Cambridge University Press
978-0-521-27274-2 - Skew Fields
P. K. Draxl
Excerpt
More information

PART I . SKEW FIELDS AND SIMPLE RINGS

The history of skew fields begins with quaternions, whose discovery W.R. Hamilton (1805-1865) regarded as the climax of his career. F. Klein [1926/27,p.184 in vol.1] writes in his famous treatise "Vorlesungen über die Entwicklung der Mathematik im 19. Jahrhundert" (which is an outstanding account):

> ...
>
> Von hier aus entwickelte sich nun bei Hamilton das größte Interesse an der Fragestellung, ob man die nützliche, geometrische Interpretation des Rechnens mit $x + iy$ in der Ebene nicht irgendwie - durch Schaffung neuer komplexer Zahlen - auf den Raum, d.h. unsern gewöhnlichen R_3, übertragen könne. Seine unermüdlichen Anstrengungen führen ihn endlich 1843 zur Erfindung der *Quaternionen*, d.h. geeigneter viergliedriger Zahlen, deren Erforschung und Verbreitung er sich fortan ausschließlich widmete. Ihre Theorie legte er dar in den beiden ausführlichen Werken:
>
> *Lectures on Quaternions*, Dublin 1853
> *Elements on Quaternions*, London 1866 (posthum).
>
> Sehr bald wurden die Quaternionen in Dublin ein alles andere überragender Gegenstand des mathematischen Interesses, ja sogar ein offizielles Examensfach, ohne dessen Kenntnis keine Absolvierung des College mehr denkbar war. Hamilton selbst gestaltete sie für sich zu einer Art orthodoxer Lehre des mathematischen Credo, in die er alle seine geometrischen und sonstigen Interessen hineinzwang, je mehr sich gegen Ende seines Lebens sein Geist vereinseitigte und unter den Folgen des Alkohols verdüsterte.
>
> ...

In Part I of these lectures we start with a brief description of Hamilton's quaternions; however, we do not take his point of view since

Cambridge University Press
978-0-521-27274-2 - Skew Fields
P. K. Draxl
Excerpt
More information

we use a definition involving matrices and these were only later introduced into mathematics by A. Cayley (1821-1895) in 1855. All this is done in §1. which also includes some remarks on (skew) formal Laurent series fields introduced by D. Hilbert (1862-1943) in 1898. (Later, in Part II. (§ 14.) we shall come back to the quaternions from a more abstract point of view.)In §§2/3 we develop a theory of simple rings as suggested by E. Artin (1898-1962) in the late 1920's; important special cases of the material presented here have been introduced by J.H.M. Wedderburn (1882--1948) as early as 1907. In §§4/5/6 we discuss certain techniques involving tensor products which are relevant to our subject. §7. contains the backbone of these lectures, the Skolem-Noether Theorem, proved in 1927 by T. Skolem (1887-1963) and rediscovered in 1933 by E. Noether (1882--1935); we treat this theorem in a setting which goes back to E. Artin and G. Whaples (1914-1981). We close Part I with a discussion of the corestriction of algebras intruduced by C. Riehm [1970]; here (in §8.) we present only a simplified version which is sufficient for our purposes.

Roughly speaking one may say that §§2,..,7 comprise a slightly modified and modernized version of the first seven chapters of the classical set of notes by E. Artin *et al.* [1948]; however, in our lectures we do not discuss (and make no use of) semisimple rings; those interested in such things may consult for example C.W. Curtis & I. Reiner [1962] or vol. 2 of P.M. Cohn [1974/77] (cf. also some of the exercises).

§ 1 . SOME AD HOC RESULTS ON SKEW FIELDS

Consider the set of matrices

$$(1) \qquad H := \left\{ \begin{pmatrix} z & u \\ -\bar{u} & \bar{z} \end{pmatrix} \middle| \; z,u \in C \right\} \subseteq M_2(C)$$

where $\bar{z}$ denotes the complex conjugate of $z \in C$. An easy calculation shows that H is in fact a ring with unit element the unit matrix 1 . If $\begin{pmatrix} z & u \\ -\bar{u} & \bar{z} \end{pmatrix} \neq 0$, i.e. $|z|^2+|u|^2 \neq 0$, then

$$\begin{pmatrix} z & u \\ -\bar{u} & \bar{z} \end{pmatrix}^{-1} = (|z|^2+|u|^2)^{-1} \begin{pmatrix} \bar{z} & -u \\ \bar{u} & z \end{pmatrix} \in H \quad ,$$

hence H is even a skew field, called the skew field of (*ordinary* or *real*) *quaternions* . Of course, H is a 4-dimensional R-vector space with basis

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} , \; i := \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} , \; j := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} , \; k := \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

with the usual $i \in C$ satisfying $i^2 = -1$. The elements $1,i,j,k$ satisfy the multiplication table on the right. Usually one writes $a1 + bi + cj + dk$ in place of $\begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix}$ ($a,b,c,d \in R$) .

1	i	j	k
i	-1	k	$-j$
j	$-k$	-1	i
k	j	$-i$	-1

Obviously the eight elements $1,i,j,k,-1,-i,-j,-k \in H^*$ form a finite subgroup of the multiplicative group H^* of our skew field H - called the *Quaternion Group* - which clearly is non commutative and hence not a cyclic group; this could never happen in a commutative field since any finite subgroup of the multiplicative group of a commutative field is necessarily cyclic (cf. Field Theory). Moreover the equation $X^2 + 1 = 0$ obviously has the six solutions $i,j,k,-i,-j,-k \in H$; over a commutative field it could have at most two solutions. Here the above equation even has an infinite number of solutions: choose $b, c, d \in R$ such that $b^2 + c^2 + d^2 = 1$, then a straightforward calculation shows $(bi + cj + dk)^2 = .. = -1$. This phenomenon will be understood later (cf. Example 1 in §7.).

Now consider the injection $R \to H$, $t \mapsto t1$; this makes R a commutative subfield of the skew field H such that $R \subseteq Z(H)$, but even $R = Z(H)$ holds:
indeed, assume $\begin{pmatrix} z & u \\ -\bar{u} & \bar{z} \end{pmatrix} \in Z(H)$, hence $\begin{pmatrix} z & u \\ -\bar{u} & \bar{z} \end{pmatrix} \begin{pmatrix} 0 & v \\ -\bar{v} & 0 \end{pmatrix} =$
$= \begin{pmatrix} 0 & v \\ -\bar{v} & 0 \end{pmatrix} \begin{pmatrix} z & u \\ -\bar{u} & \bar{z} \end{pmatrix}$ for all $v \in C$. This amounts to $vz = v\bar{z}$ and $u\bar{v} = \bar{u}v$ for all $v \in C$, hence $z \in R$ and $u = 0$. Therefore we have $|H:Z(H)| = |H:R| = 4 = 2^2$. The fact that $Z(H)$ is a field is not surprising, in fact we have

Lemma 1 . *Let* D *be a skew field, then* Z(D) *is a commutative subfield of* D .

Proof. Obviously $Z(D)$ is a subring and even a field since $zd = dz$ for all $d \in D$ clearly implies $d^{-1}z^{-1} = z^{-1}d^{-1}$ for all $d \in D$ ($z, d \neq 0$) for any given $z \in Z(D)$. □

The above example may be generalized as follows: replace the extension C/R by an arbitrary separable quadratic extension L/K , select some $a \in K^*$ and consider the set of matrices

$$(2) \qquad D := D_a(L/K) := \left\{ \begin{pmatrix} z & u \\ a\bar{u} & \bar{z} \end{pmatrix} \middle| \ z, u \in L \right\} \subseteq M_2(L)$$

where $\bar{z}$ denotes the conjugate of $z \in L$. Again D is a ring, and an easy calculation shows that

$\begin{pmatrix} z & u \\ a\bar{u} & \bar{z} \end{pmatrix}^{-1}$ exists if and only if $z\bar{z} - au\bar{u} \neq 0$, i.e. if and only if a is *not* a norm for the extension L/K.

Moreover we have the formula

$$\begin{pmatrix} z & u \\ a\bar{u} & \bar{z} \end{pmatrix}^{-1} = (z\bar{z} - au\bar{u})^{-1} \begin{pmatrix} \bar{z} & -u \\ -a\bar{u} & z \end{pmatrix} ,$$

provided either side exists. Again D is a 4-dimensional K-algebra with $Z(D) = K$ (here, as above, we identify $t \in K$ with $t1 \in D$); this follows in the same way as in the case of the real quaternions.

Summarizing our remarks gives

Lemma 2 . $D = D_a(L/K)$ according to (2) *is a 4-dimensional* K*-algebra with centre* K *, and it is a skew field if and only if* a *is not a norm for the extension* L/K . □

Let us now study another classical example: let L be a commutative field and σ an automorphism of L . Call $K := \mathrm{Fix}_L(\sigma) := = \{ x \in L \mid \sigma(x) = x \}$ the fixed field of σ in L .

Definition 1 . *Denote by* $L((T;\sigma))$ *the ring of formal Laurent series* $\sum_{i=R}^{\infty} a_i T^i$ *in the indeterminate* T *with coefficients* $a_i \in L$ ($R \in \mathbb{Z}$) , *with usual addition but skew multiplication such that* $Ta = \sigma(a)T$, i.e. $T^i a = \sigma^i(a) T^i$ ($a \in L$).

If $\sigma = \mathrm{id}_L$ then $L((T;\sigma))$ is the usual commutative field of formal Laurent series over L in T , customarily denoted $L((T))$. We want to show that $L((T;\sigma))$ is always a skew field: indeed, let $0 \neq d = = \sum_{i=R}^{\infty} a_i T^i$ ($a_R \neq 0$) be given, let us calculate its inverse

$$d^{-1} = \sum_{j=S}^{\infty} x_j T^j \quad (x_S \neq 0)$$

where $S \in \mathbb{Z}$ and the $x_j \in L$ are not yet known. We have necessarily

$$T^0 = 1 = (\sum_{j=S}^{\infty} x_j T^j)(\sum_{i=R}^{\infty} a_i T^i) =$$

$$= \sum_{r=R+S}^{\infty} (\sum_{i+j=r} x_j \sigma^j(a_i)) T^r \quad ,$$

hence $R + S = 0$, i.e. $S = -R$. Comparing coefficients at $r = 0$ gives

$$(3) \qquad x_{-R} = \sigma^{-R}(a_R{}^{-1}) \neq 0 \quad ;$$

doing the same for $r \geq 1$ we get immediately

$$0 = \sum_{i+j=r} x_j \sigma^j(a_i) = \sum_{j=-R}^{-R+r} x_j \sigma^j(a_{r-j}) \quad ,$$

i.e. the recurrence relations

$$(4) \qquad x_{-R+r} = - \sigma^{-R+r}(a_R{}^{-1}) \sum_{j=-R}^{-R+r-1} x_j \sigma^j(a_{r-j}) \quad (r \geq 1) \quad .$$

Hence for $d \neq 0$ we may calculate the coefficients x_j of its inverse d^{-1} successively with the aid of (3) and (4). Therefore we have proved

Lemma 3 . *The ring* $L((T;\sigma))$ according to Definition 1 *is a skew field* . □

Now let L again be a commutative field (cf. Lemma 2 in §24.), then:

Lemma 4 . *Let* $D := L((T;\sigma))$ *be given. If* σ *has infinite order, then* $Z(D) = K$, *hence* $|D:Z(D)| = \infty$; *if* σ *has the finite order* n *in* $\mathrm{Aut}(L)$, *then* $Z(D) = K((T^n))$, *hence* $|D:Z(D)| = n^2$ ($K = \mathrm{Fix}_L(\sigma)$) .

Proof. "$\supseteq$" is obvious in both cases; let us prove the converse: pick an element

$$z = \sum_{i=R}^{\infty} z_i T^i \in Z(D) \text{ , i.e. } az = za \text{ for all } a \in D \text{ .}$$

Set $a = \sum_{j=S}^{\infty} a_j T^j$ ($a_S \neq 0$, because we may assume $a \neq 0$) , then $az =$ $= za$ amounts to

$$\sum_{r=R+S}^{\infty} \Big(\sum_{i+j=r} a_j \sigma^j(z_i) \Big) T^r = \Big(\sum_{j=S}^{\infty} a_j T^j\Big)\Big(\sum_{i=R}^{\infty} z_i T^i\Big) = az = za =$$

$$= \Big(\sum_{i=R}^{\infty} z_i T^i\Big)\Big(\sum_{j=S}^{\infty} a_j T^j\Big) = \sum_{r=R+S}^{\infty} \Big(\sum_{i+j=r} z_i \sigma^i(a_j) \Big) T^r \text{ ,}$$

hence

$$(5) \qquad \sum_{j=S}^{-R+r} z_{r-j}\sigma^{r-j}(a_j) = \sum_{j=S}^{-R+r} a_j \sigma^j(z_{r-j}) \text{ for all } r \geq R+S \text{ .}$$

Now take in (5) $S := 1$, $a_1 := 1$ and $a_j := 0$ for $j \geq 2$. It follows $z_{r-1} = \sigma(z_{r-1})$ for all $r-1$, hence $z_r \in \mathrm{Fix}_L(\sigma) = K$ for all r , therefore

$$Z(D) \subseteq K((T)) \text{ in any case.}$$

Let us now suppose that σ has infinite order in Aut(L) . Take in (5) $S := 1$, $a_1 \in L$ such that $\sigma^{r-1}(a_1) \neq a_1$ for any $r \neq 1$, and $a_j := 0$ for $j \geq 2$. It follows that $z_{r-1}\sigma^{r-1}(a_1) = a_1\sigma(z_{r-1}) = a_1 z_{r-1}$; by construction of a_1 this means $z_{r-1} = 0$, and this implies

$$z_r = 0 \text{ for all } r \neq 0 \text{ , i.e. } z = z_0 T^0 = z_0 \in K \text{ .}$$

Finally, if σ has the finite order n , we proceed as follows: take in (5) $S := 1$, $a_1 \in L$ such that $\sigma^{r-1}(a_1) \neq a_1$ for all $r \not\equiv 1$ (*mod* n) , and $a_j := 0$ for $j \geq 2$. Just like in the previous case it follows that $z_{r-1}\sigma^{r-1}(a_1) = a_1\sigma(z_{r-1}) = a_1 z_{r-1}$ for all these r ; again by our choice of a_1 this amounts to $z_{r-1} = 0$, hence

$$z_r = 0 \text{ for all } r \not\equiv 0 \ (\mathit{mod}\ n) \text{ , i.e. } z \in K((T^n)) \text{ .}$$

It remains to calculate the dimension $|D:Z(D)|$ in the latter case: first we observe $|L:K| = n$ (see Galois Theory, in particular Artin's Lemma (cf. also §6.) for L/K is obviously cyclic with generating automorphism σ . Now choose a basis $\{1,t,t^2,..,t^{n-1}\}$ of L as a K-space, then our considerations show immediately that $\{ t^i T^j \mid 0 \leq i,j < n \}$ is a basis of D as a $K((T^n))$-space, hence $|D:Z(D)| = n^2$. □

Let us note that so far we have only seen skew fields D such that the dimension $|D:Z(D)|$ is either infinite or a square. Later we shall learn that nothing else is possible (cf. §5.).

Exercise 1 . Call $a\mathit{1}$ (resp. $b\mathit{i} + c\mathit{j} + d\mathit{k}$) the scalar (resp. pure) component of a quaternion $a\mathit{1} + b\mathit{i} + c\mathit{j} + d\mathit{k} \in H$ ($a,b,c,d \in R$) and identify the scalar (resp. pure) quaternions - i.e. those with vanishing pure (resp. scalar) component - with the elements in R (resp. R^3). Now show that the scalar (resp. pure) component of the product of two pure quaternions equals the negative scalar product (resp. the vector product) of these two quaternions (viewed as vectors in R^3) .

Exercise 2 . Study the first two chapters of P.M. Cohn [1977].

§ 2 . RINGS OF MATRICES OVER SKEW FIELDS

Let R be a ring with $1 \neq 0$. We shall henceforth deal with right(left) R-modules $M \neq \{0\}$.

Definition 1 . *A right(left)* R*-module* M *is called "simple" (or "irreducible") if* M *contains no proper right(left)* R*-submodules;* M *is called "right(left) Noetherian[Artinian]" if every increasing[decreasing] sequence of right(left)* R*-submodules of* M *is necessarily finite.*

Definition 2 . *If in* Definition 1 *we are in the special case* $M = R$, *then we say "right(left) ideal of* R *" rather than right(left)* R*-submodule of* R *; also we say "minimal" right(left) ideal rather than simple right(left) ideal.*

Now let D be a skew field and consider the full matrix ring $M_n(D)$; it is an n^2-dimensional right(left) vector space over D with basis

$$e_{ij} := \begin{array}{cc} \downarrow \text{ j-th column} & \\ \begin{pmatrix} & & \\ & 1 & \\ & & \end{pmatrix} & \leftarrow \text{ i-th row} \end{array} \qquad (1 \leq i,j \leq n)$$

containing one 1 and n^2-1 0's .

The above basis elements multiply according to

$$e_{ij}e_{rs} = \begin{cases} 0 & \text{in case } j \neq r \\ e_{is} & j = r \end{cases} .$$

Call $1 := \sum_{i=1}^{n} e_{ii}$ the unit matrix . Then we may consider the *elementary matrices*

$$E_{ij}(t) := 1 + te_{ij} = \begin{array}{cc} \downarrow \text{ j-th column} & \\ \begin{pmatrix} 1 & & \\ t & \ddots & \\ & & 1 \end{pmatrix} & \leftarrow \text{ i-th row} \end{array}$$

$$(t \in D ; i \neq j ; 1 \leq i,j \leq n) .$$

It is well-known from Linear Algebra that these elementary matrices have the following properties (most of which are fairly obvious):

(1) $$E_{ij}(t)E_{ij}(t') = E_{ij}(t+t') \ , \ E_{ij}(0) = 1 \ , \ E_{ij}(t)^{-1} = E_{ij}(-t) \ ,$$

(2) $$E_{ij}(t)E_{rs}(t') = E_{rs}(t')E_{ij}(t) \quad (j \neq r \neq s \neq i \neq j)$$

and

(3) $$E_{ij}(tt') = E_{ir}(t)^{-1}E_{rj}(t')^{-1}E_{ir}(t)E_{rj}(t') \quad (r \neq i \neq j \neq r) \ .$$

Furthermore we introduce matrices

$$D_i(u) := 1 + (u-1)e_{ii} = \begin{array}{cc} \downarrow & \text{i-th column} \\ \begin{pmatrix} 1 & & 0 \\ & u & \\ 0 & & 1 \end{pmatrix} & \leftarrow \text{i-th row} \end{array}$$

$$(u \in D^* \ ; \ 1 \leq i \leq n)$$

with the properties

(4) $$D_i(u)D_i(u') = D_i(uu') \ , \ D_i(1) = 1 \ , \ D_i(u)^{-1} = D_i(u^{-1})$$

and

(5) $$D_i(u)D_j(u') = D_j(u')D_i(u) \quad (i \neq j) \ .$$

Finally we assign to every permutation $\pi \in S_n$ of n ciphers a matrix

$$P(\pi) := \begin{array}{cc} \left(\ \delta_{i,\pi(j)} \ \right) & \leftarrow \text{i-th row} \\ \uparrow & \text{j-th column} \end{array}$$

$$\text{where} \quad \delta_{i,\pi(j)} = \begin{matrix} 1 \\ 0 \end{matrix} \quad \text{if} \quad \begin{matrix} i = \pi(j) \\ i \neq \pi(j) \end{matrix} \ .$$

Obviously in each row and each column of such a *permutation matrix* there is exactly one 1 and $n-1$ 0's . Moreover one checks easily

(6) $$P(\pi)P(\pi') = P(\pi\pi') \ , \ P(id) = 1 \ , \ P(\pi)^{-1} = P(\pi^{-1}) = P(\pi)^t \ .$$

In this context the following is well-known from Linear Algebra:

Lemma 1 . *Given* $A \in M_n(D)$ *then the "elementary row(column) operations" are as follows:*

transforming from A *to*		*amounts to*
$E_{ij}(t)A$	($AE_{ji}(t)$)	*adding the left(right)* t*-multiple of the* j*-th row(column) to the* i*-th row(column)* ;
$D_i(u)A$	($AD_i(u)$)	*multiplying the* i*-th row(column) from the left(right) by* u ;
$P(\pi)A$	($AP(\pi)^{-1}$)	*moving the* i*-th row(column) into the position of the* $\pi(i)$*-th row(column)* .

□

Example 1 . Transforming from A to $\begin{pmatrix} 0 & & 1 \\ & \diagup & \\ 1 & & 0 \end{pmatrix} A \begin{pmatrix} 0 & & 1 \\ & \diagup & \\ 1 & & 0 \end{pmatrix}$ amounts to rotating the matrix A by 180 degrees (Note: this is different from going over to the transpose A^t).

Example 2 .
If we have $A = \Big(\overset{\text{j-th column}}{\overset{\downarrow}{a_{ij}}} \Big) \leftarrow \text{i-th row}$, then we get for every $\pi \in S_n$

$$P(\pi)^{-1}AP(\pi) = \Big(\underset{\text{j-th column}}{\underset{\uparrow}{a_{\pi(i),\pi(j)}}} \Big) \leftarrow \text{i-th row} \quad .$$

Lemma 2 . *Let* $A = M_n(D)$ *be the full matrix ring over a skew field* D *; then the set of matrices in* A *which commute with all elementary matrices* $E_{ij}(t)$ *is exactly the set of matrices of the form* $z1$ *where* $z \in Z(D)$ *; in particular: the mapping* $d \mapsto d1$ *from* D *into* A *induces an isomorphism* $Z(D) \simeq Z(A)$.

Proof. Obviously it suffices to prove the first statement. Call $K := Z(D)$ and note that K is a commutative field (cf. Lemma 1 in §1.; the reader should notice that we do not use this fact in the course of this proof). Clearly we get $z1 \in Z(A)$ for all $z \in K$. Conversely assume that the matrix $A = (a_{rs})$ commutes with all matrices $E_{ij}(t)$; then

$$B := (b_{rs}) := AE_{ij}(t) = E_{ij}(t)A \quad .$$

Equating the main diagonal of B gives

$$a_{jj} = b_{jj} = a_{jj} + a_{ji}t \quad \text{for all} \quad t \in D \text{ , hence}$$

$$a_{ji} = 0 \quad \text{for all} \quad i \neq j \text{ , i.e. } A \text{ is a diagonal matrix.}$$

On the other hand, equating the (i,j)-th position of B gives the relation

$$a_{ij} + ta_{ii} = b_{ij} = a_{jj}t + a_{ij} \quad \text{for all} \quad t \in D \text{ , hence}$$

$z := a_{ii} = a_{jj} \in D$ for $i \neq j$ (take $t = 1$ and note $a_{ij} =$ $= 0$ according to the above) and therefore $tz = zt$ for all $t \in D$, i.e. $z \in Z(D) = K$.

All this implies $A = z1$. □

So far we have not made use of the fact that D is a skew field; in fact we could replace it *mutatis mutandis* by any ring R with $1 \neq 0$. For the rest of this paragraph, however, we have to use the field property of D .