PACIFIC JOURNAL OF MATHEMATICS
Vol. 27, No. 2, 1968

CHARACTERIZING PRIMES IN SOME NONCOMMUTATIVE RINGS

HAROLD G. RUTHERFORD

For a ring R with identity 1, a preprime is a nonempty subset T of R which is closed under the two binary operations, addition and multiplication, of R and with $-1 \notin T$. A prime of R is a preprime of R which is maximal with respect to set inclusion. A field K is locally finite if every member of K is a member of some finite subfield of K. For a finite dimensional vector space V over K let $\mathfrak{G} = \mathrm{Hom}_K(V, V)$ denote the full ring of linear transformations of V over K. Let W and L be subspaces of V with $W \subset L \subset V$ aud $W \neq L$. Let $T(L, W) = \{\alpha \in \mathfrak{G} / \alpha \cdot L \subset W\}$. Then $T(L, W)$ is a preprime of $\mathfrak{G}$. Let

$$\mathscr{T} = \{T(L, W) / W, L \text{ are subspaces of } V, W \subset L, W \neq L\}$$

We will show that the primes of $\mathfrak{G}$ are exactly those preprimes $T(L, W) \in \mathscr{T}$ with $\dim_K L = 1 + \dim_K W$.

There is also an associative monoid with zero element reminiscent of a value group for a valuation of a field. One actually finds that this monoid is independent of which prime is used to define it. However, this shows rather that while this concept yields an abelian group when the ring is commutative, it may not be the proper concept in noncommutative rings, see [1, Prop. 2.2].

A number field is a finite field extension of the field Q of rational numbers. In [1, Prop. 3.4, 3.5, 3.6], Harrison has shown that for a number field K, the primes are exactly the useful prime divisiors of algebraic number theory and all of them when K is a normal extension of Q. Since the definition of primes is made in arbitrary rings with 1, it is desirous to investigate the concept for nonfields. Commutative rings have been investigated considerably in [1] and [3]. A locally finite field has no primes but $\{0\}$ (see [1, Lemma 1.4]). Thus one would expect $\mathfrak{G} = \mathrm{Hom}_K(V, V)$ to be one of the simplest noncommutative rings to investigate.

All rings are assumed to have an identity. If A and B are subsets of a ring R and d a member of an R-module, dA denotes $\{da / A \in A\}$, Ad denotes $\{ad / a \in A)$, $A \cdot B$ denotes $\{ab / a \in A, b \in B\}$ and $-A$ denotes $\{-a / a \in A\}$. K will denote a locally finite field, V a finite dimensional vector space over K, and $\mathfrak{G} = \mathrm{Hom}_K(V, V)$ is the ring of all K-linear transformations of V.

1. P-productive.

A prime P of a ring is called *finite* if $-1 \notin P$ *infinite* otherwise. P is finite if and only if $-P \subset P$. Since the

characteristic of K is not zero, every prime of $\mathfrak{G}$ is finite. Let P be a finite prime of $\mathfrak{G}$. Let

$$B_P = \{\alpha \in \mathfrak{G}/\alpha \cdot P \subset P\},\ C_P = \{\beta \in \mathfrak{G}/P \cdot \beta \subset P\}\ .$$

We can define $A_P = B_P \cap C_P$ since P is a finite prime. For reference see [1, Prop. 1.2, Prop. 1.3].

DEFINITION. Let P be a prime of $\mathfrak{G}$. An element x of V is called *P-productive* if $x \notin Px$. Here V is considered as a $\mathfrak{G}$-module by the operation $\alpha \cdot v = \alpha(u)$ for $\alpha \in \mathfrak{G}, v \in V$.

Let P be a prime of $\mathfrak{G}$. We consider K as embedded in $\mathfrak{G}$ by the isomorphism which sends k into $k \cdot 1_V$ for every $k \in K$, 1_V the identity linear transformation of V. A straight forward generalization of Prop. 2.1 in [1] gives that if a and b in K and their product ab is in A_P, then $a \in A_P$ or $b \in P$. This gives the following:

LEMMA 1.1. *Let P be a prime of $\mathfrak{G}$. Then $K \subset A_P$ and $K \cap P = \{0\}$.*

Proof. For any $a \in K, a \neq 0$, there is a least positive integer m with $a^m = 1$ since a is contained in a finite subfield F of K. Now suppose $a \in K \cap P, a \neq 0$. Then $a^m = 1, m$ a positive integer. Then $1 = a^m \in P$ since P is closed under multiplication. But since every prime of $\mathfrak{G}$ is finite, this cannot happen. So, $K \cap P = \{0\}$. Now for any $a \in K, a \neq 0, a^m = 1$ for some least positive integer m. Then if $a \notin A_P, a^{m-1} \in P$ and also K so $a^{m-1} = 0$ and $a = 0$ a contradiction. So $a \in A_P$. Thus $K \subset A_P$.

PROPOSITION 1.2. Let P be a prime of $\mathfrak{G}$. Then there is an element $x \in V$ which is P-productive.

Proof. For each $\alpha \in \mathfrak{G}$, define $V_\alpha = \{x \in V/(1 + \alpha) \cdot x = 0\}$. V_α is easily checked to be a subspace of V. The dimension of V over K is finite so the dimension of V_α over K is finite also. Among all $\alpha \in P$ choose a $\beta \in P$ with $\dim_K V_\beta \geqq \dim_K V_\alpha$ for all $\alpha \in P$. Just suppose $V_\beta = V$. Then $(1 + \beta)x = 0$ for all $x \in V$ and so $1 + \beta = 0$. Thus $-1 = \beta \in P$ a contradiction.

Since $V_\beta \neq V$, there is a $c \in V$ with $c \notin V_\beta$. Let $d = (1 + \beta)c$. Then d is P-productive. For if not, we would have $d \in Pd$. So there is a $\gamma \in P$ with $\gamma d = d$. Then for any $k \in K, (1 - \gamma)(1 + \beta)kc = k \cdot (1 - \gamma)(1 + \beta)c = k(1 - \gamma)d = k(d - \gamma d) = 0$. Also, for any $x \in V_\beta$, $(1 - \gamma)(1 + \beta)x = (1 - \gamma)0 = 0$. Hence $(1 + \beta - \gamma - \gamma\beta)V_\beta = 0$ so, $V_\beta \subset V_{\beta - \gamma - \gamma\beta}$ and $c \in V_{\beta - \gamma - \gamma\beta}$ and $c \notin V_\beta$. So $\dim_K V_{\beta - \gamma - \gamma\beta} > \dim_K V_\beta$ which is a contradiction for $\beta - \gamma - \gamma\beta \in P$ and $\dim_K V_\beta \geqq \dim_K V_\alpha$ for all $\alpha \in P$.

2. **Some preprimes of $\mathfrak{G}$.** Let W and L be subspaces of V with $W \subset L$ and $W \neq L$. Let $T(L, W) = \{\alpha \in \mathfrak{G} / \alpha L \subset W\}$. One may check that $T(L, W)$ is a preprime of $\mathfrak{G}$. Let $\mathscr{T} = \{T(L, W) / W$ and L subspaces of V, $W \subset L$, $W \neq L\}$. Using the fact that $\mathfrak{G}$ is transitive [2, Chapter, II, § 4] we can tell when two members of $\mathscr{T}$ are equal. The first step is given by

LEMMA 2.1. *Let $T(L, W)$ and $T(L', W')$ be members of $\mathscr{T}$. $T(L', W') \subset T(L, W)$ if and only if $W' \subset W \subset L \subset L'$.*

Proof. By choosing a basis of V in such a way that it is the extension of a basis for proper subspaces, we will use transitivity to assert the existence of linear transformations needed to give the appropriate contradictions.

$L \subset L'$. For if not, there is an $x \in L$ with $x \notin L'$. Since $W \subset L$ and $W \neq L$, there is a $y \in L, y \notin W$. Thus there is an $\alpha \in \mathfrak{G}$ with $\alpha L' = \{0\} \subset W'$ and $\alpha x = y \notin W$. So, $\alpha \in T(L', W')$ and $\alpha \notin T(L, W)$ a contradiction.

$W' \subset W$. For if not, there is an $x \in W'$ with $x \notin W$. Then since $L \subset L'$, we may find $\beta \in \mathfrak{G}$ with $\beta L' = Kx \subset W'$ and $\beta L = Kx \not\subset W$. Thus $\beta \in T(L', W')$ and $\beta \notin T(L, W)$, a contradiction.

Conversely, if $W' \subset W$ and $L \subset L'$, one easily verifies that $T(L', W') \subset T(L, W)$.

The following corollary gives the desired criterion for equality.

COROLLARY 2.2. *Let $T(L', W')$ and $T(L, W)$ be members of $\mathscr{T}$. Then $T(L', W') = T(L, W)$ if and only if $L = L'$ and $W = W'$.*

3. **The primes in $\mathfrak{G}$.** We remarked earlier that all primes of $\mathfrak{G}$ are finite since the characteristic of K is not 0. Thus

THEOREM 3.1. *$\mathscr{P} = \{T(L, W) / W$ and L are subspaces of V, $W \subset L$, $\dim_K L = 1 + \dim_K W\}$ is the set of all primes of $\mathfrak{G}$.*

Proof. Let P be a prime of $\mathfrak{G}$. There is a $v \in V$ which is P-Productive, Prop 1.2. So $v \notin Pv$. One checks that Pv is a subspace of V. Let $Pv = W$ and $L = Kv + W$. Now let $\alpha \in P$. Then $\alpha W \subset W$ and $\alpha v \in Pv = W$. So $\alpha L \subset W$. Thus $P \subset T(L, W)$. But $T(L, W)$ is a preprime containing P a maximal preprime so $P = T(L, W)$.

Conversely, let $T(L, W) \in \mathscr{P}$. Then an easy application of Zorn's lemma gives that $T(L, W)$ is contained in a prime P, since $T(L, W)$ is a preprime. But then there are L' and W' of V with $W' \subset L'$ and $\dim_K L' = 1 + \dim_K W'$ and we have $T(L, W) \subset P = T(L', W')$.

So by Lemma 2.1, $W \subset W' \subset L' \subset L$. But $\dim_K L = 1 + \dim_K W$ gives that $W = W'$ and $L = L'$ since $W' \neq L'$. Hence by Corollary 2.2, $T(L, W) = T(L', W') = P$ so $T(L, W)$ is indeed a prime.

4. **The value monoid.** For any prime P of a ring R, there is a natural subring A_P of R which contains P. In our case $A_P = B_P \cap C_P$. Then one can define for each $x \in R$, $P: x = \{(y, z)/y, z \in R, yxz \in P\}$ and for a and $b \in R$ define $a \sim b$ if $P: a = P: b$. This defines an equivalence relation on R. Let $[a]$ denote the equivalence class containing a and let Γ_P denote the set of equivalence classes of R. Define $\phi_P(a) = [a]$. Then $\phi_P: R \to \Gamma_P$. When R is a commutative ring, Γ_P is an abelian group. See [1, 11 and Prop. 2.2]. We first characterize B_P and C_P.

LEMMA 4.1. *Let P be a prime of $\mathfrak{G}$. Then there are subspaces W and L of V with $\dim_K L = 1 + \dim_K W$ and $P = T(L, W)$ by Theorem 3.1. Then $B_P = \{\alpha \in \mathfrak{G}/\alpha W \subset W\} = T(W, W)$ and $C_P = \{\alpha \in \mathfrak{G}/\alpha L \subset L\} = T(L, L)$, so that $A_P = T(L, L) \cap T(W, W)$.*

Proof. Clearly $T(L, L) \subset C_P$. Now let $\alpha \in C_P$. Suppose $\alpha L \subset L$. Let $V = L \oplus D$. Choose $\beta \in \mathfrak{G}$ with $\beta \cdot L = \{0\}$, $\beta(v) = v$ for all $v \in D$. Then $\beta \in P$ and $\beta\alpha L \not\subset L$, a contradiction. Hence $\alpha \in T(L, L)$ and $T(L, L) = C_P$. Similarly $B_P = T(W, W)$. Hence $A_P = T(L, L) \cap T(W, W)$.

Now we can be more specific that in Lemma 1.1 and give a characterization of A_P in terms of P.

PROPOSITION 4.2. Let P be a prime of $\mathfrak{G}$. Then $A_P = P \oplus K$ as K-modules.

Proof. We already know that $K \subset A_P$ and $P \cap K = \{0\}$. Thus it only remains to show that each $\alpha \in A_P$ is expressible as $\beta + k$, $\beta \in P$, $k \in K$. Let $P = T(L, W)$ as Theorem 3.1 gives. Let $L = Kv \oplus W$. Suppose $a \in A_P$. If $\alpha \in P$, $\alpha = \alpha + 0$, $0 \in K$. So if $\alpha \notin P$, $\alpha L \not\subset W$ while $\alpha L \subset L$. Thus $\alpha v = kv + w$, $k \in K$, $w \in W$. Consider $\alpha - k$. $\alpha W \subset W$ gives $(\alpha - k)W \subset W$ since $k \in A_P$. Also,

$$(\alpha - k)v = \alpha v - kv = kv + w - kv = w .$$

So $(\alpha - k)v \in W$. Thus $\alpha - k \in T(L, W) = P$. Hence

$$\alpha = (\alpha - k) + k \in P \oplus K .$$

Hence $A_P = P \oplus K$.

We are now in a position to show that the monoids corresponding to each prime P of $\mathfrak{G}$ are all the same monoid.

THEOREM 4.3. *There is a natural associative monoid Γ with zero element and a natural monoid homomorphism ϕ of $\mathfrak{S}$ onto Γ such that for each prime P of $\mathfrak{S}$, $\Gamma_P = \Gamma$ and $\phi_P = \phi$.*

Proof. We will outline the proof in the form of a series of claims, whose proofs are straight forward but often lengthy. We leave their proofs to the reader.

First of all we will show that if α and β are in $\mathfrak{S}$ and there is a $k \in K$ with $\beta = k\alpha$ then $\beta \sim_P \alpha$ where $\sim_P$ denotes the equivalence relation determined by any prime P of $\mathfrak{S}$. For if $(\gamma, \delta) \in P\colon \alpha$ then $\gamma\beta\delta = \gamma k\alpha\delta = k\gamma\alpha\delta \in KP \subset P$ since $K \subset A_P$. So $(\gamma, \delta) \in P\colon \beta$. Thus $P\colon \alpha \subset P\colon \beta$. Similarly, $P\colon \beta \subset P\colon \alpha$, so $P\colon \alpha = P\colon \beta$ and $\beta \sim_P \alpha$.

Now if conversely we can show that if $\beta \sim_P \alpha$ then $\beta = k\alpha$ for some $k \in K$ we will have shown that the equivalence relations $\sim_P$ are really all the same and hence the monoids Γ_P and monoid homomorphisms ϕ_P are all the same for each P. To this end, let $\beta \sim_P \alpha$.

Claim 1. Let Kv be any one-dimensional subspace of V. Then $\beta Kv = \alpha Kv$.

Proof. Let $\delta \in \mathfrak{S}$ with $\delta L = Kv$, $v \in V$. For (γ, δ) to be in $P\colon \alpha$, we must have $\gamma\alpha Kv \subset W$. So choosing $\gamma \in \mathfrak{S}$ with this true, one gets $(\gamma, \delta) \in P\colon \alpha = P\colon \beta$ and so $\gamma\beta Kv \subset W$. If $\beta Kv \neq \alpha Kv$, one could redefine a $\gamma_2 \in \mathfrak{S}$ with $(\gamma_1, \delta) \in P\colon \beta$ and $(\gamma_1, \delta) \notin P\colon \alpha$. This contradiction proves that $\beta Kv = \alpha Kv$, so long as $\beta Kv \neq 0$. The similar agrument beginning with β will then show that $\alpha Kv = \beta Kv$.

This gives us that if $v \in V$, there is an $a \in K$, possibly depending upon v, with $\beta v = a\alpha v$. We will show that a is independent of the choice of v.

Claim 2. If $\dim_K \alpha V > 1$, then for any v_1 and v_2 in V which are linearly independent and $\beta v_1 = b\alpha v_1$ and $\beta v_2 = c\alpha v_2$, we get $b = c$.

Proof. If αv_1 and αv_2 are linearly independent, consider $\beta(v_1 + v_2) = d\alpha(v_1 + v_2)$ and one finds that $b = d = c$. If not, there is a $v \in V$ with αv and αv_1 linearly independent, since $\dim_K \alpha V > 1$. Then also αv and αv_2 are linearly independent. Consider $\beta v = e\alpha v$. Then one finds that $b = e$ and $e = c$ so again $b = c$. This proves the claim.

Claim 3. If $\dim_K \alpha V = 1$, then $\operatorname{Ker} \alpha = \operatorname{Ker} \beta$ and $\alpha V = Kv$ for some $v \in V$ and $\beta V = Kv$ also. In addition, if $v' \in V$, $v' \notin \operatorname{Ker} \alpha$, then $\beta' v = b\alpha v'$ and indeed $\beta = b\alpha$.

Proof. For $x \in \operatorname{Ker} \alpha$, $\beta x = c\alpha x$ for some $c \in K$ and $\alpha x = 0$ so

$\beta x = 0$ so $\operatorname{Ker}\alpha \subset \operatorname{Ker}\beta$. By dimension arguments, $\operatorname{Ker}\alpha = \operatorname{Ker}\beta$. $\beta V = \alpha V$ by the Claim 1. Now any $w \in V$ is $w = x + kv'$, $x \in \operatorname{Ker}\alpha = \operatorname{Ker}\beta$ and $k \in K$. Then one checks that $\beta w = k\beta v' = bk\alpha v' = b\alpha w$ since $a\alpha x = 0 = \alpha x$. Thus $\beta = b\alpha$.

Combining the last two claims, we see that if $\dim_K \alpha V = 1$, $\beta = a\alpha$ for some $a \in K$. If $\dim_K \alpha V > 1$, then we showed a is independent of the choice of $v \in V$ used to define it. Hence again $\beta = a\alpha$. This concludes the proof that if $\beta \sim_P \alpha$, then $\beta = a\alpha$, $a \in K$.

Sincere thanks are due David Harrison for his constant inspiration while this work was being done. Few are able to transmit their enthusiasm to students as well as he, at least it is difficult to conceive of someone doing it better. I would also like to thank Merle Manis for many informative conversations as well as his computations in matrices which served as guidelines for my characterizations. Thanks are also due to the Health, Education, and Welfare Department who provided support for three years as an N.D.E.A. Fellow at New Mexico State University and to the National Science Foundations who provided support one year as an N.S.F. Trainee at the University of Oregon. Without their aid, individuals who produce well at home would be hard pressed to produce well mathematically.

BIBLIOGRAPHY

1. D. K. Harrison, *Finite and infinite primes for rings and fields*, Amer. Math. Soc. Memoirs, No. 68, 1967.
2. N. Jacobson, *Structures of Rings*, Amer. Math. Soc. 1956.
3. M. Manis, *Valuations on a commutative rings*, Ph. D. thesis, University of Oregon, 1966.

Received September 21, 1967.