

THE p -PRIMES OF A COMMUTATIVE RING

K. G. VALENTE

The p -primes of a commutative ring and their associated completions are introduced. We prove that these completions are unique up to isomorphism and give several examples.

Introduction. The theory of finite and infinite primes is well-known to be a fundamental tool in understanding algebraic number fields. A key feature of these primes is that they admit unique completions, and a great amount of information pertaining to the structure and arithmetic of a number field can be obtained by studying the completions at all primes of the field. This paper is dedicated to the introduction of the p -primes of a commutative ring, which were developed to serve as an analogue to the aforementioned classical primes.

One of the most important aspects of p -primes (where $p = 0$ or a rational prime), and the main theorem contained in this paper, is that each p -prime possesses a completion which is unique up to isomorphism. Involved in this result are three important theories: the Artin-Schreier theory of formally real fields, the work on formally p -adic fields and Kaplansky's contributions to the theory of maximally complete fields.

Throughout this discussion, all rings are assumed to be commutative. We will also adopt the usual conventions on unity: all rings have an identity, S a subring of R implies that the identity of S coincides with that of R and ring homomorphisms send identity to identity. Lastly, if A and B are sets, we write $A - B$ for $\{a \in A \mid a \notin B\}$.

0. In this opening section we wish to introduce some precursory definitions and propositions to which we will freely refer in later portions of this paper. The first such definition, which originally appeared in [4], concerns valuations of a commutative ring.

DEFINITION 0.1. Let R be a commutative ring. By a *valuation pair* of R we mean a pair (A, \mathfrak{p}) , where A is a subring of R and \mathfrak{p} is a prime ideal of A , such that for each $r \in R - A$ there exists $x \in \mathfrak{p}$ with $rx \in A - \mathfrak{p}$.

Throughout the remainder of this section let R and (A, \mathfrak{p}) be such. We may at times suppress the word "pair" and simply refer to (A, \mathfrak{p}) as a valuation of R . The domain A/\mathfrak{p} will be called the *residue class domain*,

and we write $U(A, \mathfrak{p})$ for $A - \mathfrak{p}$. Also, for convenience, we let $\text{Val}(R)$ denote the set of all valuation pairs of R and note that, for \mathfrak{m} in $\text{Spec}(R)$, we allow for a trivial valuation: (R, \mathfrak{m}) .

PROPOSITION 0.2. *With the notation as above, we have*

- (i) $A = \{r \in R \mid r\mathfrak{p} \subseteq \mathfrak{p}\}$,
- (ii) $R - \mathfrak{p}$ is closed under multiplication,
- (iii) $I(\mathfrak{p}) := \{r \in R \mid rR \subseteq \mathfrak{p}\}$ is a prime ideal of R and
- (iv) $r \in R - I(\mathfrak{p}) \Rightarrow \exists s \in R - I(\mathfrak{p})$ with $rs \in U(A, \mathfrak{p})$.

Proof. See [4].

If we consider the special case in which $R = F$ is a field, then (A, \mathfrak{p}) is a classical (non-archimedean) valuation of F . Hence A/\mathfrak{p} is a field, the *residue class field*, which we will denote by $k(A)$. Also, we have that the multiplicative group of units of A , $U(A)$, coincides with $U(A, \mathfrak{p})$. The group $\dot{F}/U(A)$ will be referred to as the *value group* of (A, \mathfrak{p}) and will be denoted by $G(A)$. To repeat: this terminology and notation will only be in effect when we are dealing with valuations of fields.

Letting

$$\eta: R \rightarrow R/I(\mathfrak{p})$$

denote the natural homomorphism, one can easily verify that

$$\hat{A} = \eta(A)_{\eta(U(A, \mathfrak{p}))} \quad (\text{the localization of } \eta(A) \text{ at } \eta(U(A, \mathfrak{p})))$$

is a valuation subring of $qf(R/I(\mathfrak{p}))$. We call \hat{A} the *valuation ring associated to* (A, \mathfrak{p})

PROPOSITION 0.3. *Let the notation be as above with*

$$\pi: A \rightarrow A/\mathfrak{p}$$

the canonical projection. Let (B, \mathfrak{p}_B) be a valuation pair of A with $\mathfrak{p} \subseteq \mathfrak{p}_B$. Then $(\pi(B), \pi(\mathfrak{p}_B))$ is a valuation pair of the residue class domain A/\mathfrak{p} . Further, in this manner,

$$\text{Val}(A, \mathfrak{p}) =: \{(B, \mathfrak{p}_B) \mid (B, \mathfrak{p}_B) \text{ is a valuation of } A \text{ with } \mathfrak{p} \subseteq \mathfrak{p}_B\}$$

corresponds bijectively with the set $\text{Val}(A/\mathfrak{p})$.

Proof. Let $(B, \mathfrak{p}_B) \in \text{Val}(A, \mathfrak{p})$ and $(C, \mathfrak{p}_C) \in \text{Val}(A/\mathfrak{p})$. It is an easy matter to verify that

$$(B, \mathfrak{p}_B) \mapsto (\pi(B), \pi(\mathfrak{p}_B))$$

gives rise to a well-defined map from $\text{Val}(A, \mathfrak{p})$ to $\text{Val}(A/\mathfrak{p})$ and that

$$(C, \mathfrak{p}_C) \mapsto (\pi^{-1}(C), \pi^{-1}(\mathfrak{p}_C))$$

determines a map from $\text{Val}(A/\mathfrak{p})$ to $\text{Val}(A, \mathfrak{p})$. Also, it is clear that

$$(\pi(\pi^{-1}(C)), \pi(\pi^{-1}(\mathfrak{p}_C))) = (C, \mathfrak{p}_C).$$

To conclude the proof, one observes that

$$\pi^{-1}(\pi(B)) \cap \mathfrak{p}_B = \pi^{-1}(\pi(\mathfrak{p}_B)).$$

Thus, appealing to Proposition 1.10 of [4], we have

$$(\pi^{-1}(\pi(B)), \pi^{-1}(\pi(\mathfrak{p}_B))) = (B, \mathfrak{p}_B),$$

and the maps we have constructed are bijections.

PROPOSITION 0.4. *Let $R = F$ be a field. Then*

$$\text{Val}(A, \mathfrak{p}) = \text{Val}(F, \mathfrak{p}).$$

Proof. Let $(B, \mathfrak{p}_B) \in \text{Val}(A, \mathfrak{p})$. By 0.3 $(\pi(B), \pi(\mathfrak{p}_B))$ is in $\text{Val}(k(A))$. Let $a \in F - B$. If $a \in A$, then $\pi(a) \in k(A) - \pi(B)$ and $\pi(A^{-1}) \in \pi(B)$. If $a \notin A$, then $a^{-1} \in \mathfrak{p}$. In either case we have $a^{-1} \in B$ and $(B, \mathfrak{p}_B) \in \text{Val}(F, \mathfrak{p})$.

Now choose $(C, \mathfrak{p}_C) \in \text{Val}(F, \mathfrak{p})$ and let $c \in C$. If we assume $c \notin A$, then $c^{-1} \in \mathfrak{p} \subseteq \mathfrak{p}_C$, and we have a contradiction (\mathfrak{p}_C is a prime ideal of C). Thus $C \subseteq A$ and (C, \mathfrak{p}_C) is in $\text{Val}(A, \mathfrak{p})$.

We close this discussion by introducing a relation on the set $U(A, \mathfrak{p})$ which will be of importance in the following section. Let T be a subset of R such that $1 \notin T$ and $A - T$ is closed under multiplication. Set

$$I(A, T) = \{a \in A \mid aT \subseteq T\},$$

and, for any prime number q ,

$$\begin{aligned} \text{Rel}(T, q) = \{ & (a, b) \in U(A, \mathfrak{p}) \times U(A, \mathfrak{p}) \mid \text{there exists} \\ & u_1, u_2 \in I(A, T) - T \text{ and } v_1, v_2 \in U(A, \mathfrak{p}) \\ & \text{with } av_1^q u_1 - bv_2^q u_2 \in I(\mathfrak{p})\}. \end{aligned}$$

PROPOSITION 0.5. *With the notation as above, $\text{Rel}(T, q)$ is an equivalence relation on $U(A, \mathfrak{p})$.*

Proof. It is clear that $\text{Rel}(T, q)$ is reflexive and symmetric. It is transitive since $I(A, T)$ and $A - T$ are multiplicatively closed and $I(\mathfrak{p})$ is an ideal of R .

For $a \in U(A, \mathfrak{p})$ we set

$$T(a)q = \{b \in U(A, \mathfrak{p}) \mid (a, b) \in \text{Rel}(T, q)\}$$

and

$$\text{REL}(T, q) = \{T(b)q \mid b \in U(A, \mathfrak{p})\}.$$

1. We are now ready to introduce the objects to which this paper is dedicated.

DEFINITION 1.1. Let R be a commutative ring, $A = (A, \mathfrak{p})$ in $\text{Val}(R)$ and $P \subseteq A$. We say (A, P) is a *prime pair* of R if the following conditions are satisfied:

- (i) $\text{char}(A/\mathfrak{p}) = 0$,
- (ii) $P + P \subseteq P$,
- (iii) $PP \subseteq P$,
- (iv) $0 \in P, -1 \notin P$,
- (v) $a, b \in A$ with $ab \in -P \Rightarrow a \in -P$ or $b \in -P$,
- (vi) $\mathfrak{p} = \{a \in A \mid aA \subseteq P\}$ and
- (vii) $a \in U(A, \mathfrak{p}) \Rightarrow \exists b \in U(A, \mathfrak{p})$ such that $ab \in I(A, P) - (-P)$ where $I(A, P) := \{a \in A \mid aP \subseteq P\}$.

We employ the notation (R, A, P) to denote R is a ring and (A, P) is a prime pair of R . Let (R, A, P) be such with $A = (A, \mathfrak{p})$. $I(\mathfrak{p}) \in \text{Spec}(R)$ will be referred to as the *core* of the prime pair.

DEFINITION 1.2. We say (A, P) is a *0-prime* of R if

- (i) $P \cap -P \subseteq \mathfrak{p}$ and
- (ii) $A^2 := \{a^2 \mid a \in A\} \subseteq P$.

DEFINITION 1.3. Let p be a rational prime. We say (A, P) is a *p-prime* of R if the following conditions are met:

- (i) $P = -P$,
- (ii) $a \in A - I(A, P) \Rightarrow \exists x \in P$ with $ax \in I(A, P) - P$,
- (iii) $p \in P$,
- (iv) $\dim(\hat{I}/p\hat{I}) < \infty$ (as a $\mathbf{Z}/p\mathbf{Z}$ vector space) where $\hat{I} = \widehat{I(A, P)}$ and
- (v) $|\text{REL}(P, q)| = q$ for every prime number q .

We point out that if (A, P) satisfies conditions (i) and (ii) of 1.3, then $(I(A, P), P)$ is a valuation pair of A . Hence (iv) makes sense. Also, $P \subseteq A$ meets the criteria necessary to construct the equivalence relation $\text{Rel}(P, q)$ as introduced in the previous section. For $p \neq 0$, the dimension of $\hat{I}/p\hat{I}$ is called the *rank* of (A, P) . We will use the terminology

“ p -prime” for either case ($p = 0$ or a rational prime) when no confusion can result. We write $P_p(R)$ for the set of all p -primes of R , and $P_p(R, J)$ for the set of all p -primes having core J .

In the discussion which follows, we use the definition of an ordering of a commutative ring as provided by [2]. For an ordering O of a ring, we say that O is *full* if $O \cap -O = \{0\}$. Set

$$\text{SRV}(R) = \{(A, O) \mid A = (A, \mathfrak{p}) \in \text{Val}(R) \text{ and } O \text{ is a full ordering of } A/\mathfrak{p}\}.$$

THEOREM 1.4. *Let R be a commutative ring, $(A, P) \in P_0(R)$ with $A = (A, \mathfrak{p})$ and $\pi: A \rightarrow A/\mathfrak{p}$ the natural projection. Then $(A, \pi(P))$ is in $\text{SRV}(R)$. Further, the mapping*

$$(A, P) \mapsto (A, \pi(P))$$

provides a bijective correspondence between $P_0(R)$ and $\text{SRV}(R)$.

Proof. The proof is a straight-forward check with

$$(A, O) \mapsto (A, \pi^{-1}(O))$$

the inverse map.

We now wish to provide an alternate characterization of p -primes ($p \neq 0$) in a field-theoretic setting. To complete this task we will make use of the concept of formally p -adic fields as defined in [5]. For a field K (of characteristic 0) and (B, \mathfrak{p}_B) a p -valuation of K , we say (B, \mathfrak{p}_B) is *strong* if $G(B)$ is a \mathbf{Z} -group and, in such a case, refer to K as a *strongly p -adic field*.

Let F be a field with valuation pairs (A, \mathfrak{p}_A) and (B, \mathfrak{p}_B) such that $\mathfrak{p}_A \subseteq \mathfrak{p}_B$. Further, we assume $\text{char}(k(A)) = 0$ and let $\pi: A \rightarrow k(A)$ be the natural map. Via 0.4, (B, \mathfrak{p}_B) can be considered to be a valuation pair of A . One can check that, with this perspective, $I(\mathfrak{p}_B) (= \{a \in A \mid aA \subseteq \mathfrak{p}_B\})$ coincides with \mathfrak{p}_A . Thus, $\pi(B) = \hat{B}$ is the valuation ring associated with (B, \mathfrak{p}_B) (as a valuation of A).

PROPOSITION 1.5. *Let q be a prime number and the notation be as above. Then*

$$|\text{REL}(\mathfrak{p}_B, q)| = |G(\hat{B})/G(\hat{B})^q|.$$

Proof. First one checks, for $a, b \in U(A)$,

$$(a, b) \in \text{Rel}(\mathfrak{p}_B, q) \Leftrightarrow aU(A)^qU(B) = bU(A)^qU(B).$$

Therefore, we may think of $\text{REL}(\mathfrak{p}_B, q)$ as the group

$$U(A)/(U(A)^q U(B)).$$

Now, we have a surjective group homomorphism

$$\Gamma: U(A) \rightarrow G(\hat{B})$$

defined as

$$\Gamma(a) = \pi(a)U(\hat{B})$$

for all $a \in U(A)$. One easily checks that $\ker(\Gamma) = U(B)$. Hence, Γ induces a group isomorphism

$$\hat{\Gamma}: U(A)/U(B) \rightarrow G(\hat{B}).$$

To complete the proof, we make use of the natural isomorphism

$$\theta: U(A)/(U(A)^q U(B)) \rightarrow (U(A)/U(B))/(U(A)/U(B))^q.$$

For a field F and p a prime number, set

$$\begin{aligned} \text{SV}(F, p) = \{ (A, \hat{B}) \mid A = (A, \mathfrak{p}_A) \in \text{Val}(F) \text{ with} \\ \text{char}(k(A)) = 0 \text{ and } \hat{B} = (\hat{B}, \mathfrak{p}_B) \text{ a} \\ \text{strong } p\text{-valuation of } k(A) \}. \end{aligned}$$

THEOREM 1.6. *For F a field and p a rational prime, the set $P_p(F)$ is in bijective correspondence with the set $\text{SV}(F, p)$. This correspondence is achieved by a mapping*

$$(A, P) \mapsto (A, \pi(I(A, P)))$$

where $\pi: A \rightarrow k(A)$ is the natural projection and

$$I(A, P) = (I(A, P), P).$$

Proof. For $(A, P) \in P_p(F)$ we know that $(I(A, P), P)$ is a valuation pair of A with $\mathfrak{p} \subseteq P$. Hence, by the remarks above

$$(A, P) \mapsto (A, \pi(I(A, P)))$$

gives a well-defined map from $P_p(F)$ to $\text{SV}(F, p)$.

Now choose $(A, \hat{B}) \in \text{SV}(F, p)$ with $A = (A, \mathfrak{p}_A)$ and $\hat{B} = (\hat{B}, \mathfrak{p}_B)$. We write B for $\pi^{-1}(\hat{B})$ and \mathfrak{p}_B for $\pi^{-1}(\mathfrak{p}_B)$. By 0.3 and 0.4 $B = (B, \mathfrak{p}_B)$ is a valuation pair of A as well as F , $\mathfrak{p}_A \subseteq \mathfrak{p}_B$ and $I(A, \mathfrak{p}_B) = B$. Lastly, using 1.5, $(A, \mathfrak{p}_B) \in P_p(F)$ and

$$(A, \hat{B}) \mapsto (A, \pi^{-1}(\mathfrak{p}_B))$$

gives a well-defined map from $\text{SV}(F, p)$ to $P_p(F)$.

Finally, it is a simple task to show that these maps are, in fact, bijections.

2. Throughout this section we let (R, A, P) be a ring with prime pair where $A = (A, \mathfrak{p})$. We write $F(R, A)$ for the quotient field of $R/I(\mathfrak{p})$ and $U(P)$ for $I(A, P) - (-P)$. We have

$$U(P) \subseteq U(A, \mathfrak{p}) \subseteq A.$$

The following proposition gives a convenient way of describing the elements of $F(R, A)$.

PROPOSITION 2.1. *With the notation as above*

$$F(R, A) = \{ \bar{r}/\bar{u} \mid r \in R \text{ and } u \in U(P) \}$$

where $\bar{r} = r + I(\mathfrak{p}) \in R/I(\mathfrak{p})$ for all $r \in R$.

Proof. Consider \bar{r}/\bar{s} in $F(R, A)$. Since $s \notin I(\mathfrak{p})$, there exists $t \in R - I(\mathfrak{p})$ such that $st \in A - \mathfrak{p}$, and we may write

$$\bar{r}/\bar{s} = \overline{rt}/\overline{st}.$$

Further, $st \in A - \mathfrak{p}$ implies the existence of $u \in A - \mathfrak{p}$ with $stu \in U(P)$. Thus,

$$\bar{r}/\bar{s} = \overline{rtu}/\overline{stu}.$$

To complete the proof, it suffices to observe that $U(P)$ and \mathfrak{p} are disjoint sets.

With the notation as in 2.1, we show that

$$\bar{A} = \{ \bar{a}/\bar{u} \mid a \in A \text{ and } u \in U(P) \},$$

$$\bar{\mathfrak{p}} = \{ \bar{x}/\bar{u} \mid x \in \mathfrak{p} \text{ and } u \in U(P) \}, \text{ and}$$

$$\bar{P} = \{ \bar{p}/\bar{u} \mid p \in P \text{ and } u \in U(P) \}.$$

THEOREM 2.2. *Let (R, A, P) be a commutative ring with prime pair where $A = (A, \mathfrak{p})$. Then $(F(R, A), \bar{A}, \bar{P})$ is a field with prime pair where $\bar{A} = (\bar{A}, \bar{\mathfrak{p}})$.*

Proof. We first note that, by definition, $U(P)$ is closed under multiplication. With this, \bar{A} is clearly a subring of $F(R, A)$ and $\bar{\mathfrak{p}}$ is a proper ideal of \bar{A} .

Claim. $(\bar{A}, \bar{\mathfrak{p}})$ is a valuation pair of $F(R, A)$.

Subproof. Let $\bar{a}_1/\bar{u}_1, \bar{a}_2/\bar{u}_2 \in \bar{A}$ with $(\bar{a}_1/\bar{u}_1)(\bar{a}_2/\bar{u}_2) \in \bar{\mathfrak{p}}$. Hence $\exists x \in \mathfrak{p}$ and $v \in U(P)$ with

$$\overline{(a_1 a_2)} / \overline{(u_1 u_2)} = \bar{x} / \bar{v}.$$

So

$$a_1 a_2 - u_1 u_2 x \in I(\mathfrak{p}) \subseteq \mathfrak{p},$$

and, as such,

$$a_1 a_2 v \in \mathfrak{p}.$$

Since $v \in U(P)$, we have

$$a_1 \in \mathfrak{p} \quad \text{or} \quad a_2 \in \mathfrak{p}.$$

Therefore

$$\bar{a}_1/\bar{u}_1 \in \bar{\mathfrak{p}} \quad \text{or} \quad \bar{a}_2/\bar{u}_2 \in \bar{\mathfrak{p}},$$

and $\bar{\mathfrak{p}}$ is a prime ideal of \bar{A} .

Let $\bar{r}/\bar{u} \in F(R, A) - \bar{A}$. Then $r \notin A$ and $\exists y \in \mathfrak{p}$ with

$$ry \in A - \mathfrak{p}.$$

Consider $\bar{y}/\bar{1} \in \bar{\mathfrak{p}}$. Just suppose $\bar{r}\bar{y}/\bar{u} \in \bar{\mathfrak{p}}$. Then $\bar{r}\bar{y}/\bar{u} = \bar{z}/\bar{w}$ for some $z \in \mathfrak{p}$ and $w \in U(P)$. Hence $ryw \in \mathfrak{p} + I(\mathfrak{p}) \subseteq \mathfrak{p}$. Thus $ry \in \mathfrak{p}$, which is a contradiction. So

$$(\bar{r}/\bar{u})(\bar{y}/\bar{1}) \in \bar{A} - \bar{\mathfrak{p}},$$

and we see $(\bar{A}, \bar{\mathfrak{p}})$ is a valuation pair of $F(R, A)$.

Claim 2. $\alpha, \beta \in \bar{A}, \alpha\beta \in -\bar{P} \Rightarrow \alpha \in -\bar{P}$ or $\beta \in -\bar{P}$.

Subproof. Choose $a, b \in A$ and $u, v \in U(P)$ with $\alpha = a/u$ and $\beta = b/v$. We have

$$\alpha\beta = -\bar{x}/\bar{w}$$

for some $x \in P$ and $w \in U(P)$. Hence

$$abw = -xuw + i$$

for some $i \in I(\mathfrak{p})$. Thus

$$abw = -(xuw + (-i)) \in -(P + P) \subseteq -P$$

(recall $uw \in U(P)$). Hence $ab \in -P$, and either $a \in -P$ or $b \in -P$. Therefore $\alpha \in -\bar{P}$ or $\beta \in -\bar{P}$.

We leave it to the reader to check that the conditions (i)–(iv) of 1.1 are met. The above claim gives (v), and the remaining requirements easily follow given that $(\bar{A}, \bar{\mathfrak{p}})$ is a valuation pair of the field $F(R, A)$, $I(\bar{P})$ is an ideal of \bar{A} and $\bar{\mathfrak{p}} \subseteq \bar{P}$.

THEOREM 2.3. *If (A, P) is a p -prime of R , then (\bar{A}, \bar{P}) is a p -prime of $F(R, A)$.*

Proof.

Case 1. $p = 0$. This case is a very straight-forward check.

Case 2. $p \neq 0$. First, recall that $(I(A, P), P)$ is a valuation of A and

$$U(P) = I(A, P) - (-P) = I(A, P) - P.$$

Clearly $\bar{P} = -\bar{P}$.

Claim 1. $\alpha \in \bar{A} - I(\bar{A}, \bar{P}) \Rightarrow \exists \pi \in \bar{P}$ with $\alpha\pi \in I(\bar{A}, \bar{P}) - \bar{P}$.

Subproof. Write $\alpha = \bar{a}/\bar{u}$. Since $\alpha \notin I(\bar{A}, \bar{P})$, $\exists x \in P$ with $ax \in I(A, P) - P$. Let $\pi = \bar{x}/\bar{1} \in \bar{P}$. We now have

$$\alpha\pi = \bar{a}\bar{x}/\bar{u} \in I(\bar{A}, \bar{P}).$$

Just suppose $\alpha\pi \in \bar{P}$. Then

$$axv \in P = -P$$

for some $v \in U(P)$. Hence $ax \in -P = P$, which contradicts our choice of x . Therefore

$$\alpha\pi \in I(\bar{A}, \bar{P}) - \bar{P}.$$

With 2.2, we have that $(I(\bar{A}, \bar{P}), \bar{P})$ is a valuation of \bar{A} with $\bar{\mathfrak{p}} \subseteq \bar{P}$, and, hence, is also a valuation of $F(R, A)$. Further, $p \in \bar{P}$.

Claim 2. $a + \mathfrak{p} \mapsto (\bar{a}/\bar{1}) + \bar{\mathfrak{p}}$ induces an isomorphism

$$\phi: qf(A/\mathfrak{p}) \rightarrow \bar{A}/\bar{\mathfrak{p}}.$$

Moreover, $\phi(\hat{I}) = (\hat{\bar{I}})$, where $\bar{I} = I(\bar{A}, \bar{P})$.

Subproof. The proof of Claim 1 of 2.2 shows that $a + \mathfrak{p} \mapsto (\bar{a}/\bar{1}) + \bar{\mathfrak{p}}$ is indeed injective. Hence, we have a well-defined homomorphism $\phi: qf(A/\mathfrak{p}) \rightarrow \bar{A}/\bar{\mathfrak{p}}$ where

$$\phi((a_1 + \mathfrak{p})/(a_2 + \mathfrak{p})) = (\bar{a}_1/\bar{a}_2) + \bar{\mathfrak{p}}.$$

It is easy to see that ϕ is a ring isomorphism.

We leave the remainder of the claim to the reader with the remark that, for $a \in A$ and $u \in U(P)$, $\bar{a}/\bar{u} \in I(\bar{A}, \bar{P})$ if and only if $a \in I(A, P)$. Clearly, with the above, we have condition (iv) of 1.3.

We now use $\bar{P} \subseteq \bar{A}$ to define the equivalence relation $\text{Rel}(\bar{P}, q)$ (for every prime number q) on the set $U(\bar{A})$.

Claim 3. For every rational prime q , $|\text{REL}(\bar{P}, q)| = q$.

Subproof. One easily checks that, for $a, b \in A - \mathfrak{p}$, $(a, b) \in \text{Rel}(P, q)$ implies $(\bar{a}, \bar{b}) \in \text{Rel}(\bar{P}, q)$, and, with this, we have a well-defined map

$$\rho(q): \text{REL}(P, q) \rightarrow \text{REL}(\bar{P}, q),$$

with

$$\rho(q)(P(a)q) = \bar{P}(\bar{a})q$$

for all $a \in U(A, \mathfrak{p})$.

Let $\alpha = \bar{a}/\bar{u}$ be in $U(\bar{A})$. Now, $\alpha = (\bar{a}/\bar{1})(\bar{1}/\bar{u})$ and $\bar{1}/\bar{u} \in U(\bar{P})$. Hence

$$(\alpha, \bar{a}) \in \text{Rel}(\bar{P}, q) \quad \text{and} \quad \rho(q)(a) = \bar{P}(\alpha)q.$$

Thus $\rho(q)$ is a surjection.

Suppose $\bar{P}(\bar{a})q = \bar{P}(\bar{b})q$ for some $a, b \in U(A, \mathfrak{p})$. Then $\exists \mu_1, \mu_2 \in U(\bar{A})$ and $\nu_1, \nu_2 \in U(\bar{P})$ with

$$\bar{a}\mu_1^q\nu_1 - \bar{b}\mu_2^q\nu_2 = 0.$$

Choose $a_1, a_2 \in U(A, \mathfrak{p})$ and $b_1, b_2, u_1, u_2, v_1, v_2 \in U(P)$ with

$$\mu_1 = \bar{a}_1/\bar{u}_1, \quad \mu_2 = \bar{a}_2/\bar{u}_2, \quad \nu_1 = \bar{b}_1/\bar{v}_1 \quad \text{and} \quad \nu_2 = \bar{b}_2/\bar{v}_2.$$

Then

$$aa_1^q(b_1u_2^qv_2) - ba_2^q(b_2u_1^qv_1) \in I(\mathfrak{p}),$$

and we see $(a, b) \in \text{Rel}(P, q)$. Hence $\rho(q)$ is injective, and the proof is complete.

DEFINITION 2.4. Given (R, A, P) a commutative ring with p -prime, we call $(F(R, A), \bar{A}, \bar{P})$ the *associated field with p -prime*.

3. By the previous section, we have a natural way to associate a field with p -prime to a commutative ring with p -prime. In light of this, we will, for the present, restrict our attention to fields with p -primes. The main theorem of this section asserts that to each such object there exists a unique “completion”.

DEFINITION 3.1. Fix $p = 0$ or a rational prime, and let (F, A, P) and (F', A', P') be fields with p -prime. We say that (F', A', P') is a *semi-immediate extension* of (F, A, P) if

- (i) F' is a field extension of F ,
- (ii) $A = A' \cap F$,
- (iii) $P = P' \cap F$,
- (iv) $k(A')$ is an algebraic extension of $k(A)$,
- (v) $[G(A') : G(A)] = 1$ and
- (vi) for $p \neq 0$, $\text{rank}(A, P) = \text{rank}(A', P')$.

As notation, we will write $(F, A, P) < (F', A', P')$ to indicate (F', A', P') is a semi-immediate extension of (F, A, P) .

PROPOSITION 3.2. For $(F, A, P) < (F', A', P')$, $I = I(A, P)$ and $I' = I(A', P')$ we have

- (i) $I = I' \cap F$,
- (ii) $\hat{I} = \hat{I}' \cap k(A)$ and
- (iii) $\hat{P} = \hat{P}' \cap k(A)$

where $\hat{}$ denotes the associated valuation.

Proof. One checks.

DEFINITION 3.3. Let $(\underline{F}, \underline{A}, \underline{P})$ be a field with p -prime. Now, $(\underline{F}, \underline{A}, \underline{P})$ is said to be *maximal as a p -primed field*, or simply *maximal*, if it admits no proper, semi-immediate, p -primed extension.

THEOREM 3.4. Fix $p = 0$ or a rational prime, and let (F, A, P) be a field with p -prime. Then, there exists a field \underline{F} with p -prime $(\underline{A}, \underline{P})$ such that

- (i) $(F, A, P) < (\underline{F}, \underline{A}, \underline{P})$ and
- (ii) $(\underline{F}, \underline{A}, \underline{P})$ is maximal.

Proof. The proof is a long, though straight-forward, check using Zorn's lemma.

PROPOSITION 3.5. Let $(\underline{F}, \underline{A}, \underline{P})$ be a maximal as a p -primed field with $\underline{A} = (\underline{A}, \underline{p})$. Then \underline{F} is maximally complete with respect to the valuation \underline{A} .

Proof. Just suppose not. Then we are assured a proper field extension \underline{F}' of \underline{F} with valuation $\underline{A}' = (\underline{A}', \underline{p}')$ such that

- (i) $\underline{A} = \underline{A}' \cap \underline{F}$,
- (ii) $[k(\underline{A}') : k(\underline{A})] = 1$ and
- (iii) $[G(\underline{A}') : G(\underline{A})] = 1$.

Let

$$i : k(\underline{A}) \rightarrow k(\underline{A}')$$

be the natural inclusion (in this case, isomorphism) and

$$\underline{P}' = (\pi')^{-1} \circ i \circ \pi(\underline{P})$$

where π and π' are the projections to residue class fields. We see (using 1.4 or 1.6) that $(\underline{F}, \underline{A}, \underline{P})$ is a proper, semi-immediate, primed extension of $(\underline{F}, \underline{A}, \underline{P})$. This contradicts our choice of $(\underline{F}, \underline{A}, \underline{P})$, and \underline{F} must be maximally complete with respect to \underline{A} .

PROPOSITION 3.6. *Fix $p = 0$ (respectively a rational prime) and (F, A, P) a field with p -prime. Let $(\underline{F}, \underline{A}, \underline{P})$ be a maximal semi-immediate extension of (F, A, P) . Then $k(A)$ is real (p -adically) closed. Further, $k(\underline{A})$ is the real (p -adic) closure of $k(A)$.*

Proof. We verify the above for $p \neq 0$ remarking that the case in which $p = 0$ is proved by a similar argument. Recall that \underline{P} provides a strong p -valuation on $k(\underline{A})$.

Just suppose that $k(\underline{A})$ is not p -adically closed. Then the p -adic closure, k , is a proper, separable, algebraic extension of $k(\underline{A})$, and k possesses a (unique) strong p -valuation (having the same p -rank) which extends the valuation determined by \underline{P} . Now, there exists a proper field extension, \underline{F}' , of \underline{F} with valuation $(\underline{A}', \underline{p}')$ such that

- (i) $\underline{A} = \underline{A}' \cap F$,
- (ii) $k(\underline{A}') = k$ and
- (iii) $[G(\underline{A}') : G(\underline{A})] = 1$.

By construction, there exists a (necessarily unique) subset, \underline{P}' , of \underline{A}' with $(\underline{F}', \underline{A}', \underline{P}')$ a p -primed field, and $(\underline{F}, \underline{A}, \underline{P}) < (\underline{F}', \underline{A}', \underline{P}')$. We now have a contradiction to the maximality of $(\underline{F}, \underline{A}, \underline{P})$. Hence $k(\underline{A})$ is p -adically closed.

To conclude the proof we need only remark that $k(\underline{A})$ is an algebraic extension of $k(A)$.

THEOREM 3.7. *Fix $p = 0$ or a rational prime, and let (F, A, P) be a p -primed field. If $(\underline{F}_1, \underline{A}_1, \underline{P}_1)$ and $(\underline{F}_2, \underline{A}_2, \underline{P}_2)$ are maximal semi-immediate extensions of (F, A, P) , then there exists an isomorphism $\theta : \underline{F}_1 \rightarrow \underline{F}_2$ such that*

- (i) $\theta(\alpha) = \alpha$ for all $\alpha \in F$,
- (ii) $\theta(\underline{A}_1) = \underline{A}_2$ and
- (iii) $\theta(\underline{P}_1) = \underline{P}_2$.

Proof. As above, we will restrict our attention to the case $p \neq 0$. We know \underline{F}_1 and \underline{F}_2 are maximally complete with respect to the valuations $\underline{A}_1 = (\underline{A}_1, \underline{p}_1)$ and $\underline{A}_2 = (\underline{A}_2, \underline{p}_2)$. Also, $k(\underline{A}_1)$ and $k(\underline{A}_2)$ are p -adic closures of $k(A)$. Hence, there exists an isomorphism $\theta: \underline{F}_1 \rightarrow \underline{F}_2$ with $\theta(\underline{A}_1) = \underline{A}_2$, $\theta(\underline{p}_1) = \underline{p}_2$ and which fixes F (see [1], Theorem 7). Thus θ induces an isomorphism

$$\hat{\theta}: k(\underline{A}_1) \rightarrow k(\underline{A}_2).$$

Since these residue class fields are p -adically closed,

$$(\pi_1(I(\underline{A}_1, \underline{P}_1)), \pi_1(\underline{P}_1)) \quad \text{and} \quad (\pi_2(I(\underline{A}_2, \underline{P}_2)), \pi_2(\underline{P}_2))$$

are (respectively) the unique p -valuations on $k(\underline{A}_1)$ and $k(\underline{A}_2)$ (respectively, where π_1 and π_2 are the natural projections). Thus

$$\hat{\theta}(\pi_1(\underline{P}_1)) = \pi_2(\underline{P}_2),$$

and, with this, one can show $\theta(\underline{P}_1) = \underline{P}_2$.

DEFINITION 3.8. Let (R, A, P) be a commutative ring with p -prime. By 3.7, $(F(R, A), \bar{A}, \bar{P})$ has a unique (up to isomorphism) maximal semi-immediate extension $(\underline{F}, \underline{A}, \underline{P})$, which we call the *completion* of R at the p -prime (A, P) .

4. In this final section we give some examples of p -primes and their completions.

EXAMPLE 4.1. F an algebraic number field. In this situation, if (A, P) is a p -prime of F , then A must be the trivial valuation (since $\text{char}(k(A)) = 0$). With this we have that $P_p(F)$, $p \neq 0$, corresponds to the set of valuations of f which extend the p -adic valuation of \mathbf{Q} (the so-called finite primes of F). On the other hand, $P_0(F)$ is simply the set of all orderings of F . The completions in this first example are either the standard valuation-theoretic completions ($p \neq 0$) or \mathbf{R} .

In particular, if $F = \mathbf{Q}$, then the p -primes correspond bijectively to the rational primes together with the unique ordering of \mathbf{Q} .

EXAMPLE 4.2. $R = \mathbf{Q}[X]$. Fix $\{0\} \neq I \in \text{Spec}(R)$ and p a rational prime. Now, R/I is a number field. For any valuation (B, \mathfrak{p}_B) of R/I which extends the p -adic valuation of \mathbf{Q} , one can verify that $\pi_I^{-1}(\mathfrak{p}_B)$ together with the trivial valuation (R, I) is a p -prime of R , where $\pi_I: R \rightarrow R/I$ is the canonical projection. We now wish to prove that every p -prime arises in this fashion.

LEMMA. Let S be a PID and (A, \mathfrak{p}) be a valuation pair of S . Then $(A_{\mathfrak{p}}, \mathfrak{p}A_{\mathfrak{p}})$ is a valuation pair of $F = \text{qf}(S)$. Further $A_{\mathfrak{p}} \cap S = A$.

Proof. Consider $s/t \in \dot{F}$. Write

$$s = \pi^m s' \quad \text{and} \quad t = \pi^n t',$$

where π generates the (prime) ideal $I(\mathfrak{p})$ in S . We now must examine cases.

Case 1. $m < n$. Then $s/t = s'/(\pi^{n-m}t')$.

Subcase 1. $s' \in \mathfrak{p} - I(\mathfrak{p})$. Then $\exists x \in S - A$ with $s'x \in U(A, \mathfrak{p})$. Thus $t/s = (\pi^{n-m}t'x)/s'x \in A_{\mathfrak{p}}$.

Subcase 2. $s' \in U(A, \mathfrak{p})$. Then $t/s \in A_{\mathfrak{p}}$.

Subcase 3. $s' \in S - A$. Then $\exists y \in \mathfrak{p}$ such that $s'y \in U(A, \mathfrak{p})$. So $t/s = (\pi^{n-m}t'y)/s'y \in A_{\mathfrak{p}}$.

Case 2. $n < m$. Examining the three subcases above, with s' replaced by t' , it follows that $s/t \in A_{\mathfrak{p}}$.

Case 3. $m = n$. Here $s/t = s'/t'$.

Subcase 1. $t' \in \mathfrak{p} - I(\mathfrak{p})$. Then $\exists x \in S - A$ such that $t'x \in U(A, \mathfrak{p})$. If $s'x \in A$, we have $s/t \in A_{\mathfrak{p}}$. Else $s'x \notin A$, and $\exists y \in \mathfrak{p}$ with $s'xy \in U(A, \mathfrak{p})$. This gives $t/s \in A_{\mathfrak{p}}$.

Subcase 2. $t' \in U(A, \mathfrak{p})$. If $s' \in A$, then $s/t \in A_{\mathfrak{p}}$. Otherwise, $\exists x \in \mathfrak{p}$ with $s'x \in U(A, \mathfrak{p})$, and $t/s \in A_{\mathfrak{p}}$.

Subcase 3. $t' \notin A$. Again (as in Subcase 1 immediately above) one can check that either s/t or t/s is in $A_{\mathfrak{p}}$.

In any event, we have shown that $(A_{\mathfrak{p}}, \mathfrak{p}A_{\mathfrak{p}})$ is a valuation pair of F . To conclude the proof of the lemma, we note that $s \in A_{\mathfrak{p}} \cap S$ implies $su = a$ for some $a \in A$ and $u \in U(A, \mathfrak{p})$. It now follows that s is also in A .

COROLLARY. Let (A, P) be a p -prime of $R = \mathbf{Q}[X]$ with $A = (A, \mathfrak{p})$. Then A is trivial (i.e. $A = R$ and $\mathfrak{p} \in \text{Spec}(R)$).

Proof. Let $A = (A, \mathfrak{p})$ be as above. Since $\text{char}(A/\mathfrak{p}) = 0$, we have that $\mathbf{Q} \subseteq U(A, \mathfrak{p})$, and, hence, $\mathbf{Q} \subseteq A_{\mathfrak{p}}$. By the lemma, $A_{\mathfrak{p}}$ is then either $\mathbf{Q}[X]_{\mathfrak{m}}$ where \mathfrak{m} is the ideal generated by some irreducible polynomial or

$$A_{\infty} := \{f/g \in \mathbf{Q}(X) \mid (f, g) = 1 \text{ and } \deg(g) \geq \deg(f)\}.$$

If $A_{\mathfrak{p}}$ is of the former type, then $A = \mathbf{Q}[X]_{\mathfrak{m}} \cap \mathbf{Q}[X] = \mathbf{Q}[X]$.

We conclude the proof by showing that $A_{\mathfrak{p}}$ could not be the latter subring. Indeed, if it were, then $A = A_{\mathfrak{p}} \cap \mathbf{Q}[X] = \mathbf{Q}$ is a valuation subring of $\mathbf{Q}[X]$; that is, $(\mathbf{Q}, \{0\})$ is a valuation pair of $\mathbf{Q}[X]$. This contradiction establishes the corollary.

With this, one checks that our initial construction accounts for all of the p -primes ($p \neq 0$) of R having core $I \neq \{0\}$.

In a similar manner, our corollary allows us to determine all of the 0-primes of R . For $I \in \text{Spec}(R)$, $P_0(R, I)$ is found by “pulling back” orderings of R/I .

We now claim that $P_0(R, \{0\})$ is empty for $p \neq 0$. If this were not the case, then there would exist a strong p -valuation of $\mathbf{Q}(X)$ necessarily extending the p -adic valuation of \mathbf{Q} . But any such extension produces either a value group which is not a \mathbf{Z} -group or a residue class field having transcendence degree 1 over $\mathbf{Z}/p\mathbf{Z}$ (see [3] and [5]).

Lastly from the construction, we already know the field with p -prime associated to each p -prime of R . Hence, with 4.1, the completions to the p -primes of R have been determined.

EXAMPLE 4.3. $F = \mathbf{Q}(X)$. As above, if (A, P) is a p -prime of F , then $\mathbf{Q} \subseteq A$. Further, for any such (non-trivial) valuation, $k(A)$ is a number field. Thus all p -primes of F are found by choosing a suitable valuation, (A, \mathfrak{p}) , of F (see 4.2) and pulling back the p -primes of $k(A)$ (see 4.1). Note that by the remark at the end of the previous example, there are no p -primes ($p \neq 0$) corresponding to the trivial valuation, while the 0-primes in this situation are exactly the orderings of F .

EXAMPLE 4.4. Let K be a formally real (respectively strongly p -adic) field. Using 1.4 (respectively 1.6), the formal power series field, $K((X))$, can be given a 0-prime (p -prime) with the natural valuation,

$$A_N := \left\{ \sum_{i=0}^{\infty} \alpha_i X^i \mid \alpha_i \in K \text{ for all } i \right\} \quad \text{and}$$

$$\mathfrak{p}_N := \left\{ \sum_{i=1}^{\infty} \beta_i X^i \mid \beta_i \in K \text{ for all } i \right\}$$

(see [6]), and the pull back of an ordering (the maximal ideal of some strong p -valuation) of $K (= A_N/\mathfrak{p}_N)$ to A_N .

Appealing to 3.5, 3.6 and [1] Theorem 6, it can be shown that, in most cases (up to appropriate embedding), the completion to a p -prime of $\mathbf{Q}(X)$ can be realized as a formal power series field as above. Let (A, P) be a p -prime of $\mathbf{Q}(X)$.

Case 1. $p = 0$.

(i) $A = \mathbf{Q}(X)$ (i.e. P is an ordering of $\mathbf{Q}(X)$). Then, \underline{F} is the real closure of $\mathbf{Q}(X)$ with respect to P , $\underline{A} = \underline{F}$ and \underline{P} is the unique ordering of \underline{F} extending P .

(ii) $A = A_\infty$. Here $\underline{F} = \tilde{\mathbf{Q}}((X))$ where $\tilde{\mathbf{Q}}$ is the real closure of \mathbf{Q} with respect to \mathbf{Q}^+ . The 0-prime of \underline{F} is as described above.

(iii) $A = \mathbf{Q}[X]_{\mathfrak{m}}$. The completion, \underline{F} , is given by $\tilde{k}(\mathfrak{m}, P)((X))$ where $\tilde{k}(\mathfrak{m}, P)$ is the real closure of $k = \mathbf{Q}[X]/\mathfrak{m}$ at the ordering induced by P .

Case 2. $p \neq 0$.

(i) $A = A_\infty$. In this case, $\underline{F} = \mathbf{Q}_p((X))$ where \mathbf{Q}_p denotes the field of p -adic numbers.

(ii) $A = \mathbf{Q}[X]_{\mathfrak{m}}$. Here we have $\underline{F} = \bar{k}(\mathfrak{m}, P)((X))$ where $\bar{k}(\mathfrak{m}, P)$ is the valuation-theoretic completion of $k = \mathbf{Q}[X]/\mathfrak{m}$ with respect to the strong p -valuation induced by $(I(A, P), P)$.

REFERENCES

- [1] I. Kaplansky, *Maximal fields with valuation*, I, Duke J. Math., **9** (1942), 303–321.
- [2] T.Y. Lam, *An Introduction to Real Algebra*, Lecture Notes, Sexta Escuela Latinoamericana de Matematicas, Oaxtepec, Mexico, 1982.
- [3] S. MacLane, *A construction for absolute values in polynomial rings*, Trans. Amer. Math. Soc., **40** (1936), 363–395.
- [4] M. Manis, *Valuations on a commutative ring*, Thesis, Univ. of Oregon, Eugene, Oregon, 1966.
- [5] A. Prestal and P. Roquette, *Formally p -adic Fields*, Lecture Notes in Math. No. 1050, Springer-Verlag, Berlin, 1980.
- [6] O. F. G. Schilling, *The Theory of Valuations*, Math. Surveys No. IV, Amer. Math. Soc., New York, 1950.

Received November 6, 1985. This work represents a portion of the author's Ph.D. dissertation which was completed under the guidance of D. K. Harrison at the University of Oregon.

UNIVERSITY OF CALIFORNIA
BERKELEY, CA 94720