Nathan
Jacobson

Finite-Dimensional Division Algebras over Fields

Springer

Nathan Jacobson

Finite-Dimensional Division Algebras over Fields

Springer

Nathan Jacobson
Yale University
Department of Mathematics
10 Hillhouse Avenue
New Haven, CT 06520-8283
USA

Library of Congress Cataloging-in-Publication Data

Jacobson, Nathan, 1910-
Finite-dimensional division algebras over fields / Nathan Jacobson.
p. cm.
Includes bibliographical references (p. -).
ISBN 3-540-57029-2 (Berlin : hardcover : alk. paper)
1. Division algebras. 2. Fields (Algebra). I. Title.
QA247.45.J33 1996
512'.24--dc20 96-31625
CIP

Mathematics Subject Classification 1991): 13-xx, 16-xx, 17-xx

ISBN 3-540-57029-2 Springer-Verlag Berlin Heidelberg New York

Printed in Germany

Typeset from the author's output file
using a Springer $\mathrm{T_EX}$ macro package
SPIN: 10078372 41/3143-543210 - Printed on acid-free paper.

Nathan Jacobson Finite-Dimensional Division Algebras over Fields

PREFACE

These algebras determine, by the Wedderburn Theorem, the semi-simple finite dimensional algebras over a field. They lead to the definition of the Brauer group and to certain geometric objects, the Brauer-Severi varieties.

We shall be interested in these algebras which have an involution. Algebras with involution arose first in the study of the so-called "multiplication algebras of Riemann matrices". Albert undertook their study at the behest of Lefschetz. He solved the problem of determining these algebras. The problem has an algebraic part and an arithmetic part which can be solved only by determining the finite dimensional simple algebras over an algebraic number field. We are not going to consider the arithmetic part but will be interested only in the algebraic part. In Albert's classical book (1939), both parts are treated. A quick survey of our Table of Contents will indicate the scope of the present volume.

The largest part of our book is the fifth chapter which deals with involutorial simple algebras of finite dimension over a field.

Of particular interest are the Jordan algebras determined by these algebras with involution. Their structure is determined and two important concepts of these algebras with involution are the universal enveloping algebras and the reduced norm. Of great importance is the concept of isotopy. There are numerous applications of these concepts, some of which are quite old.

In preparing this volume we have been assisted by our friends, notably Jean-Pierre Tignol and John Faulkner. Also, I am greatly indebted to my secretary, Donna Belli, and to my wife, Florie. I wish to thank all of them for their help.

Table of Contents

I. Skew Polynomials and Division Algebras

We assume the reader is familiar with the standard ways of constructing "simple" field extensions of a given field F, using polynomials. These are of two kinds: the simple transcendental extension $F(t)$, which is the field of fractions of the polynomial ring $F[t]$ in an indeterminate t, and the simple algebraic extension $F[t]/(f(t))$ where $f(t)$ is an irreducible polynomial in $F[t]$. In this chapter we shall consider some analogous constructions of division rings based on certain rings of polynomials $D[t; \sigma, \delta]$ that were first introduced by Oystein Ore [33] and simultaneously by Wedderburn. Here D is a given division ring, σ is an automorphism of D, δ is a σ-derivation (1.1.1) and t is an indeterminate satisfying the basic commutation rule

$$ta = (\sigma a)t + \delta a \tag{1.0.1}$$

for $a \in D$. The elements of $D[t; \sigma, \delta]$ are (left) polynomials

$$a_0 + a_1 t + \cdots + a_n t^n, \qquad a_i \in D \tag{1.0.2}$$

where multiplication can be deduced from the associative and distributive laws and (1.0.1) (cf. Draxl [83]). We shall consider two types of rings obtained from $D[t; \sigma, \delta]$: homomorphic images and certain localizations (rings of quotients) by central elements. The special case in which $\delta = 0$ leads to cyclic and generalized cyclic algebras. The special case in which $\sigma = 1$ and the characteristic is $p \neq 0$ gives differential extensions analogous to cyclic algebras.

The rings $D[t; \sigma, \delta]$ are principal ideal domains, that is, they are rings without zero divisors in which all one-sided ideals are principal. We shall develop the necessary arithmetic of such domains and use this to derive results on cyclic and generalized cyclic algebras and their differential analogues.

1.1. Skew-polynomial Rings

Let R be a ring (with 1 and the usual conventions on homomorphisms and subrings of unital rings), σ a ring endomorphism of R, δ a left σ-derivation of R, that is, δ is additive and for $a, b, \in R$,

$$\delta(ab) = (\sigma a)(\delta b) + (\delta a)b \tag{1.1.1}$$

which implies $\delta(1) = 0$. Let $R[t;\sigma,\delta]$ be the set of polynomials

$$a_0 + a_1t + \cdots + a_nt^n \qquad (1.1.2)$$

where the $a_i \in R$ and equality and addition are defined as usual. In particular, t is transcendental over R in the sense that $a_0 + a_1t + \cdots + a_nt^n = 0 \Rightarrow a_i = 0, \quad 0 \leq i \leq n$. Evidently, $R[t;\sigma,\delta]$ is a free (left) R-module (with the obvious module structure). We wish to make $R[t;\sigma,\delta]$ into a ring in which we have the relation

$$ta = (\sigma a)t + \delta a, \qquad a \in R. \qquad (1.1.3)$$

Then associativity and the distributive laws imply that

$$t^na = \sum_{j=0}^{n}(S_{nj}a)t^j, \qquad n \geq 0 \qquad (1.1.4)$$

where S_{nj} satisfies the recursion formula

$$S_{nj} = \delta S_{n-1,j} + \sigma S_{n-1,j-1} \qquad (1.1.5)$$

and $S_{00} = 1_R$ (identity map), $S_{10} = \delta$, $S_{11} = \sigma$, by (1.1.3). It follows that $S_{nj}, \quad 0 \leq j \leq n$, is a sum of all the monomials in σ and δ that are of degree j in σ and of degree $n-j$ in δ, e.g.,

$$S_{nn} = \sigma^n, \ S_{n,n-1} = \sigma^{n-1}\delta + \sigma^{n-2}\delta\sigma + \cdots + \delta\sigma^{n-1}.$$

We now define

$$(at^n)(bt^m) = \sum_{j=0}^{n} a(S_{nj}b)t^{j+m} \qquad (1.1.6)$$

where S_{nj} is defined by (1.1.5) and $S_{00} = 1_R$, and we define products of polynomials in t by this and the distributive laws:

$$(\Sigma a_nt^n)(\Sigma b_mt^m) = \Sigma(a_nt^n)(b_mt^m).$$

To see that $R[t;\sigma,\delta]$ is a ring it suffices to check the associative law of multiplication. A direct verification of this is rather tedious. We shall prove associativity by using a representation by infinite row-finite matrices with entries in R. We denote the set of matrices whose rows are infinite sequences of elements of R with only a finite number of nonzero entries in each row by $M_\omega(R)$. It is well known and readily verified that this is a ring under the usual matrix compositions.

For $a \in R$ we define

$$a' = (S_{ij}a) = \left(\begin{array}{ccccccc} a & 0 & 0 & & & & \\ \delta a & \sigma a & 0 & \cdots & & & \\ \cdot & \cdot & \cdot & & & & \\ \cdot & \cdot & \cdot & \cdots & & & \\ S_{n0}a & S_{n1}a & \cdot & \cdots & S_{nn}a & 0 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{array}\right) \qquad (1.1.7)$$

and

$$t' = \sum_{1}^{\infty} e_{i,i+1} \tag{1.1.8}$$

where e_{ij} is the matrix in $M_\omega(R)$ with 1 in (i, j)-position and 0's elsewhere. Using (1.1.5) we can prove by induction on n the Leibniz formula

$$S_{nm}ab = \sum_{m \le j \le n} (S_{nj}a)(S_{jm}b) = \sum_{j=0}^{\infty} (S_{nj}a)(S_{jm}b) \tag{1.1.9}$$

where we take $S_{nj} = 0$ if $j > n$. This formula implies that $a \rightsquigarrow a'$ is a monomorphism of R onto a subring R' of $M_\omega(R)$. Direct verification shows also that $t'a' = (\sigma a)'t' + (\delta a)'$. This implies that $(a't'^n)(b't'^m) = \sum_{j=0}^{n} a'(S_{nj}b)'t'^{j+m}$. It follows that $\Sigma a_j t^j \rightsquigarrow \Sigma a_j' t'^j$ is a homomorphism of $R[t; \sigma, \delta]$ into $M_\omega(R)$. It is readily seen also that $\Sigma a_j' t'^j = 0 \Rightarrow a_j' = 0,\ j \ge 0$. This implies that we have a monomorphism of $R[t; \sigma, \delta]$ into $M_\omega(R)$ and hence that $R[t; \sigma, \delta]$ is a ring.

From now on we assume $R = D$ is a division ring. Then σ is a monomorphism. If $f(t) = a_0 + a_1 t + \cdots + a_n t^n$ with $a_n \ne 0$ we define deg $f(t) = n$. Also, we put deg $0 = -\infty$. If $g(t) = b_0 + b_1 t + \cdots + b_m t^m$, $b_m \ne 0$, then $f(t)g(t) = \cdots + a_n(\sigma^n b_m)t^{n+m}$ and $a_n(\sigma^n b_m) \ne 0$. Hence

$$\deg fg = \deg f + \deg g. \tag{1.1.10}$$

This implies that $D[t; \sigma, \delta]$ is a domain, that is, has no zero divisors $\ne 0$.

We establish next a left division algorithm in $D[t; \sigma, \delta]$, that for any $f(t), g(t) \in D[t; \sigma, \delta]$ with $g \ne 0$ there exist unique $q(t), r(t)$ with deg $r(t) <$ deg $g(t)$ such that

$$f(t) = q(t)g(t) + r(t). \tag{1.1.11}$$

Suppose $f(t) = a_0 + a_1 t + \cdots + a_n t^n$, $g(t) = b_0 + b_1 t + \cdots + b_m t^m$ where $b_m \ne 0$. If $n < m$ we have $f(t) = 0g(t) + f(t)$, and if $n \ge m$, we have

$$f(t) - a_n(\sigma^{n-m} b_m)^{-1} t^{n-m} g(t) = a_{n-1}' t^{n-1} + \cdots. \tag{1.1.12}$$

Hence the existence of $q(t)$ and $r(t)$ follow by induction on n. The uniqueness follow by degree considerations.

A ring R is called a *left (right) principal ideal domain* (abbreviated as left or right PID) if every left (right) ideal in R is principal, that is, has the form Ra (aR). The existence of the left division algorithm in $R = D[t; \sigma, \delta]$ implies in the usual way that R is a left PID.

A ring R is called *left noetherian* if it satisfies the ascending chain condition for left ideals. R is said to satisfy the *left Ore-Wedderburn condition* if given $a \in R$ and s regular in R (that is not a zero divisor) there exist $a_1 \in R$, s_1 regular in R such that $s_1 a = a_1 s$. For a domain this is equivalent to: $Ra \bigcap Rb \ne 0$ for any $a \ne 0,\ b \ne 0$.

Proposition 1.1.13. *If R is a domain we have the following implications: (i) R is a left PID $\Rightarrow$ (ii) R is left noetherian $\Rightarrow$ (iii) R satisfies the left Ore-Wedderburn condition.*

Proof. (i) $\Rightarrow$ (ii) is clear since (ii) is equivalent to the condition that every left ideal is finitely generated. To show that (ii) $\Rightarrow$ (iii), let a and b be non-zero elements of R. We have the ascending chain of left ideals

$$Ra \subset Ra + Rab \subset Ra + Rab + Rab^2 \subset \cdots.$$

Hence we have $Ra + Rab + \cdots + Rab^k = Ra + Rab + \cdots + Rab^{k+1}$ for some k. Then we have $x_i \in R$ such that

$$0 \neq ab^{k+1} = x_0 a + x_1 ab + \cdots + x_k ab^k.$$

Not all the $x_i = 0$. Let x_h be the first $\neq 0$. Then $ab^{k+1} = x_h ab^h + \cdots + x_k ab^k$ with $x_h \neq 0$. Cancelling b^h we obtain

$$0 \neq x_h a = ab^{k-h+1} - x_{h+1}ab - \cdots - x_k ab^{k-h} \in Ra \cap Rb$$

and the Ore-Wedderburn condition holds. □

This condition insures that R can be embedded in a (left) quotient division ring $Q(R)$ (or $Q_\ell(R)$), that is, a division ring containing R as subring such that every element of Q has the form $b^{-1}a, b, a \in R$. We shall not give the proof since the theorem will play only a marginal role in the sequel (see Section 1.11). An interested reader may consult Jacobson [43], p. 118f or ex. 6 on p. 119 of BAI for a proof.

Conditions (ii) and (iii) hold for $R = D[t; \sigma, \delta]$ since this is a left PID. On the other hand, we have

Proposition 1.1.14. *$R = D[t; \sigma, \delta]$ is a right PID if and only if σ is an automorphism.*

Proof. If σ is an automorphism we have the relation

$$at = t(\sigma^{-1}a) - \delta\sigma^{-1}a \tag{1.1.15}$$

which implies that if we put $\sigma' = \sigma^{-1}$ and $\delta' = -\delta\sigma^{-1}$ then

$$\delta'(ab) = a(\delta' b) + (\delta' a)(\sigma' b) \tag{1.1.16}$$

(cf. 1.1.1). Moreover, every element of R can be written in one and only one way in the form $a_0 + ta_1 + t^2 a_2 + \cdots + t^n a_n$, $a_i \in D$. It follows by symmetry that we have a right division algorithm and hence that R is a right PID.

Conversely, suppose R is a right PID and let $a \in D^* = D \backslash \{0\}$ ($\backslash$ denotes set theoretic complement). By the right-handed version of Proposition 1.1.13, R has the right Ore property. Hence $tR \bigcap atR \neq 0$ and so we have $f(t), g(t) \neq 0$ such that $tf(t) = atg(t)$. Then deg $f(t) =$ deg $g(t)$ and $f(t) = a_0 + a_1 t + \cdots +$

a_nt^n, $g(t) = b_0 + b_1t + \cdots + b_nt^n$ with $a_n \neq 0$, $b_n \neq 0$. Comparing terms of highest degree we obtain

$$\sigma a_n = a\sigma b_n, \qquad a = \sigma a_n b_n^{-1}.$$

Thus $a \in \sigma D$. Since a was any non-zero element of D, we see that σ is surjective and hence σ is an automorphism. □

We shall call $D[t; \sigma, \delta]$ a *differential polynomial ring* if $\sigma = 1$ and a *twisted polynomial ring* if $\delta = 0$ or, more generally, if these situations can be realized by replacing t by another generator for R over D of the form $t' = ut + v, u \in D^*, v \in D$. Then $t = u't' + v'$ where $u' = u^{-1}, v' = -u^{-1}v$ and $t'a = (\sigma' a)t' + \delta'$ where

$$\sigma' a = u(\sigma a)u^{-1}, \ \delta' a = u(\delta a) + va - u(\sigma a)u^{-1}v. \tag{1.1.17}$$

The first of these equations shows that if σ is an inner automorphism then we may take $\sigma' = 1$ so we have a differential polynomial ring. The second equation in (1.1.17) shows that if we have $\delta = 0$ then replacing t by $t' = t + v$ gives the new σ-derivation

$$\delta' = \delta_{\sigma,v} : a \rightsquigarrow (\sigma a)v - va \tag{1.1.18}$$

which we call an *inner* σ*-derivation.* Also we see that if δ has this form then replacing t by $t' = t - v$ gives $\delta' = 0$ so we have a twisted polynomial ring. We therefore have

Proposition 1.1.19. *If σ is an inner automorphism, then $R = D[t; \sigma, \delta]$ is a differential polynomial ring and if δ is an inner σ-derivation then R is a twisted polynomial ring.*

From now on we assume that σ is an automorphism. This implies that the center C of D is stabilized by σ and we have the following

Proposition 1.1.20. *If the restriction $\sigma|C \neq 1_C$ then R is a twisted polynomial ring.*

Proof. By hypothesis, there exists a $c \in C$ such that $\sigma c \neq c$ so we can replace t by $t' = ct - tc = (c - \sigma c)t - \delta c$. This replaces δ by δ' as in (1.1.17) where $u = c - \sigma c$ and $v = -\delta c$. Then for any $a \in D$,

$$\begin{aligned}\delta' a &= (c - \delta c)\delta a - (\delta c)a + (\sigma a)\delta c \qquad (\text{since } u \in C)\\ &= c(\delta a) + (\sigma a)(\delta c) - (\sigma c)(\delta a) - (\delta c)a\\ &= \delta(ac) - \delta(ca) = 0\end{aligned}$$

Hence R is a twisted polynomial ring. □

Theorem 1.1.21. *If the dimensionality $[D : C] < \infty$ then $R = D[t; \sigma, \delta]$ is either a twisted polynomial ring or a differential polynomial ring.*

Proof. If $\sigma \mid C \neq 1_C$ then R is a twisted polynomial ring by 1.1.20. On the other hand, if $\sigma \mid C = 1_C$ then σ is an inner automorphism by the Skolem-Noether theorem. Then R is a differential polynomial ring by 1.1.19. □

Since we are assuming σ is an automorphism, $R = D[t; \sigma, \delta]$ is both a left and a right PID. A ring of this sort will be called simply a PID.

We now consider the (two sided) ideals in any PID R. If I is such an ideal, then $I = Rd = d^*R$ and for any $a \in R$ there exist a', $\tilde{a} \in R$ such that $da = a'd$, $ad^* = d^*\tilde{a}$. Also $d = d^*u$, $d^* = vd$ for $u, v \in R$ and $d = vdu = vu'd$. Hence $vu' = 1$ and since R is a domain $u'v = 1$ (by $(u'v - 1)u' = 0$). Hence v is a unit. Similarly u is a unit. Then $dR = d^*uR = d^*R = I$ so we have $I = Rd = dR$. Conversely, if d is an element such that for any $a \in R$ there is an a' and an $\tilde{a}$ such that $da = a'd$ and $ad = d\tilde{a}$ then Rd is an ideal and $Rd = dR$. An element having this property will be called a *two-sided* element of R. It is readily seen that $a \rightsquigarrow a'$ is an automorphism of R with $a \rightsquigarrow \tilde{a}$ as its inverse. It is easily seen also that if d is a two-sided element, then so is udv for any units u and v and if $d_1 = d_2d_3$ and any two of these are two-sided, then so is the third.

We shall now determine the two-sided elements, hence, the ideals in twisted polynomial and differential polynomial rings. We assume first that $R = D[t; \sigma] \equiv D[t; \sigma, 0]$.

Theorem 1.1.22. *(i) The two-sided elements of $R = D[t; \sigma]$ are the elements $ac(t)t^n$ where $a \in D$, $n = 0, 1, \ldots$ and $c(t) \in$ Cent R, the center of R.*

(ii) Cent R = Cent $D \bigcap$ Inv $\langle\sigma\rangle$, *where* $\text{Inv}\langle\sigma\rangle = \{d \in D \mid \sigma d = d\}$, *if no non-zero power of σ is an inner automorphism of D.*

(iii) Let σ have finite order r modulo inner automorphisms and suppose $\sigma^r = I_u : x \rightsquigarrow uxu^{-1}$, $u \in D^*$. Then Cent R *is the set of polynomials of the form*

$$\gamma_0 + \gamma_1 u^{-1} t^r + \gamma_2 u^{-2} t^{2r} + \cdots + \gamma_s u^{-s} t^{sr} \tag{1.1.23}$$

where $\gamma_i \in$ Cent D and $\gamma_i u^{-i} \in \text{Inv}\langle\sigma\rangle$. Moreover, if r is also the order of $\sigma \mid$ Cent D then u can be chosen in $\text{Inv}\langle\sigma\rangle$ *and then* Cent $R = F[u^{-1}t^r]$ *the ring of polynomials in $u^{-1}t^r$ with coefficients in $F =$* Cent $D \bigcap \text{Inv}\langle\sigma\rangle$. *The last situation holds if* $[D : \text{Cent } D] < \infty$.

Proof. (i) The elements t^n are two-sided and any element of D is two-sided. Hence any two-sided element has the form $ac(t)t^n$ where $a \in D$ and $c(t)$ is a two-sided element of the form

$$c(t) = 1 + c_1 t + c_2 t^2 + \cdots + c_m t^m, c_i \in D, c_m \neq 0. \tag{1.1.24}$$

The conditions that $c(t)$ is two-sided are that for every $a \in D$ there exists an $a' \in R$ such that $c(t)a = a'c(t)$ and there exists a $t' \in R$ such that $c(t)t = t'c(t)$. It follows that $a' \in D$ and then that $a' = a$. Also $t' = t$. Hence $c(t) \in$ Cent R.

(ii) We have Cent R = Cent $D \bigcap$ Inv$\langle\sigma\rangle$. Let F denote this field. If Cent $R \supsetneqq F$ then Cent R contains an element $\sum_0^m c_i t^i$ of degree $m > 0$.

Then every $c_i t^i \in$ Cent R. In particular, $c_m t^m \neq 0$ is in Cent R. Then $\sigma^m a = c_m^{-1} a c_m, a \in D$, so σ^m is inner.

(iii) Let r be the order of σ modulo inner automorphisms and let $\sigma^r = I_u$. Then $m = rs$ and $\sigma^m x = c_m^{-1} x c_m = u^s x u^{-s}$ implies that $c_m = \gamma_s u^{-s}, \gamma_s \in$ Cent D. A similar argument applies to every $c_i t^i \neq 0$ in Cent R. This implies that any element of Cent R has the form (1.1.23) with $\gamma_i \in$ Cent D. The condition that such an element commutes with t is $\gamma_j u^{-j} \in \operatorname{Inv}\langle\sigma\rangle$.

We have $\sigma^r x = uxu^{-1}$ and $\sigma\sigma^r = \sigma^r\sigma$ so $(\sigma u)(\sigma x)(\sigma u)^{-1} = u(\sigma x)u^{-1}$. Hence $\sigma u = \mu u$ where $\mu \in$ Cent D. Then $\sigma^2 u = (\sigma\mu)\mu u$ and $u = uuu^{-1} = \sigma^r u = (\sigma^{r-1}\mu)\cdots(\sigma\mu)\mu u$ so $(\sigma^{r-1}\mu)\cdots(\sigma\mu)\mu = 1$. If r is the order of $\sigma \mid$ Cent D then this reads $N_{\text{Cent } D/F}(\mu) = 1$ where N is the norm. Hence, by Hilbert's norm theorem ("Satz 90") there exists a $\lambda \in$ Cent D such that $\mu = \lambda(\sigma\lambda)^{-1}$. We may replace u by λu and so we may suppose that $\sigma u = u$. Then also $\sigma\gamma_i = \gamma_i$ and Cent $R = F[u^{-1}t^r]$. The last statement follows from the Skolem-Noether Theorem. □

We suppose next that $R = D[t;\delta] \equiv D[t;1,\delta]$. We recall that the set of δ-constants, that is, the $a \in D$ such that $\delta a = 0$ form a division subring, Const δ, of D. We recall also that if $\gamma \in$ Cent D then $\gamma\delta$ is a derivation and if the characteristic char $D = p \neq 0$ then δ^p is a derivation. It follows in the characteristic p case that if the $\gamma_i \in$ Cent D then

$$\gamma_0\delta + \gamma_1\delta^p + \gamma_2\delta^{p^2} + \cdots \tag{1.1.25}$$

is a derivation. We note also that as a special case of (1.1.4) we have

$$t^j a = \sum_{i=0}^{j} \binom{j}{i} (\delta^{j-i}a)t^i. \tag{1.1.26}$$

Hence, if $c(t) = \sum_0^n c_j t^j$ then

$$c(t)a = \sum_{j=0}^{n}\sum_{i=i}^{n} \binom{j}{i} c_j(\delta^{j-i}a)t^i. \tag{1.1.27}$$

We now define a D-linear transformation Δ_i, $i = 0, 1, \ldots$ in $D[t;\delta]$ by

$$\Delta_i t^j = \binom{j}{i} t^{j-i} \text{ if } j \geq i,\ \Delta_i t^j = 0 \text{ if } j < i. \tag{1.1.28}$$

Then $\Delta_i c(t) = \sum_{j=i}^n \binom{j}{i} c_j t^{j-i}$ if $i \leq n$ and $\Delta_i c(t) = 0$ if $i > n$. If char $D = 0$ then $\Delta_i c(t) = \frac{1}{i!}c^{(i)}(t)$ where $c^{(i)}(t)$ is the formal i-th derivative of $c(t)$. For arbitrary characteristic, we can verify that $\Delta_k\Delta_i t^j = \binom{k+i}{k} \Delta_{k+i} t^j$. Hence

$$\Delta_k\Delta_i = \binom{k+i}{k} \Delta_{k+i} = \Delta_i\Delta_k. \tag{1.1.29}$$

Since δ is a derivation in D we have $a_L\delta = \delta a_L + (\delta a)_L$ for $a \in D$ and a_L the left multiplication $x \rightsquigarrow ax$. Since $a \rightsquigarrow a_L$ is a ring homomorphism the relation we have noted implies that we have a unique homomorphism of R into End D such that $a \rightsquigarrow a_L$, $t \rightsquigarrow \delta$. We denote the image of $f(t)$ under this homomorphism by $f_L(\delta)$ and we abbreviate $f_L(\delta)a$ to $f(\delta)a$. Using this notation and the definition of the Δ_i we can write (1.1.27) as

$$c(t)a = \sum_0^n((\Delta_i c)(\delta))at^i. \tag{1.1.30}$$

We can now prove

Lemma 1.1.31.

(i) If $c(t) = \sum_0^n c_i t^i$, $c_i \in D$, and $[c(t), a] = 0$ for $a \in D$ then $[\Delta_k c(t), a] = 0$ for all k.

(ii) If $c(t) \in$ Cent R then every $\Delta_k c(t) \in$ Cent R.

Proof. (i) By (1.1.30), $[c(t), a] = 0$ if and only if $ac(t) = \sum_0^n(\Delta_i c)(\delta)at^i$. Apply Δ_k for $0 \leq k \leq n$ to both sides of this relation. This gives

$$\begin{aligned} a\Delta_k c(t) &= \sum_0^n(\Delta_i c)(\delta)a\Delta_k t^i = \sum_k^n(\Delta_i c)(\delta)a\binom{i}{k}t^{i-k} \\ &= \sum_k^n(\Delta_{i-k}\Delta_k c)(\delta)at^{i-k} \end{aligned}$$

which shows that $\Delta_k c(t)$ satisfy the condition $[\Delta_k c(t), a] = 0$. Since $\Delta_k c(t) = 0$ for $k > n$ we obtain (i).

(ii) $c(t) \in$ Cent R if and only if $[c(t), a] = 0$ for all $a \in D$ and $[c(t), t] = 0$. The last condition holds if and only if $\delta c_i = 0$ for all i. It is now clear that (ii) follows from (i). □

We can now determine the two-sided elements of a ring of differential polynomials.

Theorem 1.1.32 (Amitsur [57]).

(i) The two-sided elements of $R = D[t;\delta]$ are the elements $uc(t)$ where $u \in D$ and $c(t) \in$ Cent R.

(ii) Either Cent $R = F =$ Cent $D \bigcap$ Const δ *or* Cent $R = F[z]$ *where z has the following form*

$$z = \begin{cases} t - d & \text{if char } D = 0 \\ t^{p^e} + \gamma_1 t^{p^{e-1}} + \cdots + \gamma_e t - d & \text{if char } D = p \end{cases} \tag{1.1.33}$$

where in the first case $\delta = i_d$ the inner derivation $x \rightsquigarrow [d, x]$ and in the second case the $\gamma_i \in F$, $\delta d = 0$ and

$$\delta^{p^e} + \gamma_1 \delta^{p^{e-1}} + \cdots + \gamma_e \delta = i_d. \tag{1.1.34}$$

Proof. (i) The condition that an element is two-sided shows that any monic two-sided element is in the center. This implies (i).

(ii) We have Cent $R \bigcap D = F$ and this is a proper subset of Cent R if and only if Cent R contains elements of positive degree. Let $c(t) = c_0 + c_1 + \cdots + c_n t^n$ be such an element of least positive degree n. By (1.1.30), every $\Delta_j c(t) \in$ Cent R. By the minimality of the degree of $c(t)$ we have $\binom{i}{j} c_i = 0, \quad 1 \leq j \leq i-1, \ i > 1$. Since the binomial coefficients $\binom{i}{j}$, $1 \leq j \leq i-1$, are 0 in D if and only if char $D = p$ and $i = p^e$ we see that if char $D = 0$ then $c(t) = c_0 + c_1 t$ and if char $D = p$ then $c(t) = c_0 + c_1 t + c_p t^p + c_{p^2} t^{p^2} + \cdots + c_{p^e} t^{p^e}$. In both cases commutativity with t implies that the $c_i \in$ Const δ. If $c(t) = c_0 + c_1 t$ then $0 = [c(t), a] = [c_0, a] + [c_1, a]t + c_1(\delta a)$. Hence $c_1 \in$ Cent D so $c_1 \in F$. Then we may assume $c_1 = 1$ and $c(t) = t - d$. Then $\delta a = [d, a]$. If char $D = p$ and $c(t) = c_0 + \sum_{j=0}^{e} c_{p^j} t^{p^j}$ then $[t^{p^j}, a] = \delta^{p^j} a$ (by (1.1.26)) and hence

$$0 = [c_0, a] + \sum_{j=0}^{e} [c_{p^j}, a] t^{p^j} + \sum_{j=0}^{e} c_{p^j} (\delta^{p^j} a).$$

Then $c_{p^i} \in F$ and $\sum_0^e c_{p^j} \delta^{p^j}$ is the inner derivation $x \rightsquigarrow [d, x]$, $d = -c_0$. We may normalize $c(t)$ to $c(t) = t^{p^e} + \gamma_1 t^{p^{e-1}} + \cdots + \gamma_e t - d$, $\gamma_i \in F$, and we have (1.1.35). We now write $z = t - d$ if char $D = 0$ and $z = t^{p^e} + \gamma_1 t^{p^{e-1}} + \cdots + \gamma_e t - d$ if char $D = p$.

It remains to show that Cent $R = F[z]$. Since $F \subset$ Cent R and $z \in$ Cent R, $F[z] \subset$ Cent R. Now let $f(t) \in$ Cent R. By division we obtain

$$f(t) = q(t)z + r(t) \tag{1.1.35}$$

where deg $r(t) <$ deg z. We claim that $q(t), r(t) \in$ Cent R. For we have $0 = [f(t), t] = [q(t), t]z + [r(t), t]$ and $0 = [f(t), a] = [q(t), a]z + [r(t), a]$, $a \in D$. Degree considerations show that $[q(t), t] = [q(t), a] = [r(t), t] = [r(t), a] = 0$ and hence $q(t), r(t) \in$ Cent R. We can now use induction on the degree of $f(t)$ to conclude that $f(t) \in F[z]$. Hence $F[z] =$ Cent R. □

The foregoing result implies that if char $D = 0$ then Cent $R = F$ unless δ is an inner derivation, and if char $D = p$ then Cent $R = F$ unless there exists a monic p-polynomial $f(\lambda) = \lambda^{p^e} + \gamma_1 \lambda^{p^{e-1}} + \cdots + \gamma_e \lambda$ with $\gamma_i \in F$ such that $f(\delta) = i_d$ where $\delta d = 0$. Moreover, these conditions are sufficient for Cent $R \not\supset F$. For in the first case if $\delta = i_d$ then $t - d \in$ Cent R and in the second case if $f(\delta) = i_d$ with $\delta d = 0$ then $t^{p^e} + \gamma_1 t^{p^{e-1}} + \cdots + \gamma_e t - d \in$ Cent R. Moreover, if z is chosen as in the proof then the corresponding polynomial $f(\lambda) = \lambda^{p^e} + \gamma_1 \lambda^{p^{e-1}} + \cdots + \gamma_e \lambda$ is the monic polynomial of least degree such that $f(\delta)$ is an inner derivation by a d such that $\delta d = 0$.

1.2. Arithmetic in a PID

Let R be a PID (= left and right PID). We shall work with left ideals Ra and the corresponding factor R-modules R/Ra. By symmetry, the results will apply equally well to right ideals.

Suppose $Ra \supset Rb \neq 0$. Then $b = ca$ so a is a right factor of b. We indicate this by writing $a \mid_r b$. Conversely, if $a \mid_r b$ then $Ra \supset Rb$. This condition implies that Ra/Rb is a submodule of R/Rb. Now Ra/Rb is cyclic with generator $a + Rb$. It is clear that the annihilator of this generator is Rc. Hence

$$Ra/Rb = Ra/Rca \simeq R/Rc. \tag{1.2.1}$$

We also have

$$(R/Rb)/(Ra/Rb) \simeq R/Ra. \tag{1.2.2}$$

We have $Ra = Rb \neq 0$ if and only if $a \mid_r b$ and $b \mid_r a$. Then $b = ca, a = db$ so $b = cdb$. Then $cd = 1$ which implies also that $dc = 1$ since R is a domain. Thus c and d are units. Hence a and b are *left associates* in the sense that $b = ua$, u a unit.

We have $Ra + Rb = Rd$. Then $d \mid_r a$ and $d \mid_r b$. Moreover, if $e \mid_r a$ and $e \mid_r b$ then $Re \supset Ra$ and $Re \supset Rb$ so $Re \supset Rd$ and $e \mid_r d$. Hence d is a *right greatest common divisor (right* g.c.d.) of a and b in the obvious sense. Any two right g.c.d. are left associates. We denote any right g.c.d. of a and b (= any d such that $Ra + Rb = Rd$) by $(a, b)_r$.

We have seen that R satisfies the left Ore condition. If $a \neq 0$ and $b \neq 0$ then $Ra \cap Rb \neq 0$. We have $Ra \cap Rb = Rm$ so $m = b'a = a'b \neq 0$. Moreover, if $a \mid_r n$ and $b \mid_r n$ then $Rm = Ra \cap Rb \supset Rn$ so $m \mid_r n$. Hence m is a *left least common multiple (left* l.c.m) of a and b in the obvious sense. Any two left l.c.m. of a and b are left associates. We denote any one of these by $[a, b]_\ell$.

We have seen that R is left noetherian. We now show that R is left artinian modulo any non-zero left ideal Ra, which means that if we have a sequence of left ideals

$$Ra_1 \supset Ra_2 \supset \cdots \supset Ra \neq 0 \tag{1.2.3}$$

then there exists a k such that $Ra_k = Ra_{k+1} = \cdots$. To see this we note that (1.2.3) is equivalent to

$$a = b_i a_i \neq 0,\ a_{i+1} = c_i a_i,\ i = 1, 2, \ldots. \tag{1.2.4}$$

Then $a = b_i a_i = b_{i+1} a_{i+1} = b_{i+1} c_i a_i$ so $b_i = b_{i+1} c_i$ and

$$b_1 R \subset b_2 R \subset \cdots. \tag{1.2.5}$$

Since R is right noetherian we have $b_k R = b_{k+1} R = \cdots$ for some k. Then $c_k, c_{k+1}, \ldots$ are units and $Ra_k = Ra_{k+1} = \cdots$. The condition that R is left artinian modulo any non-zero left ideal Ra is equivalent to R/Ra is artinian for any $a \neq 0$. Now we recall that a module has a composition series if and only if it is both artinian and noetherian. Hence we have