QUESTION: (HD1203) I would like to know if there is any characterization for rings in which the two concepts "Prime" and "Irreducible" for their elements are the same.

Answer: As there are various definitions of an "irreducible" element in general commutative rings, I will concentrate on the case of integral domains. For this we need to prepare, for general readers.

Let D be an integral domain with quotient field K and let $F(D)$ denote the set of nonzero fractional ideals of D. Define for $A \in F(D)$, $A^{-1} = \{x \in K : xA \subseteq D\}$. It is well known that $A^{-1} \in F(D)$, for each $A \in F(D)$. Now define for $A \in F(D)$, $A_v = (A^{-1})^{-1}$. Obviously $A_v \in F(D)$ for each $A \in F(D)$. As shown in part (1) of Theorem 34.1 of Gilmer's book [G] on multiplicative ideal theory for each $A \in F(D)$, $A_v = \bigcap_{A \subseteq \frac{r}{s}D} \frac{r}{s}D$ where $r, s \in D\backslash\{0\}$. Now as $D \subseteq \frac{r}{s}D$, for $r, s \in D\backslash\{0\}$, if and only if $r \mid s$ we conclude that $A_v = D \Leftrightarrow A \subseteq \frac{r}{s}D$ implies $r \mid s$.

Two elements $a, b \in D$ are said to be v-coprime if $(a, b)_v = D$ (Compare with "$a, b \in D$ are coprime if $GCD(a, b) = 1$".) Let me refer you to [Z] "What v-coprimality can do for you" for a more detailed study of the topic. For now let me note, with reference to [Z], that

Note 1. for $a, b \in D$, $(a, b)_v = D \Leftrightarrow aD \cap bD = abD$

Note 2. if for $a, b, c \in D\backslash\{0\}$, $a \mid bc$ and $(a, b)_v = D$, then $a \mid c$. (For $x, y \in D$, $x \mid y$ denotes "x divides y" which means that $y = xd$ for some $d \in D$.)

An element $x \in D$ is said to be irreducible if x is a nonzero nonunit such that $x = ab \Rightarrow a$ is a unit or b is a unit. That is an irreducible element x of D is a nonzero nonunit that cannot be expressed as a product of two nonunits of D; an irreducible element of a domain is also called an atom. On the other hand a prime p is a nonzero nonunit such that for all $a, b \in D$, $p \mid ab$ implies $p \mid a$ or $p \mid b$. (Equivalently a prime is a nonzero nonunit p with the property that if $p \mid ab$ and $p \nmid a$ then $p \mid b$. Indeed a prime is irreducible.)

To answer your question (for integral domains) I start with the following criterion for an atom to be a prime.

Observation 1. An atom a in an integral domain D is a prime if and only if $a \nmid b$ implies that $(a, b)_v = D$, for all $b \in D$.

Proof. Suppose that a is a prime and suppose that $a \nmid b$. To show that $(a, b)_v = D$ we assume that $(a, b) \subseteq \frac{r}{s}D$, for some $r, s \in D\backslash\{0\}$ and show that $r \mid s$, using the fact that a is a prime. So let $(a, b) \subseteq \frac{r}{s}D$. Then $s(a, b) \subseteq rD$ which gives $r \mid sa, sb$. Now $r \mid sa, sb$ means that

$sa = rm$ ....(A)

and

$sb = rn$ ....(B)

From (A) we get $a \mid rm$. Since a is a prime we have $a \mid r$ or $a \mid m$. So for some r_1, m_1, $r = r_1a$ or $m = m_1a$.

Suppose $a \mid m$, that is $m = m_1a$. Substituting in (A) we get $sa = rm_1a$ and consequently $s = rm_1$ which forces $r \mid s$.

Suppose next that $r = r_1 a$. Substituting in (A) we get $sa = r_1 am$. So $s = r_1 m$. Substituting this value of s in (B) we get $r_1 mb = rn$. Since $r = r_1 a$ we get $mb = an$. Since $a \nmid b$, $a \mid m$. But as we have seen above $a \mid m$ directly gives $r \mid s$ from (A). So in both cases we end up with $r \mid s$ whenever $(a,b) \subseteq \frac{r}{s}D$, which forces $(a,b)_v = D$.

Conversely suppose that a is irreducible such that for all $b \in D$ $a \nmid b$ implies that $(a,b)_v = D$. Now consider $a \mid bc$ for $b, c \in D \backslash \{0\}$. If $a \nmid b$ then by the given $(a,b)_v = D$. But then $a \mid bc$ and $(a,b)_v = D$ gives $a \mid c$ by Note 2, above.

This obviously leads to the following observation.

Observation 2. Let D be an integral domain. Then the concepts of irreducible and prime in D coincide if and only if for each irreducible element a of D $a \nmid b$ implies $(a,b)_v = D$ for all $b \in D$. Equivalently the concepts of "irreducible" and "prime" in D coincide if and only if for each irreducible element a of D $a \nmid b$ implies $aD \cap bD = abD$ for all $b \in D$.

An integral domain D is said to be an AP domain if in D the "atoms" are "primes". Next we make the following observation.

Observation 3. For X an indeterminate over D and for $a, b \in D \backslash \{0\}$ $aX + b$ is a prime in $D[X]$ if and only if $(a,b)_v = D$.

Proof. Suppose $aX + b$ is a prime and let $(a,b) \subseteq \frac{r}{s}D$ where $r, s \in D \backslash \{0\}$. Then, in $D[X]$, $r \mid s(aX+b)$. So there is $g(X) \in D[X]$ such that $s(aX+b) = rg(X)$. Since $aX + b$ is a prime in $D[X]$ and since r is of degree 0, we have $g(x) = t(aX+b)$ and this forces $r \mid s$. Thus $(a,b)_v = D$. Conversely suppose that $(a,b)_v = D$ and consider $aX + b \mid f(X)g(X)$. Since $aX + b$ is a prime in $K[X]$, $aX + b \mid f(X)$, say, in $K[X]$. Thus $f(X) = (aX+b)h(X)$ where $h(X) \in K[X]$. If we show that $h(X) \in D[X]$ we have completed the proof. We shall prove this by showing that $A_{h(X)} \subseteq D$ where $A_{h(X)}$ denotes the ideal generated by the coefficients of $h(X)$. By Dedekind-Merten Lemma (see e.g. [G, page 343]), given $f(X) = (aX+b)h(X)$ there is a positive integer k such that $A^{k+1}_{(aX+b)} A_{h(X)} = A^{k}_{(aX+b)} A_{(aX+b)h(X)}$. Applying the v-operation to both sides and noting that $(A_{(aX+b)})_v = (a,b)_v = D$ we get $(A_{h(X)})_v = (A_{(AX+b)h(X)})_v = (A_{f(X)})_v \subseteq D$ as $f(X)$ has all its coefficients in D. But then $A_{h(X)} \subseteq (A_{h(X)})_v \subseteq D$.

Using the above we can make the following observation.

Observation 4. An irreducible element a of D is a prime if and only if for all $b \in D$, $a \mid b$ in D or $aX + b$ is a prime in $D[X]$.

Of course a corresponding characterization for an AP- domain can be derived from Observation 4.

Observation 5. Let a be an irreducible element in an integral domain D. Then

(i) a is not a prime if and only if there is a $b \in D$ such that $a \nmid b$ and $(a,b)_v \neq D$,

(ii) a is not a prime if and only if there is a $b \in D$ such that $a \nmid b$ and $aX + b$ is not a prime in $D[X]$.

((i) is equivalent to Observation 1 and (ii) is equivalent to Observation 4.)

((Note added on May 6th, 2012: Tiberiu Dumitrescu has pointed out that both Observations 1 and 4, which are equivalent anyway, characterize a prime.

To see this we proceed as follows.

Observation 1'. A nonzero nonunit $a \in D$ is a prime if and only if $a \nmid b$ implies that $(a, b)_v = D$.

Proof. All we need show is that if $a \nmid b$ implies that $(a, b)_v = 1$ then a is irreducible and let Observation 1 do the rest. For this let $a = cb$ where $x, y \in D$. Now suppose that $a \nmid b$. Then by the condition $(a, b)_v = D$. But as $b \mid a$ we conclude that b must be a unit. Thus $a = cb$ implies that b is a unit or c is. That is a is irreducible.

Looking back and noting that if a is an atom in a domain D then $a \nmid b$ translates to $GCD(a, b) = 1$, we can rewrite Observation 1 as the following observation.

Observation 1". An atom $a \in D$ is a prime if and only if $GCD(a, b) = 1$ implies that $(a, b)_v = D$.

Proof. Since a is an atom $GCD(a, b) = 1$ is obviously equivalent to $a \nmid b$ and so Observation 1 applies.

Remark. Note that if we do not assume that a is an atom then, in Observation 1", "$GCD(a, b) = 1$ implies that $(a, b)_v = D$" does not deliver a prime. To see this let a be a nonzero nonunit in a nondiscrete rank 1 valuation domain D. Then for all nonunit $b \in D$, $GCD(a, b) \neq 1$ and so "$GCD(a, b) = 1$ implies that $(a, b)_v = D$" holds vacuously and if b is a unit then $GCD(a, b) = 1$ and $V = (a, b) = (a, b)_v$ and so "$GCD(a, b) = 1$ implies that $(a, b)_v = D$" holds good even in this case. But not a single nonzero nonunit element of a nondiscrete rank one valuation domain is irreducible, let alone a prime. So we have the following as an improvement on Observation 2.))

Observation 6. A integral domain D is an AP-domain if and only if for every atom $a \in D$, $GCD(a, x) = 1 \Rightarrow (a, x)_v$ for all $x \in D$.

So, in particular, domains in which $GCD(a, b) = 1 \Rightarrow (a, b)_v = D$ for all $a, b \in D$ are AP domains. The property: $GCD(a, b) = 1 \Rightarrow (a, b)_v = D$ for all $a, b \in D$ was called the property λ in [MZ] where it was shown in Proposition 6.4 that an atomic domain with property λ is a UFD. Of historical interest here is Corollary 6.5 of [MZ] which says: In a domain D with property λ every atom is a prime. By the way, the property λ is a generalization of Cohn's Pre-Bezout Property: $GCD(a, b) = 1 \Rightarrow (a, b) = D$ for all $a, b \in D$ stated slightly differently in [C]. Now there are a lot of integral domains that satisfy the AP property. I would refer you to [AZ] to verify the claims I make below.

(1) pre-Schreier domains: For all $a, b, c \in D \backslash \{0\}$ $a \mid bc \Rightarrow a = rs$ where $r \mid b$ and $s \mid c$. (A generalization of Cohn's Schreier domains, Schreier = pre-Schreier + integrally closed.) In a pre-Schreier domain D, $GCD(a_{1,} ..., a_n) = 1$ $\Rightarrow (a_{1,} ..., a_n)_v = D$.

(2) PSP-domains: Every primitive polynomial in the ring of polynomials is super-primitive. (A polynomial f is primitive if the GCD of its coefficients is 1 and super-primitive if $(A_f)_v = D$.) So obviously a pre-Schreier domain is a PSP domain. So, in particular, if $f = aX + b$ is a linear primitive polynomial in a PSP-domain, then $(A_f)_v = D$, i.e., $GCD(a, b) = 1 \Rightarrow (a, b)_v = D$. So a PSP-domain has the property λ.

(3) GL-domains: Domains over which the product of primitive polynomials is primitive.

On page 54 of [AZ] there is a nice picture that sums it all up. In short it says that: GCD property $\Rightarrow$ Pre-Schreier property $\Rightarrow$ PSP property$\Rightarrow$ GL property $\Rightarrow$ AP property and in section 3 of [AZ] you can find proofs or references to proofs that none of the arrows can be reversed. You may look up Anderson and Quintero's paper [AQ] to see more generalizations of GCD domains and proofs of nonreversal of the above arrows. (A domain D has the GCD property if every pair of nonzero elements of D have a GCD. It was shown in [C] that a GCD-domain is a Schreier domain.)

Now we know that GCD $\Rightarrow$ pre-Schreier $\Rightarrow$ PSP $\Rightarrow$ property λ and we have seen that property $\lambda \Rightarrow$ AP. This leads to the inevitable question: Can the last arrow be reversed? Sadly this last arrow cannot be reversed as well. In [AS] Arnold and Sheldon study a domain with the GL property and show in Proposition 2.9 of [AS] that the GL domain in question does not have the PSP property by showing that there exist two elements X and Y such that $GCD(X,Y) = 1$ but $(X,Y)_v \neq D$. Thus a GL-domain, which is an AP-domain, does not have the property λ. Indeed, one may conclude that, Observation 6, along with its equivalents, is the only available, simpler, characterization of domains in which the concepts of "irreducible" and "prime" coincide.

Muhammad Zafrullah

04-12-2012

Acknowledgement (added on 5-16-2012) I am thankful to Tiberiu Dumitrescu for a careful readin and for the remark mentioned above.

References.

[AQ] D.D. Anderson and R.O. Quintero, Some generalizations of GCD domains, in Factorization in Integral Domains (ed. D.D. Anderson) Marcel Dekker, New York, 1997, 189-195.

[AZ] Daniel Anderson and Muhammad Zafrullah, The Schreier property and Gauss' lemma, Boll. U. M. I. (8) 10-B (2007), 43-62.

[AS] Jimmy Arnold and Philip Sheldon, Integral domains that satisfy Gauss's lemma, Michigan Math. J. 22 (1975), 39-51.

[C] Paul Cohn, Bezout rings and their subrings, Proc. Cambridge Phil. Soc. 64 (1968), 251-264.

[G] Robert Gilmer, Multiplicative Ideal Theory, Marcel Dekker, 1972.

[MZ] Joe Mott and M. Zafrullah, On Prüfer v-multiplication domains, Manuscripta Math. 35(1981), 1-26.

[Z] Muhammad Zafrullah, What v-coprimality can do for you. Multiplicative ideal theory in commutative algebra, 387–404, Springer, New York, 2006.