DIE RINGE, DEREN ENDLICH ERZEUGBARE ECHTE UNTERRINGE HAUPTRECHTSIDEALE SIND

Von

F. SZÁSZ (Budapest)

(*Vorgelegt von* L. RÉDEI)

Hochgeehrtem Professor P. TURÁN *zu seinem 50. Geburtstage gewidmet*

Man findet in der abstrakten Algebra oft ein solches Bestreben, dessen Zweck die explizite und konstruktive Bestimmung einer festgewählten Klasse von speziellen algebraischen Strukturen ist. Diese Arbeit[1] hat ebenfalls ein Ziel derselber Art. Ähnlich gewissen gruppentheoretischen Untersuchungen von R. DEDEKIND [3] und von R. BAER [2] kann es nämlich die Klasse der sogenannten Vollidealringe bzw. Vollrechtsidealringe als ein ringtheoretisches Analogon der berühmten Hamiltonschen Gruppen untersucht werden. In diesen Ringen sind nach Definition sämtliche Unterringe stets Ideale bzw. Rechtsideale. Die explizite Bestimmung aller Vollidealringe bzw. Vollrechtsidealringe ist im allgemeinen ein schweres und bisher noch ungelöstes Problem der Algebra; obwohl schon viele hierher gehörende spezielle Ergebnisse existieren. (S. z. B. die Arbeiten von M. SPERLING [11], L. RÉDEI [8], [9], A. JONES–J. J. SCHÄFFER [6], F. SZÁSZ [12], [13], [14], [15], [16] und neulich allgemeiner P. A. FREUDMAN [21], [22], [23], [24].)

Ein beliebiger (assoziativer) Ring A wird ein voller Hauptrechtsidealring, kurz nur ein V-Ring genannt, wenn sämtliche endlich erzeugbaren echten Unterringe S von A Hauptrechtsideale von A sind.

Wir möchten nun in der vorliegenden Arbeit alle V-Ringe A bis auf Isomorphie explizit bestimmen. Der Ring I der ganzen rationalen Zahlen, als das wichtigste und einfachste Beispiel für einen V-Ring, begründet neben dem erwähnten gruppentheoretischen Analogon ebenfalls die Möglichkeit und Aufgabe der Untersuchung von V-Ringen als speziellen Vollrechtsidealringen[2].

Das Ziel dieser Arbeit ist also der Beweis des einzigen Satzes über die explizite Bestimmung aller V-Ringe. Wir werden in diesem Satz sehen, daß viele verschiedene V-Ringe existieren. Neben dem Ring I ist sowohl jeder Unterring mI ($m \in I$) von I, als auch jeder Zeroring mit torsionsfreier additiver Gruppe ersten Ranges ein V-Ring. Die Mächtigkeit aller V-Ringe mit gemischter additiver Gruppe ist das Kontinuum. Diese Ringe sind die direkten Summen eines V-Ringes mit torsionsfreier additiver Gruppe und einiger endlicher Primkörper. Der Zeroring mit additiver Gruppe, die zur Gruppe aller rationalen Zahlen mod 1 isomorph ist, ist ebenfalls ein

[1] Bezüglich des Gegenstandes dieser Arbeit verweisen wir auf den speziellen Gegenstand des elften § in der Dissertation des Verfassers und bezüglich dieses speziellen Falles auf den unbewiesenen Satz 3 unserer Note [15].

[2] Die Forderung, daß ein Ring A ein V-Ring ist, ist eine natürliche hinreichende Bedingung dafür, daß in A aus der Minimalbedingung für Hauptrechtsideale auch die Minimalbedingung für die durch ein Element erzeugten Unterringe (und umgekehrt) folgt. Das Beispiel der endlichen Körper mit echten Unterringen zeigt aber, daß die Forderung, daß A ein V-Ring ist, keine notwendige Bedingung dafür ist, daß in A die obigen zwei Minimalbedingungen untereinander übereinstimmen sollen (s. unsere Arbeiten [17] und [18]).

V-Ring. Man erkennt leicht, daß $Z(p^\infty) \oplus I/(p)$ ein V-Ring ist. Durch die Konstruktion der direkten Summe können weitere periodische unendliche V-Ringe gebildet werden. Bezüglich der vielen verschiedenen endlichen V-Ringe verweisen wir auf den Satz. Zwischen diesen Ringen sind z. B. die Unterringe von $\{a\}$ mit $pa = a^4 - a^3 = 0$, ferner gewisse durch zwei Elemente erzeugte Ringe der Mächtigkeit p^3 und p^2 zu erwähnen.

VORBEMERKUNGEN. Man sieht, daß sowohl jeder Unterring als auch jedes homomorphe Bild eines V-Ringes ebenfalls ein V-Ring ist. Ferner kann jeder endlich erzeugbare echte Unterring B eines V-Ringes A wegen $B = (b)_r = \{b\} + bA$, $bA \subseteq \{b\}$, $B = \{b\}$ durch ein Element erzeugt werden.[3] Daher sind die Unterringe eines V-Ringes sicher kommutativ, und der V-Ring A selbst ist hiernach entweder kommutativ oder einstufig nichtkommutativ im Sinne von RÉDEI [10]. Ferner ist jedes Element a ($\neq 0$) eines V-Ringes A entweder nilpotent oder die Nullstelle eines nichtidentisch verschwindenden Polynomes $f(x) \in x \cdot I[x]$ wegen $a^3 = a^2 a \in \{a^2\}$, denn a^3 kann durch die geraden Potenzen $a^2, a^4, a^6, a^8, \ldots$ ausgedrückt werden. Diese Tatsachen werden wir so erwähnen, daß die Elemente eines V-Ringes stets I-algebraisch im obigen Sinne sind. Insbesondere bestätigt der nachstehende Satz, daß jedes Element eines V-Ringes die Nullstelle eines Polynomes $f(x)$ höchstens vierten Grades in x ist. Sind nun sämtliche echten Unterringe eines Ringes A streng zyklische Rechtsideale, d. h. Rechtsideale der Gestalt aA ($a \in A$), so ist A nach [15] und nach dem Satz dieser Arbeit sicher ein V-Ring, obwohl diese Tatsache nur durch die Definitionen dieser zwei Ringeigenschaften nicht leicht eingesehen werden kann. Ferner ist jeder durch ein Element erzeugte (also kommutative) V-Ring stets ein Hauptidealring. Die endlichen V-Ringe sind aber nicht notwendig kommutativ. Jeder V-Ring A ist abzählbar, also $|A| \leqq \aleph_0$.

Nun gilt der

SATZ. *Alle V-Ringe sind bis auf Isomorphie die folgenden:*

I) *unter den endlichen Ringen mit additiver Abelscher elementarer p-Gruppe:*

I_1) *die (explizit darstellbaren) endomorphen Bilder des Ringes $\{a\}$ mit $pa = a^4 - a^3 = 0$;*

I_2) *die aus p^2 Elementen bestehenden nichtnilpotenten und nichtkommutativen Ringe $\{a, b\}$ mit $pa = pb = a^2 = b^2 - b = ab - a = ba = 0$;*

I_3) *die (explizit darstellbaren) homomorphen Bilder des aus p^3 Elementen bestehenden, nilpotenten, kommutativen Ringes $\{a, b\}$ mit $pa = pb = a^3 = b^3 = ab = ba = a^2 - kb^2 = 0$, wobei p eine ungerade Primzahl, k eine ganze rationale Zahl, $(p, k) = 1$ und $(-k)$ ein quadratischer Nichtrest* mod p *ist;*

I_4) *die aus p^3 Elementen bestehenden, nilpotenten, nichtkommutativen Ringe $\{a, b\}$ mit $pa = pb = a^3 = b^3 = ab = ba - b^2 = a^2 - kb^2 = 0$, wobei p eine ungerade Primzahl, k eine ganze rationale Zahl, $(p, k) = 1$, $4k \not\equiv 1 \pmod p$ und $(1 - 4k)$ ein quadratischer Nichtrest* mod p *ist;*

I_5) *die aus acht Elementen bestehenden, nilpotenten, nichtkommutativen Ringe $\{a, b\}$ mit $2a = 2b = a^3 = b^3 = ab = ba - b^2 = a^2 - b^2 = 0$;*

[3] Hierbei bezeichnen $(\ldots, x_\alpha, \ldots)_r$ bzw. $\{\ldots, x_\beta, \ldots\}$ das durch die eingeklammerten Elemente erzeugte Rechtsideal von bzw. den entsprechenden Unterring. Wir verweisen für die Grundbegriffe und Bezeichnungen auf [4], [5] und [10].

II) *unter den endlichen p-Ringen, deren additive Gruppe keine elementare p-Gruppe ist:* II_1) *die (explizit darstellbaren) Unterringe des Ringes* $\{a\}$ *mit* $p^n a = p(a^2 - p^f a) = (a^2 - p^f a)a - (a^2 - p^f a) = 0$, *wobei* $2 \leqq n \in I$, $1 \leqq f \in I$, $f \leqq n$ *gelten;*

III) *unter den unendlichen p-Ringen:* III_1) *die Ringe* $Z(p^\infty) \oplus I/(p)$ *bzw.* III_2) $Z(p^\infty)$, *wobei* $\oplus$ *die ringtheoretische direkte Summe bezeichnet;*

IV) *unter den beliebigen periodischen Ringen:* IV_1) *die Ringe, deren jede p-Komponente einem im Satz bei* I_1), II) *bzw.* III) *vorkommenden Ringe isomorph ist;*

V) *unter den Ringen mit torsionsfreier additiver Gruppe:*

V_1) *die Unterringe* mI $(m \in I)$ *des Ringes I der ganzen rationalen Zahlen;*

V_2) *die Zeroringe A ersten Ranges (d. h.* $A^2 = 0$ *mit dem Rang* $A^+ = 1$*);*

VI) *unter den Ringen mit gemischter additiver Gruppe* $\mathrm{VI}_{1,2}$) *die ringtheoretischen direkten Summen* $A = B \oplus C$, *wobei B einen solchen periodischen Ring bezeichnet, dessen jede von Null verschiedene p-Komponente* B_p *einem Körper* $I/(p)$ *isomorph ist, C einen bei* V_1) *bzw.* V_2) *vorkommenden torsionsfreien Ring bedeutet, und im Falle* $C \cong kI$ *auch* $|B| < \aleph_0$ *und* $k = l|B|$ $(l \in I)$ *gelten.*

DER BEWEIS DES SATZES besteht aus zwei größeren Teilen. Im Teil a) sind alle V-Ringe aufgesucht und aufgezählt worden. Ferner wird es im Teil b) bewiesen, daß die explizit gewonnenen Ringe wirklich V-Ringe sind. Insbesondere werden wir den verwickelten Teil a) in mehreren Schritten erledigen. Inzwischen benützt der Beweis beider Teile neben den ringtheoretischen Methoden sowohl gruppentheoretische als auch gewisse elementare zahlentheoretische Methoden.

Teil a) Es sei A im folgenden stets ein V-Ring. Nun werden wir noch verschiedene Nebenbedingungen voraussetzen. Die Hauptrichtung des Beweises ist die Aufzählung der möglichen Fälle bezüglich der additiven Gruppe eines V-Ringes. Inzwischen unterscheiden wir weitere Unterfälle (z. B. Anzahl der Erzeugenden, Kommutativität, Nilpotenz).

1. Ist $A = \{a\}$ ein V-Ring mit $pa = a^n = 0$ $(a^{n-1} \neq 0)$, so gilt schon $a^3 = 0$ oder $a^2 = 0$.

Aus $a^2 a \in \{a^2\}$ folgt nämlich $a^3 = n_1 a^2 + n_2 a^4 + \ldots + n_k a^{2k}$ mit $n_i \in I$. Im Falle $n_1 \not\equiv 0 \pmod p$ ergibt sich wegen $a^2 \in \{a^3\}$ durch wiederholte Einsetzung: $a^2 \in \{a^n\}$. Also ist $a^2 = 0$. Im Falle $p | n_1$ gilt aber $a^3 \in \{a^4\}$, folglich auch $a^3 \in \{a^n\}$, d. h. $a^3 = 0$.

2. Ist $A = \{a\}$ ein endlicher nichtnilpotenter V-Ring mit $pa = 0$, so ist A ein homomorphes Bild des Ringes $B = \{b\}$ mit $pb = b^4 - b^3 = 0$ $(b^3 \neq b^2)$.

Es sei nämlich N das (klassische) Radikal von A. Da A/N ein endlicher halbeinfacher V-Ring ist, und $A \neq N$ gilt, so ergibt sich wegen des Wedderburn–Artinschen Struktursatzes und der Definition des V-Ringes $A/N \cong I/(p)$. Es sei nun $e \in A$ mit $e^2 = e (\neq 0)$, $pe = 0$. Ein solches idempotentes Element existiert sicher, und $e + N$ ist das Einselement von A/N. Aus einer Peirceshen Zerlegung erhält man $A = \{e\} \oplus N_0$, wobei $N_0 = \{n\}$ ein Ideal von A in N ist. Nun gilt aber $n^3 = 0$ wegen 1. Dann ist $a = k_1 e + k_2 n + k_3 n^2$ mit $k_i \in I$. Da auch $eN_0 = N_0 e = 0$ und $\{a^3\} = \{e\}$ bestehen, erhält man die Existenz einer Zahl $l \in I$ mit $(p, l) = 1$, $a^4 = a^3 a = la^3 \neq 0$. Ist nun $l.l_1 \equiv 1 \pmod p$, so gilt $b^4 = b^3$ mit $b = l_1 a$.

3. Sowohl jedes homomorphe Bild als auch jeder Unterring des Ringes $\{b\}$ mit $pb = b^4 - b^3 = 0$ $(b^3 \neq b^2)$ ist ein endomorphes Bild von $\{b\}$. Ferner können sämtliche Unterringe als 0, $\{b^2 - b^3\}$, $\{b^3\}$, $\{b - b^2\}$, $\{b^2\}$, $\{b\}$ dargestellt werden.

Ist nämlich $S_1=\{j_1b+j_2b^2+j_3b^3\}$ $(j_2\in I)$ ein Zeroring von Primzahlordnung in $\{b\}$, so ergibt sich $j_1\equiv 0 \pmod p$ und $j_2\equiv -j_3 \pmod p$ wegen $S_1^2=0$ und wegen der linearen Unabhängigkeit von b, b^2, b^3 über $I/(p)$. Also gilt in diesem Falle $S_1=\{b^2-b^3\}$. Ist nun $S_2=\{k_1b+k_2b^2+k_3b^3\}$ $(k_j\in I)$ ein Körper von Primzahlordnung in $\{b\}$, so können $(k_1b+k_2b^2+k_3b^3)^2=k_1b+k_2b^2+k_3b^3$ und somit $k_1\equiv k_2\equiv 0 \pmod p$, $k_3^2\equiv k_3 \pmod p$, $S_2\neq 0$, also $S_2=\{b^3\}$ vorausgesetzt bzw. bestätigt werden. Es sei nun S_3 ein Unterring von $\{b\}$ mit $|S_3|=p^2$. Ist $b^3\notin S_3$, so enthält S_3 kein idempotentes Element. Also gelten dann $S_3\subseteq N$ und $S_3=\{b-b^2\}=N$ wegen $|\{b\}|=p^3$, $|\{b-b^2\}|=p^2$. Ist nun S_4 ein Unterring von $\{b\}$ mit $|S_4|=p^2$, $b^3\in S_4$, so gilt für $S_4=\{l_1b+l_2b^2+l_3b^3\}$ offenbar $(l_1b+l_2b^2+l_3b^3)^3=(l_1b+l_2b^2+l_3b^3)^2$ wegen 2 und wegen $|S_4|=p^2$, $b^3=b^4\in S$ nach einem geeigneten Wahl von $l_1, l_2, l_3\in I$. Daher gewinnen wir aber $S_4=\{b^2\}$. Man kann nun die Beziehungen $\{b\}/\{b^2-b^3\}\cong\{b^2\}$, $\{b\}/\{b^3\}\cong\{b-b^2\}$, $\{b\}/\{b-b^2\}\cong\{b^3\}$ bzw. $\{b\}/\{b^2\}\cong\{b^2-b^3\}$ leicht einsehen. Damit haben wir unsere Behauptung bewiesen.

4. Läßt sich ein endlicher V-Ring A durch ein Element nicht erzeugen, so kann A gewiß durch zwei Elemente erzeugt werden. Wir setzen also jetzt $\{a\}\neq A$ für jedes $a\in A$ voraus.

Ist nämlich M ein maximaler echter Unterring von A, so gilt $M=\{a\}$. Wählt man nun ein $b\in A$ mit $b\notin M$, so ergibt sich $\{M, b\}=A$, also $A=\{a, b\}$.

Im folgenden wird man voraussetzen, daß A ein endlicher V-ring mit $pA=0$ ist, der durch ein Element nicht erzeugt werden kann. Unter dieser Voraussetzung betrachten wir nun die Schritte von 5 bis 20.

5. Gelten $A=\{a, b\}$, $pa=a^2=pb=b^2=0$, so besteht $A^2=0$ mit $|A|=p^2$.

Man erhält nämlich $ab=ka$ und $ba=lb$ $(k, l\in I)$, denn A ist ein V-Ring. Ferner gilt $0=ab^2=(ka)b=k^2a$, folglich $p|k^2$, $p|k$, $ab=0$. Ganz ähnlich ergibt sich auch $ba=0$, also $A^2=0$. Wegen 4 gewinnen wir $|A|=p^2$.

6. Im Falle $A=\{a, b\}$, $pa=a^2-a=pb=b^2=0$ ist A dem im Satz bei I_2) erwähnten Ringe isomorph.

Dann gilt nämlich $ab=0$ ähnlich dem Schritte 5. Wäre nun auch $ba=0$, so bestände $(a+b)^2=b$, und somit $\{a, b\}=\{a+b\}$ was nach Voraussetzung ausgeschlossen ist. Hiernach gilt $ba=kb\neq 0$ mit $k\in I$, $(p, k)=1$. Ferner ergibt sich $k^2\equiv k\equiv 1 \pmod p$, also wegen $ba^2=ba$ auch $ba=b$.

7. Der Fall $A=\{a, b\}$ mit $pa=a^3=pb=b^2=0$ ist wegen 4 unmöglich.

Dann kann nämlich der Unterring $S=\{a^2, b\}$ durch ein Element erzeugt werden, denn sonst wäre $S=A$, also $A=\{a\}$ wegen $b\notin\{a\}$, $|S|=p^2$, $|\{a\}|=p^2$. Im Falle $S=\{s\}$ gilt aber $|S|=p$, also wegen 5 auch $b\in\{a^2\}$, was wegen 4 wirklich ein Widerspruch ist.

8. Der Fall $A=\{a, b\}$ mit $pa=a^3-a^2=pb=b^2=0$ kann wegen 4 ebenfalls nicht vorkommen.

Dann hat nämlich $S=\{a^2-a, b\}$ ein einziges erzeugendes Element, denn im Falle $S=A$ wäre $a^2=a^4\in S^2=0$, was offenbar unmöglich ist. Daher gelten $S=\{s\}$, $|S|=p$, also $b\in\{a^2-a\}$, und $A=\{a\}$, was wegen 4 ausgeschlossen ist.

9. Der Fall $A=\{a, b\}$ mit $pa=a^4-a^3=pb=b^2=0$ ist nach 4 ebenfalls ausgeschlossen.

Der Unterring $S=\{a^3-a^2, b\}$ ist nämlich echt in A wegen $a^3=a^6\notin S^2=0$. Dann gilt aber $|S|=p$ wegen $S=\{s\}$, also $b\in\{a\}$, was der Voraussetzung in 4 wirklich widerspricht.

10. Der im Falle $A=\{a, b\}$, $pa=a^2-a=pb=b^2-b=0$ gewonnene Ring kann zum Schritte 6 zurückgeführt werden.

Dann gelten nämlich $ab=ka$, $ba=lb$ $(k, l\in I)$ und $k\equiv kl \pmod p$ wegen $(ab)a=$ $=a(ba)$. Ähnlich erhält man auch $l\equiv kl \pmod p$, also $k\equiv l \pmod p$. Im vorausgesetzten Falle $p|k$, wenn auch $ab=ba=0$ ist, ergeben sich $(a+b)a=a$, $(a+b)b=b$, $A=\{a+b\}$, $(a+b)^2=a+b$, $|A|=p$, denn A ist ein V-Ring. $|A|=p$ ist aber nach 4 unmöglich, weil jeder Ring mit Primzahlordnung durch ein Element erzeugt werden kann. Daher ist $(p, k)=1$. Ferner folgt aus $ab=ab^2$ gewiß $k\equiv 1 \pmod p$, folglich $l\equiv 1 \pmod p$ und $ab-a=ba-b=0$. Es sei nun $c=b-a$. Dann gelten $A=$ $=\{a, c\}$, $c^2=0$, $ac=0$, $ca=c$, und somit haben wir unsere Behauptung bewiesen.

11. Der Fall $A=\{a, b\}$ mit $pa=a^3=pb=b^2-b=0$ läßt sich wegen 4 ausschließen.

Dann ist nämlich der Unterring $S=\{a^2, b\}$ echt in A, denn sonst wäre $S=A$, $|A|=p^2$ wegen 5 bzw. 6, also $A=\{a\}$, was unmöglich ist. Hiernach gilt $S=\{s\}$. Es sei ferner $ab=k_1a+k_2a^2$ $(k_i\in I)$. Daher ergibt sich $a^2b=k_1a^2$, folglich $ab^2=$ $=(k_1a+k_2a^2)b=k_1^2a+k_1k_2a^2+k_1k_2a^2$. Dies bedeutet nun $k_1\equiv k_1^2 \pmod p$ und auch $k_2\equiv 2k_1k_2 \pmod p$ wegen $a^2\notin Ia$ und $ab=ab^2$. Aus $k_1^2\equiv k_1 \pmod p$ folgt entweder $k_1\equiv 0 \pmod p$ oder $k_1\equiv 1 \pmod p$. In beiden Fällen gilt $k_2\equiv 0 \pmod p$. Hiernach gewinnen wir entweder $ab=0$ oder $ab=a$. Wäre $ab=a$, so würden $a^2b=a^2$ und $ba^2=lb$ folgen. Das bedeutet, daß $S=\{a^2, b\}=\{s\}$ wegen $b\notin\{a\}$ und wegen 5 nichtkommutativ ist. Da dies aber unmöglich ist, gilt offenbar $ab=0$. Dann ist aber $A=\{a+a^2+b\}$ wegen $(a+a^2+b)a=a^2$, $(a+a^2+b)b=b$, $a=(a+a^2+b)-$ $-(a+a^2+b)(a+b)$, denn A ist ein V-Ring. $A=\{a+a^2+b\}$ ist aber nach 4 unmöglich.

12. Der Fall $A=\{a, b\}$ mit $pa=a^3-a^2=pb=b^2-b=0$ ist wegen 4 ebenfalls ausgeschlossen.

Man erhält nämlich, ähnlich den vorigen Schritten, eine der folgenden Beziehungen: $ba=0$, $ba=b$ bzw. $ab=0$, $ab=a$, $ab=a^2$, $ab=a-a^2$ wegen $ab=k_1a+k_2a^2$ $(k_i\in I)$. Es seien ferner $c=a^2$ und $S=\{b, c\}$. Da $b\notin\{a\}$ und nach 6 bzw. 10 auch $|S|=p^2$ gelten, ist gewiß $S\neq A$. Hiernach ergibt sich $S=\{s\}$ mit $S^2\neq 0$. Daher ist $ab\neq a$, denn im Falle $ab=a$ bestünden $cb=c$, $bc=lb$ $(l\in I)$, folglich wäre S wegen $b\notin\{a\}$ nichtkommutativ. Im Falle $ab=a^2$ gelten ebenfalls $cb=c$ und $bc=lb$ $(l\in I)$, was der Bedingung $S=\{s\}$ widerspricht. Ist aber $ab=a-a^2$, so ergibt sich $cb=0$ und $bc=kb$ $(k\in I)$, $0=b(cb)c=(bc)^2=k^2b^2=k^2b$, $p|k^2$, $p|k$, $bc=0$. Dies ist aber wegen $b\notin\{c\}$, $(b+c)b=b$, $(b+c)c=c$, $(b+c)^2=b+c$, $|S|=p^2$ ebenfalls unmöglich, denn der Körper $\{b+c\}$ ist in A ein Rechtsideal.

13. Der Fall $A=\{a, b\}$ mit $pa=a^4-a^3=pb=b^2-b=0$ ist unmöglich unter der Voraussetzung in 4.

Da $S=\{a^3, b\}$ wegen $b\notin\{a\}$ weder von Primzahlordnung noch kommutativ von Ordnung p^2 ist, gilt $S=A$ mit $|S|=p^2$. Dies ist aber unmöglich wegen $|\{a\}|=p^3$, w. z. b. w.

14. Gilt $A=\{a, b\}$ mit $pa=a^3=pb=b^3=ab-ba=0$, so ist A einem im Satz bei I_3) vorkommenden Ringe isomorph.

Es seien $u=a^2$ und $v=b^2$. Da $S=\{u, v\}$ wegen $b\notin\{a\}$ und wegen 5 sicher echt in A ist, und $u^2=v^2=uv=vu=0$ bzw. $S^2=0$, $S=\{s\}$ gelten, muß eine Zahl $k\in I$ mit $u=kv\neq 0$, also mit $a^2=kb^2\neq 0$ existieren. Hiernach ergibt sich $(p, k)=1$.

Offenbar gilt nun $|A|=p^3$.

Durch eine linksseitige Multiplikation mit a (bzw. mit b) ergibt sich aus $ab = k_1a + k_2a^2$ $(k_i \in I)$ (bzw. aus $ba = l_1b + l_2b^2$, $(l_i \in I)$) sofort $a^2b = k_1a^2$ (bzw. $b^2a = l_1b^2$). Daher folgt aber auch $0 = a^2b^3 = k_1^3a^2$, $p|k_1$ und ähnlich $p|l_1$. Dies bedeutet aber $A^3 = 0$ wegen der Assoziativität von A. Es sei ferner $c = a - l_2b$. Dann gilt $A = \{b, c\}$ mit $bc = ba - l_2b^2 = 0$. Man erhält nun wegen der vorausgesetzten Kommutativität von A auch $cb = 0$. Die Untersuchung von $S_1 = \{b^2, c^2\}$ zeigt nun die Existenz einer Zahl $m \in I$ mit $(p, m) = 1$ und $c^2 = mb^2 \neq 0$, was wir am Anfang des Schrittes 14 schon gesehen haben. Wir zeigen nun, daß $(-m)$ ein quadratischer Nichtrest mod p ist. Im entgegengesetzten Falle sei $l \in I$ eine Lösung der Kongruenz $x^2 \equiv -m \pmod p$. Es sei ferner $d = c - lb$. Dann gilt ebenfalls $A = \{b, d\}$. Ferner erhält man bezüglich $d(\neq 0)$ offenbar $d^2 = (c - lb)^2 = c^2 + l^2b^2 = c^2 - mb^2 = 0$ wegen $cb = bc = 0$, $c^2 = mb^2 \neq 0$, $l^2 \equiv -m \pmod p$. Dann könnte aber $S_2 = \{d, b^2\} = \{c - lb, b^2\}$ durch ein Element erzeugt werden, was wegen $S_2^2 = 0$, $c \notin \{b\}$, $a \notin \{b\}$ unmöglich ist. Hiernach ist $(-m)$ ein quadratischer Nichtrest, und dies bedeutet, daß nur $p \neq 2$ erlaubt ist.

15. Gelten nun $A = \{b, c\}$, $pb = b^3 = pc = c^3 = bc = 0$ und ist A nichtkommutativ, so ergibt sich $cb \neq 0$ und $cb = n_1c + n_2c^2$ $(n_i \in I)$, und A ist einem im Satz bei I_4 bzw. I_5 vorkommenden Ringe isomorph.

Dann folgt $0 = c(bc)b = (cb)^2 = n_1^2c^2$ wegen $c^3 = 0$. Dies bedeutet, daß $p|n_1^2$, $p|n_1$ und $cb = n_2c^2 \neq 0$ mit $(p, n_2) = 1$ sind. Ist nun $n_2g \equiv 1 \pmod p$ und $d = gb$, so gelten $A = \{c, d\}$, $pc = c^3 = pd = d^3 = dc = cd - c^2 = 0$. Da ferner $S_1 = \{c^2, d^2\}$ ähnlich dem Schritte 5 ein Zeroring mit $|S_1| \leq p^2$ ist, bestehen $S_1 \neq A$ und $S_1 = \{s_1\}$, folglich ergibt sich auch $|S_1| = p$. Daher existiert eine Zahl $k \in I$ mit $d^2 = kc^2 \neq 0$, $(p, k) = 1$, denn es gilt $\{d^2\} = \{c^2\}$.

Wir möchten nun zeigen, daß im eventuellen Falle $p \neq 2$ notwendig $4k \not\equiv 1 \pmod p$ gilt. Der Beweis dieser Behauptung bezüglich k wird durch weitere Untersuchungen offenbar die im Satz sowohl bei I_4) als auch bei I_5) vorkommenden nichtkommutativen endlichen Ringe erledigen. Nehmen wir nämlich $4k \equiv 1 \pmod p$ an, so läßt sich ein Widerspruch ableiten. Es sei $w = c - 2d$ $(\neq 0)$. Dann ergibt sich $w^2 = c^2 - 2cd - 2dc + 4d^2$, folglich $w^2 = c^2 - 2c^2 - 0 + 4kc^2 = (4k - 1)c^2 = 0$. Daher ist $S_2 = \{w, d^2\}$ nach dem Schritt 5 ein Zeroring. Hiernach gelten $S_2 \neq A$ und $S_2 = \{s_2\}$, folglich $|S_2| = p$ und $\{w\} = \{d^2\}$. Dies bedeutet aber, daß $w = c - 2d \in \{d^2\}$, also $c \in \{d\}$ und $A = \{d\}$ bestehen, was nach dem Schritt 4 ausgeschlossen ist. Damit haben wir wirklich $4k \not\equiv 1 \pmod p$ bewiesen. Es kann nun auch $\left(\frac{1-4k}{p}\right) = -1$ gezeigt werden, wobei $\left(\frac{n}{p}\right)$ das arithmetische Legendresche Symbol bezeichnet. Wäre nämlich $f^2 \equiv 1 - 4k \pmod p$ lösbar $(f \in I, (p, f) = 1)$, so sei $z = -(1 + f)g_1c + d \in A$, wobei im Falle $p \neq 2$ die Zahl $g_1 \in I$ eine Lösung der Kongruenz $2g_1 \equiv 1 \pmod p$ bedeutet. Dann ergibt sich durch ein elementares Rechnen und wegen $d^2 = kc^2 (\neq 0)$ offenbar $z^2 = ((1 + f)^2g_1^2 - (1 + f)g_1 - 0 + k)c^2 = ((1 + f)^2 - 2(1 + f) + 4k)g_1^2c^2 = (f^2 + (4k - 1))c^2 = 0$ nach $f^2 \equiv 1 - 4k \pmod p$. Hiernach wäre $S_3 = \{z, c^2\}$ nach dem Schritt 5 ein Zeroring. Aus $S_3 \neq A$ und $S_3 = \{s_3\}$ folgt aber $|S_3| = p$, folglich $z = -(1 + f)g_1c + d \in \{c^2\}$. Dann gelten aber $d \in \{c\}$ und $A = \{c\}$, was ausgeschlossen ist. Dieser Widerspruch beweist nun wirklich $\left(\frac{1-4k}{\quad}\right) = -1$.

Gilt nun $kl \equiv 1 \pmod{p}$, also $ld^2 = c^2$, so erhält man aber wegen $l^2 - 4l \equiv l^2(1-4k) \pmod{p}$ sofort $\left(\frac{l^2-4l}{p}\right) = -1$ (vgl. [15]).

16. Gelten $A = \{a, b\}$, $pa = a^3 - a^2 = pb = b^3 = 0$, so kann man diesen Fall ausschließen.

Die Untersuchung von $S_1 = \{a^2 - a, b^2\}$ zeigt nämlich ähnlich den Vorigen $\{a^2 - a\} = \{b^2\}$. Dies bedeutet aber, daß $A = \{a^2, b\}$ ist, was dem im Schritt 11 ausgeschlossenen Falle entspricht.

17. Ist $A = \{a, b\}$ mit $pa = a^4 - a^3 = pb = b^3 = 0$, so ist dieser Fall wegen 4 unmöglich.

$S = \{a^2 - a, b\}$ ist nämlich wegen $a^3 \in A$ ein nilpotentes Rechtsideal von A im Radikal N. Folglich gilt $S = \{s\}$ mit $s^3 = 0$, $|S| \leqq p^2$ wegen des Schrittes 1. Dann zeigt aber $|A/N| = p$ offenbar, daß $|A| \leqq p^3$ gilt, was wegen $a^4 = a^3$ $(a^3 \neq a^2)$ und $b \notin \{a\}$ unmöglich ist.

18. Der Fall $A = \{a, b\}$ mit $pa = a^3 - a^2 = pb = b^3 - b^2 = 0$ ist wegen 4 unmöglich.

Dann ist nämlich $S_1 = \{a^2, b^2\}$ wegen des Schrittes 10 und $|A| \geqq p^3$, $b \notin \{a\}$ offenbar kommutativ. Folglich besteht $\{a^2\} = \{b^2\}$, weil A ein V-Ring ist. Da aber $S_2 = \{a^2 - a, b^2 - b\}$ ein nilpotentes Rechtsideal von A im Radikal N ist, gelten $|S_2| \leqq p^2$ und $\{a^2 - a\} = \{b^2 - b\}$. Daher folgt aber $\{a\} = \{a^2, a - a^2\} = \{b^2, b - b^2\} = \{b\}$, was wirklich ein Widerspruch ist.

19. Der Fall $A = \{a, b\}$ mit $pa = a^4 - a^3 = pb = b^3 - b^2 = 0$ ist wegen 4 ausgeschlossen.

Aus der Untersuchung von $S_1 = \{a^3 - a^2, b^2 - b\}$ folgt nämlich $\{a^3 - a^2\} = \{b^2 - b\}$. Ferner ist $S_2 = \{a^3, b^2\}$ echt, also kommutativ in A. Daher gilt $\{a^3\} = \{b^2\}$, und somit auch $\{b\} = \{a^2\}$, was ausgeschlossen ist.

20. Gilt zum Schluß $A = \{a, b\}$ mit $pa = a^4 - a^3 = pb = b^4 - b^3 = 0$, so ist dieser Fall nach 4 ebenfalls ausgeschlossen.

Es können nämlich, ähnlich den vorigen Schritten, $\{a^3\} = \{b^3\}$, $\{a^2 - a^3\} = \{b^2 - b^3\}$, und somit $\{a^2\} = \{b^2\}$ gezeigt werden. Ferner gilt für das Radikal N von A nach dem Schritt 1 gewiß $|N| \leqq p^2$. Da aber nach dem Wedderburn–Artinschen Struktursatz auch $A/N \cong I/(p)$ gilt, besteht $|A| \leqq p^3$, was wegen $|\{a\}| = p^3$ und $b \notin \{a\}$ ein Widerspruch ist, w. z. b. w.

21. Ist A ein endlicher V-Ring, dessen additive Gruppe A^+ eine p-Gruppe mit $pA^+ \neq 0$ ist, und gilt noch $A = \{a\}$ mit $a^n = 0$ $(a^{n-1} \neq 0)$, so ist A^+ zyklisch.

$(A/pA)^+$ ist nämlich eine elementare p-Gruppe, und daher ergibt sich wegen des Schrittes 1 sofort $a^3 \in p\{a\}$. Da hiernach Rang $A^+ = \text{Rang}\,(A/pA)^+ \leqq 2$ ist, genügt es Rang $A^+ = 1$ zu bestätigen. Es sei $S_1 = \{pa, a^2\}$. Wäre $S_1 = A$, so würde $a = k_1 pa + \ldots + k_s (pa)^s + l_1 a^2 + \ldots + l_t a^{2t}$ gelten. Ferner ergibt sich im Falle $O(a) = p^k$ wegen des Schrittes 1 $(p^{k-1}a)^3 = 0$. Da $\{p^{k-1}a\}$ ein Ideal von A ist, erhält man somit $p^{k-1}a^2 = f_1 p^{k-1}a + f_2 p^{2k-2}a^2 \in \{p^{k-1}a\}$, folglich $p^{k-1}a^2 = f_1 p^{k-1}a$ wegen $2k - 2 \geqq k$, wobei $f_i \in I$. Nun gilt aber $0 = (p^{k-1}a)a^n = p^{k-1}a^2 a^{n-1} = f_1 p^{k-1}a^2 a^{n-2} = \ldots$, also $f_1^n p^{k-1}a = 0$, $p | f_1^n$, $p | f_1$, $p^{k-1}a^2 = 0$. Dies bedeutet aber, daß $p^{k-1}\, a = p^{k-1} \cdot (k_1 pa + \ldots + l_1 a^2 + \ldots) = 0$ gilt, was wegen $O(a) = p^k$ unmöglich ist. Hiernach gilt sicher $S_1 \neq A$. Ferner ist S_1 ein Ideal von A nach Definition des V-Ringes A. Nun gilt aber $|A/S_1| = p$. Ist S_j $(j = 1, 2, 3, \ldots)$ schon definiert, so sei $S_{j+1} = \{S_j^2, pS_j\}$. Ein ähnliches Rechnen zeigt aber ebenfalls, daß $|S_j/S_{j+1}| = p$ ist. Dann ist $A =$

$= S_0 \supset S_1 \supset S_2 \supset \ldots \supset S_{k-1} \supset S_k = 0$ eine streng absteigende Kette von Idealen mit $|S_j/S_{j+1}| = p$, und $O(a) = p^k$ zeigt nun wirklich, daß $\{a\}^+$ zyklisch ist.

22. Ist nun $A = \{a, b\}$ ein endlicher V-Ring mit $A^n = 0$, dessen additive Gruppe A^+ eine p-Gruppe mit $pA^+ \neq 0$ ist, so ist A^+ ebenfalls zyklisch.

Nehmen wir nämlich an, daß A^+ keine zyklische Gruppe ist. Dann gilt aber für jedes $c \in A$ wegen des Schrittes 21 $A \neq \{c\}$. Es kann ferner auch $O(a) = O(b) = p^k \neq p$ vorausgesetzt werden, weil $A = \{a, b\} = \{a+b, b\} = \{a, a+b\}$ gilt. Es sei also $O(a) = O(b) = p^k$. Wäre nun $S_1 = \{a, pb\}$ identisch mit A, so würde aus $b \in \{a, pb\}$ offenbar $pb \in p\{a, pb\} = \{pa, p^2b\}$, und somit auch $b \in \{a, pa, p^2b\}$ folgen. Daher gewinnen wir aber $b \in \{a, p^jb\}$, $b \in \{a, p^ka\}$, also $b \in \{a\}$, $A = \{a\}$, was ausgeschlossen ist. Hiernach bleibt der Fall $S_1 \neq A$, folglich $S_1 = \{s_1\}$ übrig. Dann ist aber die additive Gruppe des V-Ringes $S_1 = \{s_1\}$ wegen $ps_1 \neq 0$, $O(s_1) = O(a) = p^k$ und wegen des Schrittes 21 offenbar zyklisch. Daher liegt pb in der zyklischen additiven Gruppe $\{pa\}^+$, und $S_2 = \{p^{k-1}a, p^{k-1}b\} = \{x | x \in A, px = 0\}$ ist zyklisch. Nach [4] ist dann aber selbst A^+ ebenfalls zyklisch.

23. Ist A ein endlicher nichtnilpotenter V-Ring, dessen additive Gruppe A^+ eine p-Gruppe, aber weder zyklisch noch eine elementare p-Gruppe ist, so gelten $A = \{a\}$, $p^ka = p(a^2 - p^fa) = (a^2 - p^fa)a - (a^2 - p^fa) = 0$ mit $k, f \in I$, $k \geqq 2$, $f \geqq 1$, $f \leqq k$.

Es sei nämlich N das (nilpotente) Radikal von A. Es gibt wegen $N \neq A$ und $A/N \cong I/(p)$ ein idempotentes Element $e(\neq 0)$ in A. Es sei $A = \{e\} \oplus \{n\}$ eine Peircesche Zerlegung in die direkte Summe von Rechtsidealen ($n \in N$).

Nehmen wir $p^ke = e^2 - e = 0$ und natürlich $p^ln = n^2 - p^fn = 0$, $k \geqq 2$, $l \geqq 2$, $f \geqq 1$, $f \leqq l$ an, denn $\{n\}^+$ ist nach 21 zyklisch. Dann wäre aber $S_1 = \{p^{k-1}e, p^{l-1}n\}$ $(\neq A)$ wegen $S_1 = \{s_1\}$ und $S_1^2 = 0$ zyklisch. Da in diesem Falle auch A^+ selbst zyklisch wäre, kann $p^ke = p^ln = 0$, $k \geqq 2$, und gleichzeitig $l \geqq 2$ ausgeschlossen werden.

Setzen wir nun voraus, daß $l \geqq 2$ ist. Dann gelten also $k = 1$, $pe = e^2 - e = p^ln = n^2 - p^fn = 0$. Offenbar ergibt sich auch $en = 0$ wegen $\{e\} \cap N = 0$, bzw. auch $ne = p^tn$ mit $t \in I$, $1 \leqq t \leqq l$, wenn n auf geeignete Art gewählt wird. Ist $S_2 = \{e, pn\}$, so gelten $S_2 \neq A$ und $S_2 = \{s_2\}$, ferner $e(pn) = 0$ bzw. $p^{t+1}n = 0$. Daher erhält man $t+1 \geqq l \geqq t$, folglich entweder $t = l$ oder $t = l-1$. Im Falle $t = l$ ist A wegen $en = ne = 0$ kommutativ. Im Falle $t = l-1$ ergibt sich aber ein Wiederspruch wegen $ne^2 = ne$, $p^{2l-2} \equiv p^{l-1} \pmod{p^l}$. Also ist A im Falle $k = 1$, $l \geqq 2$ kommutativ. Es sei nun $b = e + n$. Dann gelten $b^2 = e + p^fn$, $b^2 - b = (p^f - 1)n$ bzw. $bn = p^fn$. Daher gewinnen wir $b^3 - b^2 = (p^f - 1)p^fn = p^f(b^2 - b)$. Hiernach folgt wegen $p(b^2 - p^fb) = p(e + p^fn - p^fe - p^fn) = 0$ gewiss $(b^2 - p^fb)b = b^2 - p^fb$ mit der Bedingung $p(b^2 - p^fb) = 0$.

Im übrigbleibenden Falle $k \geqq 2$, $l = 1$ gilt $p^ke = e^2 - e = n^3 = pn = 0$. Dann ist der echte Unterring $S_3 = \{pe, n\}$ nilpotent, folglich ist die additive Gruppe von S_3 wegen 22 zyklisch, wenn $pS_3 \neq 0$ ist. Dann ist aber $n \in \{e\}$, $A = \{e\}$, was ausgeschlossen ist. Daher können wir $pS_3 = 0$, $p^2e = 0$ voraussetzen. In diesem Falle gilt für $S_3 = \{pe, n\}$ wegen des Schrittes 1 gewiß $S_3 = \{s_3\}$, also $S_3^3 = 0$, $|S_3| \leqq p^2$. Hiernach ergibt sich wegen $\{e\} \cap \{n\} = 0$ sofort $n^2 = 0$. Dann wären aber $S_3^2 = 0$, $|S_3| = p$, folglich $n \in \{e\}$, $A = \{e\}$, was unmöglich ist. Daher führt $k \geqq 2$, $l = 1$ zu einem Widerspruch.

24. Ist nun A ein unendlicher V-Ring, dessen additive Gruppe A^+ eine p-Gruppe ist, so gilt entweder $A \cong Z(p^\infty)$ oder $A = Z(p^\infty) \oplus I/(p)$.

Es sei nämlich B das Ideal von A, das aus sämtlichen Elementen von Ordnung p von A^+ besteht. Es sei ferner erstens $B = \{b_1, b_2, \ldots, b_n\}$, wobei die Anzahl n der

erzeugenden Elemente endlich, und zwar $n \geqq 3$ ist. Dann kann jeder Unterring $B_i = \{b_1, \ldots, b_{i-1}, b_{i+1}, \ldots, b_n\}$ $(i = 2, 3, \ldots, n-1)$ bzw. $B_1 = \{b_2, b_3, \ldots, b_n\}$, $B_n = \{b_1, \ldots, b_{n-1}\}$ durch ein Element erzeugt werden, wenn $b_1, b_2, \ldots, b_n$ als ein minimales erzeugendes System für B gewählt wird, und auch $n(\geqq 3)$ so klein wie möglich ist. Da aber z. B. $B_1 = \{c\}$ und auch $B = \{b_1, c\}$ gelten, ergibt sich bezüglich der Voraussetzung, daß die minimale Anzahl n der erzeugenden Elemente von B wenigstens drei ist, ein Widerspruch. Damit gilt entweder $n \leqq 2$, oder B läßt sich durch keine endliche Menge erzeugen. Gilt zweitens $B = \{b_1, b_2\}$, also $n = 2$, so hat ein beliebiges Element von B die Gestalt $f(b_1) + g(b_2)$, wobei $f(x)$ und $g(x)$ Polynome im Ring $x \cdot (I/(p))[x]$ sind, denn $\{b_i\}$ $(i = 1, 2)$ ist ein Rechtsideal von A. Dann gilt aber nach den Vorigen entweder $b_i^3 = 0$ oder $b_i^4 = k_i b_i^3$ mit $k_i \in I$, $(p, k_i) = 1$. Hiernach ist $B = \{b_1, b_2\}$ gewiß endlich. Im dritten Falle $B = \{b_1\}$, $n = 1$ ist B eben deswegen endlich. Kann viertens B durch keine endliche Menge erzeugt werden, so läßt sich jeder durch zwei Elemente erzeugte Unterring auch durch ein Element erzeugen, und somit ist B kommutativ. Unter den Voraussetzungen existiert auch ein spezielles erzeugendes System $b_1, b_2, \ldots, b_n, \ldots$ von B mit $b_{i+1} \notin \{b_1, b_2, \ldots, b_i\}$ für jeden Index $i \geqq 1$. Dann gilt offenbar $|\{b_1, b_2, \ldots, b_k\}| \geqq p^k$. Es sei insbesondere $S_1 = \{b_1, b_2, b_3, b_4\}$. Dieser Unterring S_1 ist gewiß echt in B, und somit existiert ein $s_1 \in S_1$ mit $S_1 = \{s_1\}$, $ps_1 = 0$. Man erhält aber nach 1 bzw. 2 entweder $s_1^3 = 0$ oder $s_1^4 = s_1^3$ bei geeigneter Wahl von s_1. In beiden Unterfällen ergibt sich aber $|S_1| = |\{s_1\}| \leqq p^3$, was der Bedingung $|S_1| = |\{b_1, b_2, b_3, b_4\}| \geqq p^4$ widerspricht. Daher kann der vierte Fall nicht vorkommen. Hiernach ist B endlich.

Da offenbar Rang $A^+ =$ Rang B^+ gilt, besitzt A^+ einen endlichen Rang. Nach wohlbekannten Resultaten [4] gilt nun $A^+ = C_1 \oplus C_2$, wobei C_1 die direkte Summe von endlich vielen Exemplaren von Prüferschen Gruppen $Z(p^\infty)$ und C_2 eine endliche Abelsche Gruppe ist. Ferner liegt jede Gruppe $Z(p^\infty)$ im zweiseitigen Annullator des Ringes A wegen der Lösbarkeit aller Gleichungen $p^k x = c$ $(c \in Z(p^\infty), x \in Z(p^\infty), k \in I, k \geqq 1)$. Da A ein V-ring ist, ergibt sich $C_1 \cong Z(p^\infty)$. Ist nun $C_2 = 0$, so ist $A \cong Z(p^\infty)$ offenbar ein V-Zeroring. Ist aber $C_2 \neq 0$, so seien $p^k C_2 = 0$, $p^{k-1} C_2 \neq 0$ und $a \in C_1 (\cong Z(p^\infty))$ mit $O(a) = p^{k+1}$. Da k eine natürliche Zahl $(k \geqq 1)$ ist, so gilt für den durch C_2 und a erzeugten (also endlich erzeugbaren) Unterring $S_2 = \{C_2, a\}$ gewiß $pS_2 \neq 0$. S_2 ist dann ein endlicher Unterring von A mit $S_2 = \{s_2\}$. Daher kann nach dem Schritt 23 $p^{k+1} s_2 = (s_2^2 - p^f s_2) s_2 - (s_2^2 - p^f s_2) = p(s_2^2 - p^f s_2) = 0$ vorausgesetzt werden $(k+1 \geqq 2, f \geqq 1, k+1 \geqq f)$. Hiernach erhält man wegen $|\{s_2^2 - p^f s_2\}| = p$ sofort $|C_2| = p$. Ferner gilt wegen der definierenden Relationen für $\{s_2\}$ auch $A = Z(p^\infty) \oplus I/(p)$, w. z. b. w.

25. Nun werden wir alle V-Ringe A mit periodischer additiver Gruppe A^+ aufzählen.

Man kann nach den Vorigen aufnehmen, daß A^+ keine p-Gruppe ist. Bekanntlich ist der Ring A die ringtheoretische direkte Summe seiner p-Komponenten $A_p (\neq 0)$, die Ideale von A sind. Jeder solche Ring A_p ist nun ein V-Ring und ein echter Unterring von A. Hiernach ist jedes A_p kommutativ. Dann ist aber auch A selbst kommutativ. Daher ist jede p-Komponente $A_p (\neq 0)$ von A einem im Satz bei I_1), II) bzw. III) vorkommenden Ringe isomorph.

26. Ist A ein ganz beliebiger V-Ring, so ist die additive Gruppe A^+ von A genau dann eine vollständige (nach der Terminologie von KAPLANSKY bzw. von L. FUCHS [4] teilbare („divisible")) Gruppe, wenn $A^2 = 0$ und entweder $A^+ \cong Z(p^\infty)$

oder $A^+ \cong \mathfrak{R}$ gelten, wobei $\mathfrak{R}$ die additive Gruppe aller rationalen Zahlen bezeichnet.

Zum Beweis nehmen wir an, daß A^+ vollständig ist. Gilt nun für ein beliebiges $a \in A$ entweder $a^2 = 0$ oder $a^3 = a^2 a \in \{a^2\} \neq 0$, so existiert in beiden Fallen eine Zahl $k(\in I, \neq 0)$ derart, daß die additive Gruppe $\{ka\}^+$ des Ringes $\{ka\} \neq 0$ die direkte Summe von zyklischen Gruppen ist. Es gilt nämlich im Falle $a^3 \in \{a^2\}$ eine Gleichung $k_1 a + \ldots + k_s a^s = 0$ $(k_i \in I, k_s a^s \neq 0)$, und hiernach ist $\{k_s a\}^+$ wirklich die direkte Summe von zyklischen Gruppen. Daher enthält aber $\{ka\}^+$ keine von Null verschiedene vollständige Untergruppe. Da nun bA^+ für jedes $b \in B$ ein homomorphes Bild von A^+ ist, und in V-Ringen $bA \subsetneq \{b\}$ gilt, ergibt sich $(ka)A = 0$. Dies bedeutet nun $aA = 0$, also wegen der vorausgesetzten Vollständigkeit von A^+ bzw. wegen der willkürlichen Wahl des Elementes a in A auch $A^2 = 0$. A ist also ein Zeroring mit $A^+ = P \oplus U$, wobei P eine periodische und U eine torsionsfreie Untergruppe in A^+ ist. Im Falle $P \neq 0$ ist gewiß $P \cong Z(p^\infty)$, und $U = 0$ wegen der Definition der V-Ringe, folglich $A = Z(p^\infty)$. Im Falle $P = 0$ ergibt sich aber $A = U \cong \mathfrak{R}$, und somit haben wir unsere Behauptung bewiesen. Für die Umkehrung verweisen wir auf den Teil b).

27. Es sei A jetzt ein V-Ring mit torsionsfreier additiver Gruppe. Nehmen wir zuerst insbesondere auch $A = \{a\}$ an. Wir beweisen, daß A^+ zyklisch ist.

Es kann nämlich nach dem Schritt 26 vorausgesetzt werden, daß A keine vollständige Gruppe ist. Dann existiert ein $n(\in I, \neq 0)$ mit $0 \neq nA \neq A$. Ferner gilt $nA = n\{a\} = \{na\}$, denn A ist ein V-Ring. Nun ergibt sich wegen $na \cdot a \in \{na\}$ eine Gleichung $na^2 = k_1(na) + \ldots + k_s(na)^s$. Ist hierbei $k_1 \neq 0$, so gibt es wegen $k_1 na \in \{na^2\}$ und wegen der Definition der V-Ringe gewiß ein Element $b \in \{a\}$ mit $k_1 na = nab$. Da A^+ torsionsfrei ist, kann es in der obigen Gleichung durch $n \neq 0$ abgekürzt werden, d. h. $k_1 a = ab$. Daher ist aber $\{a\}^+$ wegen $\{a\}^+ \cong k_1\{a\}^+ = \{k_1 a\}^+ = a\{b\}^+$ tatsächlich zyklisch. Ist dagegen $k_1 = 0$, so existiert ein Element $c \in \{a\}$ mit $(1 - k_2 n)a^2 = a^2 c$ wegen $n(1 - k_2 n)a^2 \in \{na^3\}$. Aus $\{a^2\} \cong (1 - k_2 n)\{a^2\}^+ = \{(1 - k_2 n)a^2\}^+ = a^2\{c\}^+$ ergibt sich sofort, daß $\{a^2\}^+$ zyklisch ist. Daher existiert eine Zahl $d \in I$ mit $a^3 (= a^2 a) = da^2$. Hiernach gilt aber Rang $A^+ \leqq 2$, und A^+ ist dann und nur dann zyklisch, wenn Rang $A^+ = 1$ erfüllt ist. Nehmen wir an, daß A^+ keine zyklische Gruppe ist. Dann ist A kein nilpotenter Ring, denn aus $a^k = 0$ $(a^{k-1} \neq 0)$ folgt im Falle $k \geqq 3$ offenbar $0 = a^k = a^{k-3} a^3 = da^{k-2}$, also wegen $a^{k-1} \neq 0$ auch $d = 0$. Nun zeigt aber $d = 0$ sofort, daß $a^3 = 0$, $a^2 \neq 0$ gilt, denn im Falle $a^2 = 0$ ist $\{a\}^+$ zyklisch. Also bleibt nur der Fall $a^3 = 0$, $a^2 \neq 0$ übrig. Dann gilt aber $na^2 = k_2(na)^2$ wegen $na \cdot a \in \{na\}$, was wir im entsprechenden Falle $k_1 \neq 0$ schon erledigt haben. Daher stammt nun $n(k_2 n - 1)a^2 = 0$, folglich $a^2 = 0$ wegen $n(k_2 n - 1) \neq 0$, $nA \neq A, 0$, weil A^+ torsionsfrei ist. Also kann A^+ höchstens nur dann keine zyklische Gruppe sein, wenn A kein nilpotenter Ring ist.

Unter der Voraussetzung des indirekten Beweises sei also notwendig $d \neq 0$. Ferner gilt für $b = na$ offenbar $b^3 = (na)^3 = n^3 da^2 = ndb^2$ $(nd \neq 0)$ mit $\{b\}^+ = \{na\}^+ = n\{a\}^+ \cong \{a\}^+$. Daher ist $\{b\}^+$ wegen der Voraussetzung ebenfalls nicht zyklisch. Der Unterring $S = \{b^2, nb\}$ ist echt in A wegen $nA \neq A$. Hiernach existiert ein einziges erzeugendes Element der Gestalt $s = jb^2 + knb \in S$ wegen der linearen Unabhängigkeit von b und b^2 über I, und wegen $b^3 = ndb^2$. Nun gilt wegen $nb \in S$ und nach der Vergleichung der Koeffizienten $|k| = 1$, also entweder $k = 1$ oder $k = -1$. Ohne Beschränkung der Allgemeinheit kann $k = 1$, und somit auch $s = jb^2 + nb$

vorausgesetzt werden. Da aber ebenfalls $b^2 \in S$ gilt, existieren gewisse Zahlen $l_1, l_2 \in I$ mit $b^2 = l_1 s + l_2 s^2$, denn man erhält $s^2 = n^2(jd+1)^2 b^2$ bzw. auch $s^3 = n^4 d(jd+1)^3 b^2 = n^2 d(jd+1)s^2$. Aus der Gleichung $b^2 = l_1(jb^2+nb) + l_2(jb^2+nb)^2$ folgt sofort $l_1 = 0$. Ferner gilt ebenfalls wegen Rang $\{b\}^+ = 2$ auch $1 = l_2 n^2(jd+1)^2$. Nun ergibt sich nach der letzten Gleichung $n^2 | 1$, also $n = 1$ oder $n = -1$. Beide Fälle widersprechen aber der Bedingung $nA \neq A$, womit wir Rang $A^+ = 1$ wirklich bewiesen haben. A^+ ist also zyklisch.

28. Ist nun A ein torsionsfreier V-Ring, so ist A isomorph entweder einem Unterringe des Ringes I der ganzen Zahlen oder einem Zeroringe ersten Ranges.

Man kann nämlich nach dem Schritt 26 den trivialen Fall, wenn A^+ vollständig ist, ausschließen. Hiernach gilt $nA \neq A, 0$ für ein $n (\in I, \neq 0)$. Sind nun $x, y \in A$ beliebige Elemente, so kann $S = \{nx, ny\}$ wegen $S \neq A$ durch ein Element erzeugt werden. Daher gilt $(nx)(ny) = (ny)(nx)$, folglich $n^2(xy - yx) = 0$. Da aber A^+ torsionsfrei ist, ergibt sich wegen $xy - yx = 0$ die Kommutativität von A. Ferner ist S^+ nach dem Schritt 27 zyklisch, und somit hat A^+ den Rang $A^+ = 1$. Daher ist A isomorph entweder einem Unterringe U des rationalen Zahlkörpers K_0 oder einem Zeroringe ersten Ranges. Im erstem Falle sei $mp^{-1} \in U$ mit $(m, p) = 1$, wobei p eine Primzahl bezeichnet. Da der Unterring $\{mp^{-1}\}$ sämtliche Potenzen $m^2p^{-2}, \ldots, m^kp^{-k}, \ldots$ enthält, so ist $\{mp^{-1}\}^+$ keine zyklische Gruppe. Nach 27 ist aber $\{mp^{-1}\}$ zyklisch, was hiernach nur im Falle $p | m$ möglich ist. Daher gilt in diesem Falle $A \cong U \cong kI$ $(k \in I)$.

29. Ist nun A ein beliebiger V-Ring mit gemischter additiver Gruppe A^+, so ist A isomorph einem im Satz bei VI) vorkommenden kommutativen Ringe, der die ringtheoretische direkte Summe seines maximalen periodischen Unterringes und eines torsionsfreien Unterringes ist.

Zum Beweis sei $a \in A$ ein beliebiges Element und T der maximale periodische Unterring von $\{a\}$. Nehmen wir $a \neq 0$, $O(a) = 0$ und $T \neq 0$ an. Dann ist $\{a\}/T$ ein durch ein Element erzeugter torsionsfreier V-Ring, der nach dem Schritt 28 eine unendliche zyklische additive Gruppe besitzt. Daher ist T nach [4] ein gruppentheoretischer direkter Summand von $\{a\}^+$ d. h. $\{a\}^+ = T \oplus U$, wobei $U \cong I^+$ ist. Es sei ferner $a = t_0 + u$ mit $t_0 \in T$, $u \in U$. Da nun $It_0 + U = T + U (= \{a\})$ und $It_0 \cap U = T \cap U (= 0)$ bzw. auch $It_0 \subseteq T$ gelten, und der Verband der Untergruppen von A^+ modular ist, ergibt sich wegen eines wohlbekannten Satzes für modulare Verbände sofort $T = It_0$. Wir möchten zeigen, daß der endliche Ring T halbeinfach ist. Gilt $|B| \neq p$ für jede Primzahl p, so hat B gewiß echte Unterringe nach unserem Lemma 1, [20] sowohl im Falle $|B| \geqq \aleph_0$ als auch im Falle $|B| < \aleph_0$. Es sei $|T| = m$ und $t_1 \in T$ mit $O(t_1) = p$ für ein p. Dann ist $\{t_1\}$ wegen $|T| < \aleph_0$ offenbar endlich. Ferner kann t_1 auch im Jacobsonschen Radikal J von T gewählt werden, wenn $J \neq 0$ ist, und somit enthält $\{t_1\}$ einen Unterring $\{t_2\}$ mit $t_2^2 = pt_2 = 0$. T ist nämlich ein endlicher Ring, und ein nichtidempotentes minimales Rechtsideal R ist bekanntlich nilpotent, und zwar gilt $R^2 = 0$. Ferner ist $m\{a\} = mIu$ ein zyklischer Ring, folglich gilt $m\{a\} \neq \{a\}$. Der Unterring $S = \{t_2, v\}$ $(v = pmu)$ ist hiernach in $\{a\}$ echt, und somit existiert ein erzeugendes Element der Gestalt $g = k_1 t_2 + k_2 v$. Nun erhält man wegen des zyklischen Verhaltens von $m\{a\}^+$ und wegen $mu \cdot u = kmu$ die folgenden Beziehungen: $v^2 = p^2 m^2 u^2 = kpmv$, $g^2 = k_2^2 v^2 = (k_2 km)(pk_2 v) = k_2 kmpg$, weil $t_2 v = vt_2 = 0$ und $pg = pk_2 v$ bestehen. Man sieht aber, daß $g^2 = k_2 kmpg$ mit $O(g) = 0$ der Voraussetzung $t_2 \neq 0$ widerspricht, denn $S^+ = \{g\}^+$ ist nach $g^2 \in Ig$ zyklisch. Dieser

Widerspruch bedeutet nun die Gültigkeit von $J=0$, also genau die Halbeinfachheit von T. T ist also endlicher halbeinfacher Ring, folglich nach dem Wedderburn–Artinschen Struktursatz die ringtheoretische direkte Summe von vollen Matrizenringen über Schiefkörpen. Da aber T gleichzeitig auch ein V-Ring ist, ist jede p-Komponente T_p von T dem Faktorring $I/(p)$ isomorph. Man erhält noch schärfer $T\cong I/(m)$, wobei $m=O(t_0)$ eine quadratfreie ganze rationale Zahl ist.

Es seien nun $T=\{e\}$, $e^2=e$, $O(e)=m$, m eine quadratfreie ganze Zahl, $\{a\}^+=\{e\}\oplus Iu$, $O(u)=0$, $u\neq 0$. Dann gilt $eu=ue=de$ $(d\in I)$, denn $\{a\}$ ist kommutativ, und $\{e\}$ ist ein Ideal von $\{a\}$. Ist nun $w=u-de$, so ergibt sich $ew=we=0$ und die ringtheoretische direkte Zerlegung $\{a\}=\{e\}\oplus W$ mit $W=Iw$. Es gibt nämlich Zahlen $l_1, l_2\in I$ mit $w^2-l_1w\in T$, also mit $w^2-l_1w=l_2e$, denn $(\{a\}/T)^+$ ist zyklisch. Man erhält daher durch Multiplikation von w^2-l_1w mit e sofort $l_2e^2=l_2e=0$. Hiernach gilt aber $w^2=l_1w$. Dies bedeutet nun genau die Tatsache, daß W ein Unterring von $\{a\}$ und die obige Zerlegung wirklich eine ringtheoretische direkte Zerlegung von $\{a\}$ ist. Es sei nun p_j ein beliebiger Primteiler von $m=|T|$, und $e_j\in T$ mit $e_j^2=e_j$, $O(e_j)=p_j$. Dann hat der Unterring $S_j=\{l_1e_j+w\}$ offenbar eine zyklische additive Gruppe S_j^+ wegen $(l_1e_j+w)^2=l_1(l_1e_j+w)$, denn es gilt $TW=WT=0$ $(e_j\in T,\ w\in W)$. Man erhält aber $S_je_j=\{l_1e_j\}\subseteq S_j\cap T$, folglich $S_je_j=0$ und $p_j|l_1$ wegen $O(l_1e_j+w)=0$ und $S_j\cap T=0$. Da m quadratfrei und p_j ein beliebiger Primteiler von m ist, ergibt sich $m|l_1$, und somit $l_1=lm$ $(l\in I)$, $w^2=lmw$. Es sei ferner $g=e+w$. Dann können $mlg=mlw$, $g^2=e+mlw$ und $g^2-mlg=e$ bestätigt werden. Daher gewinnen wir wegen $eg=ge=e$ sofort $(g^2-mlg)g=g^2-mlg$. Es gilt auch $m(g^2-mlg)=0$, weil $O(e)=m$ ist. Zum Schluß bemerken wir, daß $\{a\}=\{g\}=\{g^2-mlg\}\oplus\{(ml+1)g-g^2\}$ eine ringtheoretische direkte Zerlegung ist.

Nun gilt für den beliebigen V-Ring A mit gemischter additiver Gruppe eine Beziehung $A=\bigcup_{a\in A}\{a\}$. Es sei nun $\{a\}=\{e_a\}\oplus\{w_a\}$ mit periodischem $\{e_a\}$ und mit torsionsfreiem $\{w_a\}$ für jedes a, wobei es eventuell auch $e_a=0$ bzw. $w_a=0$ vorkommen kann. (Hiernach soll e_a nach Definition im allgemeinen kein idempotentes Element sein. Es kann aber im folgenden auch die notwendige Bedingung $e_a^2=e_a$ gezeigt werden.) Es sei ferner $T_A=\bigcup_{a\in A}\{e_a\}$ bzw. $W_A=\bigcup_{a\in A}\{w_a\}$. Hierbei ist der Ring W_A offenbar ein Rechtsideal von A, der ein kommutativer torsionsfreier Unterring ist. Ferner kann $S_{a,b}=\{e_a, 2w_b\}$ für jedes Paar a, b $(\in A)$ durch ein Element $g_{a,b}$ erzeugt werden, und somit läßt sich nach geeigneter Wahl von e_a auch $e_a^2=e_a$ voraussetzen, denn es gilt nach den Vorigen $\{e_a\}\cong I/(O(e_a))$. Dies ergibt sich bei der Untersuchung von $S_{a,b}=\{g_{a,b}\}$. Daher ist T_A eine elementare Abelsche Gruppe, in der jede p-Komponente $(\neq 0)$ ein Ring $\cong I/(p)$ ist. Offenbar erhält man $W_A\cdot T_A=0$. Im Falle $T_A\cdot W_A=0$ ist A gewiß kommutativ. Wäre nun $T_A\cdot W_A\neq 0$, so würden Elemente $t\in T_A$, $w\in W_A$ mit $tw\neq 0$ existieren. Dann ist $S=\{t, w\}$ kein kommutativer Ring, folglich gilt $A=\{t, w\}$. In diesem Falle gilt $t\in\{e_{a_1},\ldots, e_{a_n}\}$ mit endlich vielen $e_{a_1}, e_{a_2},\ldots, e_{a_n}$, und existiert wenigstens ein $e_a=e$ mit $e^2=e$, $we=0$, $ew\neq 0$, wobei $O(e)=m$ quadratfrei ist. Ferner gilt $ew=ke$, $k\in I$. Daher folgt aber $k^2e=(ke)^2=(ew)^2=e(we)w=0$, also $m|k^2$. Da der maximale quadratfreie Teiler von k^2 gleich dem von k ist, und m quadratfrei ist, ergibt sich $m|k$, was der Voraussetzung $ew\neq 0$ widerspricht. Hiernach gilt auch $ew=0$, und somit ist $A=T_A\oplus W_A$ eine ringtheoretische direkte Zerlegung mit dem im Satz bei VI) erwähnten Eigenschaften, denn im Falle $W_A\cong kI$ besteht offenbar $k=lm$ mit $l\in I$, $m=|T_A|<\aleph_0$. Ist nämlich $\{e_p\}$ ein beliebiger Primkörper im Ring A mit $e_p^2=e_p(\neq 0)$, $pe_p=0$, so besitzt $\{ke_p+w\}$,

wobei $\{w\} = W_A \cong kI$ ist, eine unendliche zyklische additive Gruppe wegen $(ke_p + w)^2 = k(ke_p + w)$ und $e_p w = we_p = 0$. Da aber A nach Voraussetzung ein V-Ring ist, gilt $\{ke_p\} = (ke_p + w)T_A \subseteq \{ke_p + w\} \cap T_A$, folglich $ke_p = 0$, und $p|k$ für jede Primzahl p, zu welcher ein Primkörper von Ordnung p in A existiert. Daher bedeutet $kI \cong W_A$ $(k \in I, \neq 0)$ wirklich die Endlichkeit von $m = |T_A|$ und die Gültigkeit einer Beziehung $k = lm$, w. z. b. w.

Damit haben wir den Teil a) des Beweises erledigt.

Teil b) Wir werden nun zeigen, daß die im Satz vorkommenen Ringe tatsächlich V-Ringe sind.

Fall I_1) Die Menge der endomorphen Bilder B von $A = \{a\}$, wobei $pa = a^4 - a^3 = 0$ $(a^3 \neq a^2)$ gilt, stimmt nach dem Schritt 3 des Teiles a) mit der Menge aller Unterringe von A überein. Diese Ringe sind ausführlich $\{0\}$, $\{a^2 - a^3\}$, $\{a^3\}$, $\{a - a^2\}$, $\{a^2\}$, $\{a\}$, und diese Unterringe von $\{a\}$ können ohne die Voraussetzung, daß A ein V-Ring ist, leicht durch ganz elementare Methoden bestimmt werden. Hiernach läßt sich aber jeder Unterring von $\{a\}$ durch ein Element erzeugen. Ferner gelten $(a^2 - a^3)a = 0$, $a^3 a = a^3$, $(a - a^2)a = (a - a^2)^2$, $a^2 a = (a^2)^2$. Daher ist jeder Unterring von A ein Hauptrechtsideal, w. z. b. w.

Fall I_2) Dann ist $A = \{a, b\}$ mit $pa = pb = a^2 = b^2 - b = ab - a = ba = 0$. Also ist A ein aus p^2 Elementen bestehender nichtnilpotenter und nichtkommutativer Ring mit $pA = 0$.[4] Jeder echte Unterring $S(\neq 0)$ von A hat eine zyklische additive Gruppe. Daher gilt für $S = \{k_1 a + k_2 b\}$ offenbar $(k_1 a + k_2 b)^2 = l(k_1 a + k_2 b)$ mit $k_i, l \in I$. Ist $p|l$, so ergibt sich $k_1 k_2 a + k_2^2 b = 0$, folglich $p|k_2^2$ wegen $\{a\} \cap \{b\} = 0$. Dies bedeutet aber, daß $p|k_2$, also $S = \{a\}(\neq 0)$ ist. Ist aber $(p, l) = 1$, so kann $l \equiv 1 \pmod p$ ohne Beschränkung der Allgemeinheit vorausgesetzt werden. Hiernach erhält man $k_1 k_2 a + k_2^2 b = k_1 a + k_2 b$, also $k_1 k_2 \equiv k_1 \pmod p$ und $k_2^2 \equiv k_2 \pmod p$. Da $S \neq 0$ ist, gilt $k_2 \not\equiv 0 \pmod p$ wegen $k_1 \equiv k_1 k_2 \pmod p$. Daher ergibt sich aus $k_2^2 \equiv k_2$ offenbar $k_2 \equiv 1 \pmod p$, und somit $S = \{k_1 a + b\}$. Nun zeigen aber $aa = 0$, $ab = a$, ferner $ba = 0$, $bb = b$ bzw. $(k_1 a + b)a = 0$, $(k_1 a + b)b = k_1 a + b$, daß jeder echte Unterring S von A wirklich ein Hauptrechtsideal von A ist.

Fall I_3) Es sei $A = \{a, b\}$ mit $pa = pb = a^3 = b^3 = ab = ba = a^2 - kb^2 = 0$, wobei $p \neq 2$ eine Primzahl, $k \in I$, $(p, k) = 1$ und $(-k)$ ein quadratischer Nichtrest mod p ist. Offenbar ist A dann ein aus p^3 Elementen bestehender kommutativer und nilpotenter Ring, dessen jedes Element in einer Gestalt $w = m_1 a + m_2 b + m_3 b^2$ $(m_i \in I)$ dargestellt werden kann. Es sei nun $w \neq 0$ mit $w^2 = 0$. Dann ergibt sich $w^2 = m_1^2 a^2 + m_2 b^2 = 0$, also $m_1^2 k + m_2^2 \equiv 0 \pmod p$. Ist hierbei $(m_1, p) = 1$, so existiert eine Zahl $g \in I$ mit $m_1 g \equiv 1 \pmod p$, und somit gilt $(m_2 g)^2 \equiv -k \pmod p$, was der Voraussetzung $\left(\frac{-k}{p}\right) = -1$ bezüglich des Legendreschen Symboles widerspricht. (Diese letzte arithmetische Kongruenz besitzt nämlich nach Voraussetzung keine Lösung in I.) Hiernach muß sicher $p|m_1$ bestehen, und daher folgt wegen $m_1^2 k + m_2^2 \equiv 0 \pmod p$ auch $p|m_2$. Dies bedeutet nun $w = m_3 b^2 (\neq 0)$, also $\{w\} = \{b^2\}$. Der einzige Unterring S von A mit $|S| = p$ ist dementsprechend $S = \{b^2\}$. Ist nun $S \neq A$ und $S \neq \{b^2\}$, so gilt offenbar $S = \{s\}$ mit jedem $s \in S$, für welches $S \notin \{b^2\}$ erfüllt ist,

[4] Dies ist von Professor L. RÉDEI im Falle $p = 2$ als ein „Szelescher Ring für alles" genannt worden.

denn A ist nilpotent, und ergibt sich nach dem Schritt 1 im Teil a) $|\{s\}| \leqq p^2$. Nun folgt aber unmittelbar aus den definierenden Relationen von A, daß jeder Unterring von A tatsächlich ein Hauptrechtsideal von A ist, w. z. b. w.

Fall I_4) Es seien $A=\{a, b\}$, $pa=pb=a^3=b^3=ab=ba-b^2=a^2-kb^2=0$; $p(\neq 2)$ eine Primzahl, $k \in I$, $(p, k)=1$, ferner $4k \not\equiv 1 \pmod p$, $\left(\frac{1-4k}{p}\right)=-1$. In diesem Falle ist A ein aus p^3 Elementen bestehender, nilpotenter und nichtkommutativer Ring. Ähnlich dem vorigen Falle I_3) sei wiederum $w \in A$ ein Element mit $w^2=0$ und $w \neq 0$. Dann besitzt w wegen $\{a^2\}=\{b^2\}$, ähnlich einem jeden Elemente von A, eine Gestalt $m_1a+m_2b+m_3b^2$. Daher gewinnen wir $w^2=m_1^2a^2+m_1m_2ba+$ $+m_2^2b^2=0$ wegen $ab=0$, $ab^2=b^2a=b^3=0$. Da aber $a^2=kb^2$, $(p, k)=1$, $p \neq 2$ gelten, und somit $2g \equiv 1 \pmod p$ in I lösbar ist, ergibt sich $w^2=(m_1^2k+m_1m_2+m_2^2)b^2=$ $=((m_2+m_1g)^2-m_1^2g^2(1-4k))b^2=0$. Hiernach erhält man $(m_2+m_1g)^2 \equiv$ $\equiv m_1^2g^2(1-4k) \pmod p$. Ist hierbei $(p, m_1)=1$, so ist die Kongruenz $m_1h \equiv 1 \pmod p$ in I lösbar, und daher folgt $(2hm_2+2hgm_1)^2 \equiv 1-4k \pmod p$, was der Voraussetzung $\left(\frac{1-4k}{p}\right)=-1$ widerspricht. Hiernacht gilt $p|m_1$ und auch $p|m_2$ wegen m_1^2k+ $+m_1m_2+m_2^2 \equiv 0 \pmod p$. Dies bedeutet nun genau $\{w\}=\{m_3b^2\}$. Daher ist $\{b^2\}$ $(=\{a^2\})$ der einzige Unterring von Primzahlordnung in A. Hiernach ist aber jeder Unterring S von A mit $|S|=p^2$ offenbar der Gestalt $S=\{s\}$, wobei $s \in S$ und $s \notin \{b^2\}$. Daher kann jeder echte Unterring von A durch ein Element erzeugt werden. Ferner folgen aus den definierenden Relationen sofort $(k_1a+k_2b+k_3b^2)A \subseteq \{b^2\}$ und $b^2 \in \{k_1a+k_2b+k_3b^2\}$, wenn $k_1a+k_2b+k_3b^2 \neq 0$ ist. Dies bedeutet mit anderen Worten, daß A ein V-Ring ist, w. z. b. w.

Es kann übrigens erwähnt werden, daß zu jeder ungeraden Primzahl p wenigstens ein k existiert derart, daß $1-4k \not\equiv 0 \pmod p$ und $1-4k$ ein quadratischer Nichtrest mod p ist. Im entgegengesetzten Falle wäre nämlich entweder $1-4k(\neq 0)$ ein quadratischer Rest mod p, oder $1-4k \equiv 0 \pmod p$ für jedes $p \neq 2$ und für beliebiges k mit $(p, k)=1$. Dann ist $l^2(1-4k)$ ebenfalls $\equiv 0$ bzw. ein quadratischer Rest mod p für jedes l mit $(l, p)=1$. Da nun auch $(4l, p)=1$ gilt, ergibt sich entweder $16l(l-1)(\equiv 4l(4l-4)) \equiv 0$ oder $\left(\frac{16l(l-1)}{p}\right)=\left(\frac{l}{p}\right)\cdot\left(\frac{l-1}{p}\right)=1$ für jedes l mit $(l, p)=1$. Da $\left(\frac{1}{p}\right)=1$ und $\left(\frac{l}{p}\right)=\left(\frac{l-1}{p}\right)$ $((l, p)=1)$ gelten, ergibt sich auch $\left(\frac{2}{p}\right)=1$ usw. Durch Wiederholung dieses Schrittes erhält man zum Schluß $\left(\frac{1}{p}\right)=\left(\frac{2}{p}\right)=\ldots=\left(\frac{p-1}{p}\right)=1$, was offenbar unmöglich ist. Damit wurde wirklich die Existenz eines $k \in I$ mit $4k \not\equiv 1 \pmod p$ und mit $\left(\frac{1-4k}{p}\right)=-1$ im Falle $p \neq 2$ bewiesen.[5]

[5] Meinem Kollegen K. CORRADI danke ich für diesen kurzen übersichtlichen Beweis der erwähnten arithmetischen Tatsache, d. h. für den der Existenz von solchem k zu jedem $p \neq 2$.

Fall I_5) Man kann diesen Fall ähnlich dem Fall I_4), aber dementsprechend viel leichter untersuchen, d. h. beweisen, daß der Ring $\{a, b\}$ mit $2a=2b=a^3=$ $=b^3=ab=ba-b^2=a^2-b^2=0$ wirklich ein V-Ring ist. Daher lassen wir den elementaren Beweis weg, weil eine Wiederholung nicht zweckmäßig wäre.

Fall II) Ist $A=\{a\}$ mit $p^n a=p(a^2-p^f a)=(a^2-p^f a)a-(a^2-p^f a)=0$, $2\leqq n\in I$, $1\leqq f\in I$, $f\leqq n$, so gilt eine ringtheoretische direkte Zerlegung $\{a\}=\{a^2-p^f a\}\oplus$ $\oplus\{(1+p^f a)-a^2\}$ wegen $((1+p^f)a-a^2)a=p^f((1+p^f)a-a^2)$. Jeder Unterring S von A mit der Bedingung $a^2-p^f a\notin S$ ist zyklisch, und so ist S ein Hauptideal von A in $\{(1+p^f a)-a^2\}$. Gilt aber $a^2-p^f a\in S$, so ist $S=\{a^2-p^f a, m((1+p^f a)-a^2)\}$. Es sei nun $s=a^2-p^f a+m((1+p^f)a-a^2)$. Dann erhält man wegen $p^f s=mp^f a$ offenbar $s^2-mp^f s=a^2-p^f a$, also $S=\{s\}$ wegen $a^2-p^f a\in\{s\}, m((1+p^f a)-a^2)\in\{s\}$. Da S ein Ideal von A ist, so ist A ein V-Ring.

Fall III) Im Unterfalle $A=Z(p^\infty)$ ist nichts zu beweisen. Es sei also $A=Z(p^\infty)\oplus$ $\oplus I/(p)$ mit $I/(p)=\{e\}$, wobei $pe=e^2-e=0$ gilt. Enthält ein endlich erzeugbarer echter Unterring S das Element e nicht, so ist S ein Ideal von A in $Z(p^\infty)$. Gilt aber $e\in S$, so ist $S=\{s\}$. Hierbei gelten entweder $ps=s^3-s^2=0$ (eventuell schon auch $s^2-s=0$), oder $O(s)\geqq p^2$; $p^n s=p(s^2-p^f s)=(s^2-p^f s)s-(s^2-p^f s)=0$; $n\geqq 2$, $1\leqq f\leqq n$ $(n, f\in I)$. Hiernach ist A ein V-Ring.

Fall IV) Es sei A ein solcher periodischer Ring, dessen jede p-Komponente isomorph einem bei I_1), II) bzw. III) vorkommenden Ringe ist. Ferner sei S ein endlich erzeugbarer echter Unterring von A, und $S=\sum_p \oplus S_p$ die ringtheoretische direkte Zerlegung von S in die Summe seiner p-Komponenten. Dann ist aber S_p offenbar ein Hauptideal in der entsprechenden p-Komponente A_p von A, und somit kann das Ideal S durch die Summe $s=s_{p_1}+\ldots+s_{p_n}$ der erzeugenden Elemente s_{p_i} von S_{p_i} erzeugt werden, denn der endlich erzeugte Unterring S besitzt nur endlich viele verschiedene p-Komponenten S_p. Daher ist aber S ein Hauptideal von A, und A ist ein V-Ring, w. z. b. w.

Fall V_1) Dann ist mI ein Hauptidealring, und somit ist nichts zu beweisen.

Fall V_2) Es sei A ein Zeroring, dessen additive Gruppe isomorph einer aus gewissen rationalen Zahlen bestehenden Gruppe ist. Jeder Unterring von A ist ein Ideal. Es sei ferner $S_n=\left\{\frac{s_1}{t_1}, \frac{s_2}{t_2},\ldots,\frac{s_n}{t_n}\right\}$ ein endlich erzeugter Unterring von $A(s_i, t_i\in I,$ $(s_i, t_i)=1,\ t_i\neq 0,\ i=1, 2,\ldots, n)$. Dann ist $\left\{\frac{s_1}{t_1}\right\}^+$ sicher zyklisch, und es sei nach der Induktionsvoraussetzung $S_{n-1}=\left\{\frac{s_1}{t_1}, \frac{s_2}{t_2},\ldots,\frac{s_{n-1}}{t_{n-1}}\right\}$ ebenfalls zyklisch. Dann gilt $S_{n-1}=\left\{\frac{s_0}{t_0}\right\}$ und $S_n=\left\{\frac{s_0}{t_0}, \frac{s_n}{t_n}\right\}$, und somit genügt es wesentlich nur den Fall $n=2$ zu untersuchen. Bezeichne nun $s=(s_1, s_2)$ den größten gemeinsamen Teiler von s_1 und s_2, bzw. bezeichne $t=[t_1, t_2]$ das kleinste gemeinsame Vielfaches von t_1 und t_2. Dann gilt offenbar $S=\left\{\frac{s_1}{t_1}, \frac{s_2}{t_2}\right\}\subseteq\left\{\frac{s}{t}\right\}$ wegen $\frac{s_1}{t_1}=\left(\frac{s_1}{s}\cdot\frac{t}{t_1}\right)\cdot\frac{s}{t}$ bzw. $\frac{s_2}{t_2}=$ $=\left(\frac{s_2}{s}\cdot\frac{t}{t_2}\right)\cdot\frac{s}{t}$.

Andererseits gilt $(s_1, s_2) = \left(s_1, s_2 \frac{t}{t_2}\right) = \left(s_1 \frac{t}{t_1}, s_2 \frac{t}{t_2}\right)$ wegen $\frac{t}{t_2} \Big| t_1; \left(s_1, \frac{t}{t_2}\right) = 1$ bzw. wegen $\frac{t}{t_1} \Big| t_2, \left(s_2, \frac{t}{t_1}\right) = 1$ und $\left(\frac{t}{t_1}, \frac{t}{t_2}\right) = 1$. Hiernach erhält man nach einer Multiplikation $(t_1, t_2)\cdot(s_1, s_2) = \left(s_1 \frac{t(t_1, t_2)}{t_1}, s_2 \frac{t(t_1, t_2}{t_2}\right) = (s_1 t_2, s_2 t_1)$.

Daher existieren ganze Zahlen x_1, x_2 mit $s_1 t_2 x_1 + s_2 t_1 x_2 = (s_1, s_2)\cdot(t_1, t_2)$. Teilt man beide Seiten dieser Gleichung mit $t_1 t_2$, so ergibt sich $\frac{s_1}{t_1} x_1 + \frac{s_2}{t_2} x_2 = \frac{s}{t}$, folglich $S = \left\{\frac{s_1}{t_1}, \frac{s_2}{t_2}\right\} \supseteq \left\{\frac{s}{t}\right\}$. Dies bedeutet aber mit $S \subseteqq \left\{\frac{s}{t}\right\}$ genau $S = \left\{\frac{s}{t}\right\}$. Hiernach ist A offenbar ein V-Ring.[6] (Die obige rein zahlentheoretische Tatsache, genauer nur die Existenz eines erzeugenden Elementes $\frac{s}{t}$ für $\left\{\frac{s_1}{t_1}, \frac{s_2}{t_2}\right\}$ folgt freilich leicht auch aus dem Fundamentalsatz der endlich erzeugbaren Abelschen Gruppen und aus der Bedingung, daß A^+ eine (torsionsfreie) Abelsche Gruppe von Rang 1 ist.)

Fall VI) Es sei $A = B \oplus C$, wobei jede p-Komponente ($\neq 0$) des periodischen Ringes B einem Körper $I/(p)$ isomorph ist, und C einen im Satz bei V_1) bzw. V_2) erwähnten Ring bedeutet. Es seien $S = \{a_1, a_2, \ldots, a_n\}$ ein echter Unterring von A, $a_i = b_i + c_i$ ($b_i \in B$, $c_i \in C$), $B_S = \{b_1, \ldots, b_n\}$, $C_S = \{c_1, \ldots, c_n\}$. Dann gelten $S = B_S \oplus C_S$, $B_S = \{b\}$, und $C_S = \{c\}$ mit $b^2 = b$, $O(b) = m$, wobei $m \neq 0$ eine quadratfreie ganze Zahl ist, $O(c) = 0$, $c^2 = kc$ ($k \in I$).

Ist nun entweder $k = 0$ oder $k \neq 0$, so gilt nach dem Schritt 29 im Teil a) des Beweises $p|k$ für jede solche Primzahl, zu welcher eine p-Komponente $B_p \neq 0$ existiert. Ist ferner $s = b + c$, so ergibt sich $s^2 - ks = (1-k)b$, $b_s = b$, folglich $(s^2 - ks)s = s^2 - ks$ mit $m(s^2 - ks) = 0$ und mit $(1-k, m) = 1$ wegen $m|k$. Daher existieren Zahlen $n_1, n_2 \in I$ mit $(1-k)n_1 + mn_2 = 1$. Hiernach erhält man aber $b = (1-k)n_1 b + mn_2 b = (1-k)n_1 b = n_1(s^2 - ks) \in \{s\}$ wegen $O(b) = m$. Dies bedeutet auch $c = s - b = s - n_1(s^2 - ks) \in \{s\}$, folglich $S = \{a_1, \ldots, a_n\} = \{b\} \oplus \{c\} = \{s\}$, d. h. die Existenz eines erzeugenden Elementes für S. Da $\{b\} \oplus \{c\}$ ein Ideal in A ist, somit ist A tatsächlich ein V-Ring.

Damit haben wir sowohl den Teil b) als auch den ganzen Beweis erledigt.

BEMERKUNGEN. Nach dem Satz können auch speziellere V-Ringe bestimmt werden:

1. die Ringe A, deren endlich erzeugte Unterringe ($= A$ oder $\neq A$) Hauptrechtsideale von A sind;

2. die Ringe A, deren echte (nicht notwendig endlich erzeugte) Unterringe Hauptrechtsideale in A sind;

3. die Ringe A, deren Unterringe ($= A$ oder $\neq A$) Hauptrechtsideale in A sind.

Hat ferner jeder echte Unterring S eines Ringes A die Gestalt $S = aA$ mit $a \in A$, wobei a von S abhängt, so ist jeder echte Unterring S von A ein Hauptrechtsideal nach unseren Resultaten [16]. Hiernach ist A dann ein spezieller V-Ring. Dann ist

[6] Ich danke meinem Kollegen I. KÖRNYEI für den obigen kurzen übersichtlichen Beweis von $(s_1, s_2)\cdot(t_1, t_2) = (s_1 t_2, s_2 t_1)$ im Falle $(s_1, t_1) = (s_2, t_2) = 1$.

aber A^+ keine gemischte Gruppe, obwohl die Mächtigkeit aller nichtisomorphen V-Ringen mit gemischter additiver Gruppe nach dem vorliegenden Satz das Kontinuum ist. Ferner ist dann jede endlich erzeugte Untergruppe von A^+ ein endomorphes Bild von A^+ [7].

Ist nun A ein beliebiger V-Ring, so gilt in A die sog. Rechtsidealisator-Bedingung: der Rechtsidealisator R_S von jedem echten Unterringe S von A ist größer als S. (Hierbei bedeutet R_S den größten solchen Unterring von A, der den Unterring S von A als ein Rechtsideal von R_S umfaßt.[7] Jeder V-Ring ist nämlich ein Vollrechtsidealring (d. h. sämtliche Unterringe sind Rechtsideale), und es gilt die erwähnte Rechtsidealisator-Bedingung in jedem Vollrechtsidealring. Nun möchten wir die folgenden Fragen aufwerfen:

PROBLEM 1. Es sind alle Vollrechtsidealringe (bzw. Vollidealringe, d. h. die Ringe, deren sämtliche Unterringe Ideale sind) zu bestimmen! (Dies bedeutet nach dem Beispiel des Falles I_2) im Satz tatsächlich zwei Aufgaben.)

Da in einem V-Ring nach dem Satz das untere Nilradikal und das Brown—McCoysche Radikal übereinstimmen, und jeder halbeinfache V-Ring eine subdirekte Summe von endlichen Primkörpen ist, lassen sich auch die weiteren Probleme erwähnen:

PROBLEM 2. Was für Beziehungen bestehen zwischen den Typen der verschiedenen Radikale in einem Ring mit Rechtsidealisator-Bedingung? (Z. B. alle Nilradikale, Jacobsonches, Brown—McCoysches, Fuchssches Radikal.)

PROBLEM 3. Was für Struktursätze gelten für spezielle (z. B. halbeinfache) Ringe mit Rechtsidealisator-Bedingung? (Z. B. im Falle einer festgewählten Kettenbedingung usw.)

MATHEMATISCHES FORSCHUNGSINSTITUT
DER UNGARISCHEN AKADEMIE DER WISSENSCHAFTEN,
BUDAPEST

(Eingegangen am 3. Oktober 1960.)

Literaturverzeichnis

[1] E. ARTIN, C. J. NESBITT and R. M. THRALL, *Rings with minimum condition* (Michigan, 1944).
[2] R. BAER, Situation der Untergruppen und Struktur der Gruppe, *S. B. Heidelberg Akad. Wiss.* **2** (1933), S. 12—17.
[3] R. DEDEKIND, Über Gruppen, deren sämtliche Teiler Normalteiler sind, *Math. Annalen* **48** (1897), S. 548—561.
[4] L. FUCHS, *Abelian groups* (Budapest, 1958).
[5] N. JACOBSON, *Structure of rings* (Providence, 1956).
[6] A. JONES and J. J. SCHÄFFER, Concerning the structure of certain rings, *Bol. Fac. Ingen. Agriment., Montevideo*, **6** (1957)—(1958).
[7] A. KERTÉSZ and T. SZELE, On abelian groups every finitely generated subgroup of which is an endomorphic image, *Acta Sci. Math. Szeged*, **15** (1953), S. 70—76.
[8] L. RÉDEI, Die Vollidealringe, *Monatshefte f. Math.*, **56** (1952), S. 89—95.

[7] P. A. FREUDMANN betrachtete [21], [22], [23], [24] ursprünglich die Ringe mit zweiseitiger Idealisator-Bedingung.

[9] L. RÉDEI, Vollidealringe im weiteren Sinn. I, *Acta Math. Acad. Sci. Hung.* **3** (1952) S. 243–268.
[10] L. RÉDEI, *Algebra, I,* (Leipzig, 1959).
[11] М. Шперлинг, О кольцах, каждое подкольцо которых является идеалом, Мат. Сборник **17** (1945), S. 371–384.
[12] F. Szász, On rings every subring of which is a multiple of the ring, *Publ. Math. Debrecen*, **4** (1956), S. 237–238.
[13] Ф. Сас, О кольцах, каждое подкольцо которых является прямым слагаемым кольца, Мат. Сборник, **40** (1956), S. 269–272.
[14] F. Szász, Über die homomorphen Bilder des Ringes der ganzen Zahlen und über eine verwandte Ringfamilie, *Monatshefte f. Math.*, **61** (1957), S. 37–41.
[15] F. Szász, Die explizite Bestimmung von einigen Klassen der assoziativen Ringe, *Bull. Acad. Polon. Sci. Classe III.*, **7**:**3** (1959), S. 107–110.
[16] F. Szász, Ringe, deren echte Unterringe streng zyklische Rechtsideale sind, *MTA Mat. Kut. Int. Közl.*, **5** (1960), S. 287–292.
[17] F. Szász, Über Ringe mit Minimalbedingung für Hauptrechtsideale. I, *Publ. Math. Debrecen*, **7** (1960), S. 54–64.
[18] F. Szász, Über Ringe mit Minimalbedingung für Hauptrechtsideale. II, *Acta Math. Acad. Sci. Hung.*, **12** (1961), S. 417–439.
[19] F. Szász, Les anneaux ne contenant que des sous-anneaux propres cycliques, *Czechoslovak Math. Journal*, **7** (82) (1957), S. 21–25.
[20] F. Szász, Note on rings in which every proper left-ideal is cyclic, *Fund. Math.*, **44** (1957), S. 330–332.
[21] П. А. Фрейдман, К теории радикала ассоциативного кольца, Изв. Высших Учёбных Заведений Математика, Казань, **3** (4) (1958), S. 225–232.
[22] П. А. Фрейдман, Кольца с идеализаторным условием I, Изв. Высших Учёных Заведений, Математика, Казань, **2** (15) (1960), S. 213–222.
[23] П. А. Фрейдман, Кольца с идеализаторным условием II, Учёные Записки Уральского Гос. Унив. и. А.М. Горького, Математика, Свердловск, **2** (1959), S. 35–48.
[24] П. А. Фрейдман, О кольцах разрешимого типа, Диссертация кандидата Физ.-мат. наук (Свердловск, 1960).