Math 494 Discussion | Localization | February 5th

Q: Why can't you grow wheat in $\mathbb{Z}/6\mathbb{Z}$?

All rings in this note are commutative.

Definition. Let $f\colon A \to B$ be a ring homomorphism. The *extension* of an ideal $\mathfrak{a}$ of A is the ideal of B generated by $f(\mathfrak{a})$, denoted $\mathfrak{a}^e$. The *contraction* of an ideal $\mathfrak{b}$ of B is $f^{-1}(\mathfrak{b})$, denoted $\mathfrak{b}^c$.

Proposition. *Let $f : A \to B$ be a ring homomorphism and $\mathfrak{a} \subset A$, $\mathfrak{b} \subset B$ non-zero ideals. Then*

1. $\mathfrak{a} \subset \mathfrak{a}^{ec}$, $\mathfrak{b}^{ce} \subset \mathfrak{b}$*;*
2. $\mathfrak{a}^e = \mathfrak{a}^{ece}$, $\mathfrak{b}^{cec} = \mathfrak{b}^c$*;*
3. *If C is the set of contracted ideals in A and if E is the set of extended ideals in B, then $C = \{\mathfrak{a} \mid \mathfrak{a}^{ec} = \mathfrak{a}\}$, $E = \{\mathfrak{b} \mid \mathfrak{b}^{ce} = \mathfrak{b}\}$, and $\mathfrak{a} \mapsto \mathfrak{a}^e$ is a bijective map of C onto E, whose inverse is $\mathfrak{b} \mapsto \mathfrak{b}^c$.*

Fact. *The contraction of a prime ideal is always prime.*

Proposition. *Let A be a ring and let S be a multiplicative subset. Extension and contraction on the natural homomorphism $A \to S^{-1}A$ induce mutually inverse bijections between the set of prime ideals of $S^{-1}A$ and the set of prime ideals of A that do not meet S.*

Proof. Let $\mathfrak{p}$ be a prime ideal of A not meeting S. Note that every element of $\mathfrak{p}^e$ has the form x/s where $x \in \mathfrak{p}$ and $s \in S$. Suppose $(x/s_1)/(y/s_2) \in \mathfrak{p}^e$, where $x, y \in A$ and $s_1, s_2 \in S$. Thus $(x/s_1)(y/s_2) = (z/s_3)$ for some $z \in \mathfrak{p}$ and $s_3 \in S$. It follows that $s_4xy - s_5z = 0$ for some $s_4, s_5 \in S$. We therefore see that $s_4xy \in \mathfrak{p}$. Since $s_4 \notin \mathfrak{p}$, it follows that $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$, and so $(x/s_1) \in \mathfrak{p}^e$ or $(y/s_2) \in \mathfrak{p}^e$, which implies that $\mathfrak{p}^e$ is prime.

We now claim that $\mathfrak{p} = (\mathfrak{p}^e)^c$. Suppose $x \in (\mathfrak{p}^e)^c$. Thus x is an element of A and $x/1 \in \mathfrak{p}^e$. Thus $x/1 = y/s$ for some $y \in \mathfrak{p}$ and $s \in S$. It follows that $s'x - s''y = 0$ for some $s', s'' \in S$, and so $s'x \in \mathfrak{p}$. Since $s' \notin \mathfrak{p}$, it follows that $x \in \mathfrak{p}$. Thus $(\mathfrak{p}^e)^c \subset \mathfrak{p}$. The reverse inclusion is obvious, and so the claim follows.

Now suppose that $\mathfrak{q}$ is a prime of $S^{-1}A$. Then $\mathfrak{q}^c$ is a prime of A, since the inverse image of a prime ideal under any homomorphism is a prime ideal. We claim that $(\mathfrak{q}^c)^e = \mathfrak{q}$. In fact, this is true for any ideal $\mathfrak{q}$, prime or not. Suppose $x/s \in \mathfrak{q}$ with $x \in A$ and $s \in S$. Then $x/1 = s(x/s)$ belongs to $\mathfrak{q}$, and so $x \in \mathfrak{q}^c$. Thus $x/1 \in (\mathfrak{q}^c)^e$, and $(1/s)(x/1) = x/s$ also belongs to $(\mathfrak{q}^c)^e$. We have thus shown that $\mathfrak{q} \subset (\mathfrak{q}^c)^e$. The reverse inclusion is obvious. ☃

Proposition. *Let $f : A \to B$ be a ring homomorphism and let $\mathfrak{p}$ be a prime ideal of A. Then $\mathfrak{p}$ is the contraction of a prime ideal of B if and only if $(\mathfrak{p}^e)^c = \mathfrak{p}$.*

Proof. If $\mathfrak{p} = \mathfrak{q}^c$, then $\mathfrak{p}^{ec} = \mathfrak{q}^{cec} = \mathfrak{q}^c$.

Conversely, if $\mathfrak{p}^{ec} = \mathfrak{p}$, let S be the image of $A \setminus \mathfrak{p}$ in B. Then $\mathfrak{p}^e$ does not meet S, therefore its extension in $S^{-1}B$ is a proper ideal and hence is contained in a maximal ideal $\mathfrak{m}$ of $S^{-1}B$. If $\mathfrak{q}$ is the contraction of $\mathfrak{m}$ in B, then $\mathfrak{q}$ is prime, $\mathfrak{p}^e \subset \mathfrak{q}$ and $\mathfrak{q} \cap S = \emptyset$. Hence $\mathfrak{q}^c = \mathfrak{p}$.

Definition. A commutative ring is called *local* if it has a unique maximal ideal.

Proposition. *Suppose A is local and $\mathfrak{m}$ is its unique maximal ideal, then $x \in A$ is a unit if and only if $x \notin \mathfrak{m}$.*

Proof. If $x \in \mathfrak{m}$ then for any $y \in A$ we have $xy \in \mathfrak{m}$, so $xy \neq 1$, and x is not a unit. Now suppose that $x \in \mathfrak{m}$. Then the ideal (x) is not contained in $\mathfrak{m}$, and therefore not contained in any maximal ideal, and is therefore the unit ideal. Thus $yx = 1$ for some y, and x is a unit.

Proposition. *Let A be a commutative ring with a prime ideal $\mathfrak{p} \subset A$. $A_{\mathfrak{p}}$ is a local ring.*

Definition. Let A be a commutative ring and $\mathfrak{p} \subset A$ a prime ideal. Then the *residue field at $\mathfrak{p}$* is the field of fraction of the integral domain $A/\mathfrak{p}$.

Remark. The residue field at $\mathfrak{p}$ can also be obtained by $A_{\mathfrak{p}}/\mathfrak{m}$, where $\mathfrak{m}$ is the maximal ideal of $A_{\mathfrak{p}}$.

Remark. This is given by the fact that quotient commutes with localization, which is an immediate consequence of the operation S^{-1} on A-modules being *exact*. Exact sequence and related topics will likely be introduced in class or in discussion when we get to module theory. In the meantime, you can search it up if you are curious.

A: It's not a field.