On a Conjecture of I. N. Herstein

M. CHACRON

Department of Mathematics, Carleton University, Ottawa, Ontario, Canada

Communicated by I. N. Herstein

Received March 20, 1984

If \( R \) is any prime ring with center \( Z \) and Jacobson radical \( J \neq 0 \), \( A \) is any subring of \( R \) such that \( x^{-1}Ax \subseteq A \) for every unit \( x \) of \( R \), \( A \neq Z \), does it follow that \( A \supseteq I \) for some non-zero ideal \( I \) of \( R \)? In this note \( I \) will answer the question in the negative for a special class of right valuation rings \( R \), which are orders in division rings \( D \neq R \). In [1], I. N. Herstein conjectured that the answer to the question would be indeed in the negative if \( R \) is without divisors of zero. Since the considered rings \( R \) are evidently without divisors of zero they will thus verify Herstein's conjecture.

Let me first recall the definition of a valued division ring \( (D; \omega) \) (in the sense of O. F. G. Schilling). If \( D \) is any division ring, \( 0 \neq G \), is any ordered abelian group with addition, \( G^* = G \cup \{ \infty \} \), is the ordered group \( G \) with infinitely adjoined (positive infinity) then the mapping \( \omega: D \to G^* \) is a valuation of \( D \) with value group \( G \), if \( \omega \) is onto, \( \omega \) maps the group \( D^* \) of non-zero elements in \( D \) onto the group \( G \),

\[
\omega(\sigma \tau) = \omega(\sigma) + \omega(\tau),
\]

for every pair \( \sigma, \tau \in D \), and

\[
\omega(\sigma + \tau) \geq \text{Min}(\omega(\sigma), \omega(\tau)),
\]

for every pair \( \sigma, \tau \) in \( D \). The system \( (D; \omega) \) is then called a valued division ring.

As is formal, if \( R = R(D; \omega) \) is the set of elements \( \sigma \) such that

\[
\omega(\sigma) \geq 0 \quad \text{(in } G),
\]

then \( R \) is a subring of \( D \), which is a right valuation ring with center \( Z = Z_D \cap R \), where \( Z_D \) is the center of \( D \), and with Jacobson radical

\[
J = J(D; \omega) = \{ \sigma \in R | \omega(\sigma) > 0 \}.
\]
Since the value group $G$ of $\omega$ is not the zero group it follows that $R \neq D$; equivalently $J \neq 0$. An added feature of $R$ is that every one-sided ideal of $R$ is two-sided as this follows from the fact that

$$[\sigma, \tau]$$ is a unit of $R$, \hspace{1cm} (5)

where $\sigma, \tau \in D^x$, and

$$[\sigma, \tau] - \sigma^{-1} \tau^{-1} \sigma \tau.$$ \hspace{1cm} (6)

As a special case of valued division ring sufficient for the considered right valuation ring $R$, $I$ will require throughout the value group $G$ to be the ordered additive group of integers $\mathbb{Z}$. To avoid confusion, $I$ will denote the first positive integer in $G$ by $0^+$. If $\mu \in D$ is such that $\omega(\mu) = 0^+$, it is clear that $\mu$ is a principal generator of the ideal $J$:

$$J = \mu R.$$ \hspace{1cm} (7)

For general ideal $I$ or $R$, if $n = n(I)$ is the first positive integer in the set

$$\omega(I) = \{ \omega(\tau) | \tau \in I \},$$ \hspace{1cm} (8)

then $\mu^n$ is a principal generator of the ideal $I$:

$$I = \mu^n R \quad (I \neq 0, R).$$ \hspace{1cm} (9)

**Theorem 1.** Let $D$ be any division ring, let $\omega_1$ and $\omega_2$ be any pair of valuations of $D$ with same value group $G = \mathbb{Z}$. If $R_i$ is the valuation ring corresponding to $\omega_i$, $J_i$ is the Jacobson radical of $R_i$ ($i = 1, 2$), $R_1 \neq R_2$, then $R_i$ contains no non-zero ideal of $R_j$ for $i \neq j$.

**Proof.** Deny the conclusion of the theorem. If, say, $R_1$ contains some non-zero ideal $I$ of $R_2$ it follows that $R_1$ contains $J_2$. This is evidently true if $I = R_2$. If not, then $I = \mu^n R_2$, where $\omega_2(\mu) = 0^+$. Then $J_2 = (\mu R_2)^n = I \subset R_1$. If $\sigma \in J_2$ then $\sigma^n \in J_2 \subset R_1$ or $\omega_1(\sigma^n) \geq 0$. Equivalently, $\omega_1(\sigma) \geq 0$. Thus $J_2 \subseteq R_1$. I proceed to show next that $J_1 \subset R_2$. For if the latter inclusion fails then there is $\sigma \in J_1$, $\sigma \notin R_2$. Since $\sigma \notin R_2$ it follows that $\sigma^{-1} \in J_2 \subseteq R_1$. From $\sigma \in J_1$ and $\sigma^{-1} \in R_1$ would follow $1 = \sigma^{-1} \sigma \in J_1$, which is nonsense.

I claim next that $R_1 \ni R_2$. For, otherwise, choose $\tau \in R_2$, $\tau \notin R_1$. Since $J_2 \subset R_1$ it follows that $\tau \notin J_2$. Thus $\tau$ is a unit of $R_2$. From $\tau \notin R_1$ follows $\tau^{-1} \in J_1 \cap R_2$. If $\phi \in R_1$ then $\phi \tau^{-1} \in J_1 \subset R_2$, resulting in $\phi \in R_2$; this for every $\phi \in R_1$. Thus $R_1 \subseteq R_2$. From $J_2 \subset R_1$ and

$$J_2 R_1 \subset J_2 R_2 \subset J_2$$
follows $J_2$ is an ideal of $R_1$. Since $J_2 \neq 0$, $J_2 \neq R_1$ there must be $m$ such that

$$J_2 \subset \mu_1^m R_2.$$ 

From $\mu_1 \in R_1 \subseteq R_2$ and $R_1 \subseteq R_2$ follows $J_2 \subset \mu_1^m R_2$, with $\mu_1 R_2$ a right ideal of $R_2$. If $\mu_1^m R_2 \neq R_2$ then $J_2 = \mu_1^m R_2$ follows. Thus $\mu_1^m R_1 = J_2 = \mu_1^m R_2$, resulting in $R_1 = R_2$, which is contrary to hypothesis. This shows that $\mu_1^m R_2 = R_2$. Thus $\mu_1$ is a unit of $R_2$. However, from $J_2 = \mu_1^m R_1$ follows $\mu_1^m \in J_2$, which is nonsense.

The preceding argument used the inclusions $J_2 \subset R_1$ and $J_1 \subset R_2$ to arrive at the inclusion $R_1 \supseteq R_2$. By symmetry, $R_2 \supseteq R_1$ follows giving the equality $R_1 = R_2$, which is ruled out. 

**Theorem 2.** Let $D$, $\omega_1$, and $\omega_2$ be as in Theorem 1, and suppose that $D$ is non-commutative. If $R$ is any one of the $R_i$, and $A = R_1 \cap R_2$ (resp. $A = J_1 \cap J_2$) then:

1. $R$ is a right valuation ring which is an order in $D$, $R$ has center $Z = Z_D \cap R$, and $R$ has Jacobson radical $J \neq 0$.
2. $\sigma^{-1} A \sigma \subseteq A$, for every unit $\sigma$ in $R$.
3. $A \neq Z$.
4. $A$ contains no non-zero one-sided ideal of $R$.

**Proof:**

1. For $R = R(D, \omega_i)$, for some non-trivial valuation $\omega_i$ of $D$.

2. Clearly $R_i$ (resp. $J_i$) is preserved under conjugation (in $D$). Hence $R_1 \cap R_2$ (resp. $J_1 \cap J_2$) is preserved under conjugation. Since $R \subset D$ the assertion follows.

3. If $A$ were contained in $Z$, then $[D^x, D^x] \subseteq Z_D$ follows. For if $A = R_1 \cap R_2$ then from $[D^x, D^x] \subseteq R_1$ follows $[D^x, D^x] \subseteq R_1 \cap R_2 = A \subseteq Z = Z_D \cap R \subseteq Z_D$. If, on the other hand, $A = J_1 \cap J_2$, choose any $\tau \notin R_1 \cup R_2$ (possible since $R_i \neq D$ is an additive subgroup of the additive group $D$). Then $\tau^{-1} \in J_1 \cap J_2 \subseteq Z_D$. If $\sigma \in R_1 \cap R_2$, then $\tau^{-1} \sigma \in J_1 \cap J_2 \subseteq Z_D$. From $\tau^{-1}$, $\tau^{-1} \sigma \in Z_D$, this for every $\sigma \in R_1 \cap R_2$. Thus, again, $[D^x, X^x] \subseteq Z_D$. Since by Scott [2, Theorem 14.4.4] every normal subgroup of $D^x$ which is solvable must be, in fact, central, it follows that $D^x \subseteq Z_D$. Equivalently, $D$ is commutative, which contradicts the hypothesis.

4. If $A$ contains some non-zero ideal of $R$, then $R_1 \cap R_2 \supseteq A$ contains some non-zero ideal of $R$. Since $R = R_1$ or $R = R_2$, it follows that some $R_i$ contains some non-zero ideal of $R_j$ with $i \neq j$, contradicting Theorem 1. 

It is appropriate to observe that in case $A = R_1 \cap R_2$, $[R^x, R^x] \subseteq A$ follows, where $R^x$ is the group of units of $R$. In fact, $[D^x, D^x] \subseteq R_1 \cap R_2 = A$. This contrasts sharply with the Lie product.
ON A CONJECTURE OF I. N. HERSTEIN

(R, R), which by a well-known theorem of Herstein, if contained in A would force A to contain some non-zero ideal of R. Even \((R^x, R^x)\) cannot be contained in A, for if \(\sigma, \tau \in J\), then \((\sigma, \tau) = (1 + \sigma, 1 + \tau) \in (R^x, R^x)\).

It is fairly standard to construct a triple \((D; \omega_1; \omega_2)\) as in Theorem 1. Start with the real field \(\mathbb{R}\). Let \((F; \omega)\) be the field of real Laurent series

\[
\phi = \sum_{i=0}^{\infty} a_i x^{q_0 + i} \quad (a_0 \in \mathbb{R})
\]
equipped with the valuation

\[
\omega(\phi) = \begin{cases} 
\infty & \text{if } \phi = 0 \\
q_0 & \text{if } a_0 \neq 0.
\end{cases}
\]

(10)

Let \(\phi: \mathbb{Z} \to \text{Aut}(F)\) be the homomorphism from the additive group of integers \(\mathbb{Z}\) into the group of automorphisms of the field \(F\) defined by

\[
\Phi(n) = \phi \mapsto \phi^{(n)},
\]
where \(\phi^{(n)}\) is the Laurent series obtained by replacing the indeterminate \(x\) by \(2^n x\).

Let \(T_\mathbb{Z} = \{ t_r \}_{r \in \mathbb{Z}}\) be the free abelian group with generator \(t = t_1\) and product \(t_r t_{r'} = t_{r + r'}\). Let now \(D\) be the ring of series

\[
\sigma = \sum_{i=0}^{\infty} \phi_{r_i} t_{r_i} \quad (\phi_{r_i} \in F),
\]
where \((r_i)\) is an increasing sequence of integers. Addition and multiplication in \(D\) are carried out according to the following laws and their consequences:

\[
0_F \cdot t_r = 0_D; \quad (13)
\]

\[
(\phi \cdot t_g)(\psi \cdot t_h) = \phi \psi^{(g)} t_{g+h} \quad (g, h \in \mathbb{Z}; \phi, \psi \in F); \quad (14)
\]

\[
1_F \cdot t_0 = 1_D, \quad \text{the unity of} \ D. \quad (15)
\]

**Theorem 3.** There is a triple \((D; \omega_1; \omega_2)\) as in Theorem 1.

**Proof.** For \(D\) as in the preceding construction it is well known that \(D\) is a division ring; it suffices to take the trivial factor set from \(T_\mathbb{Z} \times T_\mathbb{Z}\) into \(F\) and to quote, for example, [3, pp. 23–24] for the system \((D, F, T_\mathbb{Z}, \Phi)\). That \(D\) is not commutative is clear. As a first valuation of \(D\) with value group \(\mathbb{Z}\) there is the usual valuation \(\omega_2: D \to \mathbb{Z}\) defined by

\[
\omega_2 \left( \sum_{i=0}^{\infty} \phi_{r_i} t_{r_i} \right) = r_0 \quad (\phi_{r_0} \neq 0). \quad (16)
\]
To get one other valuation $\omega_1$ with value group $\mathbb{Z}$ and such that $R_1 \neq R_2$, it suffices to extend the ground valuation $\omega$ of $F$ to $D$ by setting:

$$\omega_1 \left( \sum_{i=0}^{\infty} \phi_i t_i \right) = \omega(\phi_{r_0}) \quad (\phi_{r_0} \neq 0).$$

That $\omega_1$ maps $D$ onto $\mathbb{Z}^*$ (by convention, $\omega_1(0) = \infty$) follows evidently from the fact that $\omega$ maps $F \subseteq F \cdot t_0$ onto $\mathbb{Z}^*$. Axiom (2) is easy to verify. Axiom (1) can be readily verified using the obvious fact that

$$\omega_1(\phi^n) = \omega_1(\phi) \quad (n \in \mathbb{Z}).$$

Finally, to show that $R_1 \neq R_2$ it suffices to find $\sigma \in D$ such that $\omega_1(\sigma)$ and $\omega_2(\sigma)$ have opposite signs. If, for instance, $\sigma = x \cdot t_1$, then

$$\omega_2(\sigma) = \omega(x) = 0^+, \quad \omega_1(\sigma) = -0^+,$$

proving thereby the theorem. 

ACKNOWLEDGMENTS

I wish to express my thanks to I. N. Herstein for encouraging this work and to NSERC (Canada) for partial support (Grant A7876).

REFERENCES