacking a one, $\Gamma$ is a near ring. (This shows that every group $\Gamma$ is the additive group of some near ring, possibly lacking a one.)

6. Show that in any ordered field (see 9.6) the set of all non-negative elements, with the operation $x\sigma = x + 1$, satisfies the conditions (i)–(iii) of Lemma 1.1 (this shows that the condition $e\sigma = 0$ cannot be omitted).

7. Show that any element of a ring having both a left inverse and a right inverse has a unique two-sided inverse.

8. (Kohn and Newman [71]) Show that in any field $K$ of characteristic $\neq 2$ the following identity holds:

$$[(x+y-2)^{-1}-(x+y+2)^{-1}]^{-1}-[(x-y-2)^{-1}-(x-y+2)^{-1}]^{-1}=\tfrac{1}{2}(xy+yx).$$

Why cannot $xy$ be expressed in this way unless $K$ is commutative?

9. In any ring show that if $1-xy$ is a unit, then so is $1-yx$. (Hint. Use elementary transformations to transform $\mathrm{diag}(1, 1-xy)$ to $\mathrm{diag}(1-yx, 1)$.)

10. Show that the centralizer of any subset of a field is a subfield.

## 1.2 The general embedding problem

A basic difference between groups and rings on the one hand and fields on the other is that the former, but not the latter, form a *variety*, i.e. a class defined by identical relations (see A.3, 1.3). In particular, a group may be described by generators and defining relations and any set of generators and relations yields a group; similarly for rings, whereas a given set of (ring) generators and defining relations cannot always be realized in a field. The usual method of obtaining a field, especially a skew field, is as field of fractions of a ring. This makes it important to study methods of embedding rings in fields. In this section we shall make some general observations on the embedding problem, and we begin by introducing some terminology.

Let $R$ be a ring; by a *field of fractions* of $R$ we understand a field $K$ together with an embedding $R \to K$ such that $K$ is the field generated by the image of $R$. Our task then is to find when a ring has a field of fractions. For commutative rings the answer is easy (and well known). It falls into three parts:

(i) Existence. A field of fractions exists for a ring $R$ if and only if $R$ is an *integral domain*, i.e. the set $R^\times = R\backslash\{0\}$ is non-empty and closed under multiplication.

(ii) Uniqueness. When a field of fractions exists, it is unique up to a unique isomorphism, thus given two fields of fractions of $R$, $\lambda_i: R \to K_i$ $(i = 1, 2)$, there exists a unique isomorphism $\varphi: K_1 \to K_2$ such that $\lambda_1\varphi = \lambda_2$.

(iii) Normal form. Each element of the field of fractions can be written in the form $a/b$, where $a, b \in R$, $b \neq 0$, and $a/b = a'/b'$ if and only if $ab' = ba'$.

Of course this is not really a 'normal form'; only in certain cases such as $\mathbf{Z}$ or $k[x]$ is there a canonical representative for each fraction (see also Ex. 1).

Let us now pass to the non-commutative case. The absence of zero-divisors is still necessary for a field of fractions to exist, but not sufficient. The first counter-example was found by Malcev [37], who writes down a semigroup whose semigroup ring over $\mathbf{Z}$ is an integral domain but cannot be embedded in a field (see Ex. 3 below). Malcev expressed his example as a cancellation semigroup not embeddable in a group, and it prompted him to ask for a ring $R$ whose set $R^\times$ of non-zero elements can be embedded in a group, but which cannot itself be embedded in a field. This question was answered affirmatively nearly 30 years later, in 1966, and will be dealt with in 5.7 below.

After giving his example, Malcev went on in a remarkable pair of papers (Malcev [39]) to provide a set of necessary and sufficient conditions for a semigroup to be embeddable in a group. This is an infinite set of conditions, and Malcev showed that no finite subset could be sufficient. The first two conditions express cancellability:

$$xy = xz \Rightarrow y = z, \quad yx = zx \Rightarrow y = z; \tag{1}$$

next came the condition (using $\wedge$ to mean 'and'):

$$ax = by \wedge cx = dy \wedge au = bv \Rightarrow cu = dv. \tag{2}$$

The other conditions were similar, but more complicated (Malcev [39], or UA, VII. 3), and they were all of the form

$$A_1 \wedge A_2 \wedge \ldots \wedge A_n \Rightarrow B, \tag{3}$$

where $A_1, \ldots, A_n, B$ are certain equations, with the universal quantifier $\forall$ for all the variables prefixed. Such a condition (3) is called a *quasi-identity* or a *universal Horn sentence*; when the $A$s are missing, we have an *identity*.

As a matter of fact it follows from general principles of universal algebra that the class of semigroups embeddable in groups is a *quasi-variety*, i.e. definable by quasi-identities. For it can be shown to be a *universal class* (definable by sentences with universal quantifiers over all variables, i.e. universal sentences), and one has the following theorem (see e.g. UA, VI. 4):

*A class of algebras is a quasi-variety if and only if it is universal and admits direct products, or equivalently, if and only if it admits direct products and subalgebras.*

We remark that such a class always contains the one-element subalgebra, as the product of the empty family. With the help of this result it is not hard to check that the class of semigroups embeddable in groups is a quasi-variety. At the same time we see that integral domains do not form a quasi-variety, since they do not admit direct products, and neither do rings embeddable in fields. Nevertheless they come very close to being a quasi-variety. To be precise, if $\mathfrak{D}$ denotes the class of integral domains, $\mathfrak{F}$ the class of fields and $s\mathfrak{F}$ the class of subrings of fields, then there is a quasi-variety $\mathfrak{Q}$ such that

$$s\mathfrak{F} = \mathfrak{D} \cap \mathfrak{Q}. \tag{4}$$

To find $\mathfrak{Q}$, we recall some definitions. A ring $R$ is called *regular* (in the sense of von Neumann) if for any $a \in R$ there exists $x \in R$ such that $axa = a$. If for each $a \in R$ there exists $x \in R$ such that $a^2x = a$, $R$ is said to be *strongly regular*. Despite its appearance, the condition of strong regularity is left–right symmetric, as the next lemma shows. We recall that a ring is said to be *reduced*, if it contains no nilpotent elements $\neq 0$, i.e. $x^2 = 0$ implies $x = 0$.

LEMMA 1.2.1. *A ring is strongly regular if and only if it is regular and reduced.*

*Proof.* Assume that $R$ is strongly regular. If $a^2 = 0$, take $x$ to satisfy $a^2x = a$; then $0 = a^2x = a$, so $R$ is reduced. Moreover, for any $a \in R$ and for $x \in R$ such that $a^2x = a$, we have

$$\begin{aligned}(axa - a)^2 &= axa^2xa - axa^2 - a^2xa + a^2\\ &= axa^2 - axa^2 - a^2 + a^2 = 0,\end{aligned}$$

hence $axa - a = 0$ and this shows $R$ to be regular.

Conversely, if $R$ is regular and reduced, let $a \in R$ and take $x \in R$ such that $axa = a$. Then

$$\begin{aligned}(a^2x - a)^2 &= a^2xa^2x - a^2xa - a^3x + a^2\\ &= a^3x - a^2 - a^3x + a^2 = 0,\end{aligned}$$

hence $a^2x - a = 0$ and so $R$ is strongly regular. ■

Now any regular ring $R$ is *semiprimitive*, i.e. its Jacobson radical $\mathfrak{J}$ is zero. For if $a \in \mathfrak{J}$ and $axa = a$, then $a(xa - 1) = 0$ and $xa - 1$ is a unit, by the definition of $\mathfrak{J}$, so $a = 0$. It follows that $R$ is a subdirect product of primitive rings, which as homomorphic images of $R$ are again regular (see A.3, Th. 10.4.1, p. 405). Now any primitive ring is clearly prime (A.3,