# WORKSHEET # 7

MATH 435 SPRING 2011

In this worksheet, we'll learn about factoring elements in abstract rings. For this worksheet, we follow Rotman's definition of a ring. In particular, all rings are commutative, associative, and have a multiplicative identity.

**Definition 0.1.** Given two elements $x, y$ in a ring $R$, we say that $x$ *divides* $y$ if there exists an element $r \in R$ such that $rx = y$. In this case we write $x|y$ just like with numbers.

**1.** Show that $x|y$ if and only if $y \in (x)$ (recall that $(x)$ is the *ideal generated by* $x$). This should be very easy.

**Solution:** $x|y$ occurs if and only if $y = rx$ for some $r \in R$. Now $y \in (x)$ means $y = rx$ for some $r \in R$. They mean the same thing!

**Definition 0.2.** Fix $R$ to be an integral domain. We say that a non-zero element $x \in R$ is *irreducible*, if whenever we write $x = ab$ for some $a, b \in R$, then either $a$ or $b$ is a unit.

We say that a non-zero *non-unit* element $x \in R$ is *prime*, if whenever $x|(ab)$ then either $x|a$ or $x|b$.

**2.** Identify the units and prime elements in $\mathbb{Z}$. Fix $k$ to be a field. Identify the units and prime elements in the polynomial ring $k[x]$. However, we will see on the next page that not every irreducible element in a ring is prime! *WARNING* prime factorization does not hold in all rings (it is fine for polynomials and integers though).

**Solution:** The units of $\mathbb{Z}$ are simply $-1$ and 1. The prime elements are just the prime numbers and their additive inverses.

In $k[x]$, the units are just the non-zero elements of $k$ (ie, degree 0 polynomials). The prime elements are exactly those polynomials that cannot be factored. As I gave the definition, the units are technically also prime, but by convention, we assume that units are not prime!

**3.** Show that an element $x \in R$, $R$ is an integral domain, is prime if and only if $(x)$ is a prime ideal, which as we saw was equivalent to $R/(x)$ being an integral domain.

Also show that if $x$ is prime, then $x$ is irreducible.

*Hint:* Suppose that $x = ab$ and $x$ is prime. Now, $x$ divides itself, so $x|(ab)$, use the definition now.

**Solution:** As in the hint, suppose $x = ab$, so that $x|(ab)$. Thus since $x$ is prime, either $x|a$ or $x|b$. If $x|a$, then $a = xr$ for some $r \in R$. Thus $x = ab = (xr)b$. Therefore $1 = rb$ by cancelation (we are in an integral domain) so that $b$ is a unit. Likewise, if $x|b$, then $b = xs$ for some $s \in R$. Thus $x = ab = a(xs)$ and so $1 = as$ again by cancelation (and the fact that integral domains are commutative) and so $a$ is a unit. Therefore, either $a$ or $b$ is a unit, as desired.

**4.** Fix $k$ to be a field and consider the ring

$$R = k[x, y, z]/(x^2 - yz).$$

Show that the element (coset) $x + (x^2 - yz)$ is not prime. Then convince yourself that the element $x + (x^2 - yz)$ is irreducible.
*Hint:* The second part can be tricky to actually prove (thus I say convince yourself). If you get stuck on it for 5 minutes, move on. If it helps though, feel free to assume you have unique factorization, and that every irreducible element is prime in $k[x, y, z]$.

**Solution:** For the non-primality, we check that $x+(x^2-yz)$ divides $\big(y + (x^2 - yz)\big)\big(z + (x^2 - yz)\big)$ but doesn't divide either of the individual entries. The irreducibility is more involved and I won't write down the proof right now, I'm still working on giving a not-too-long proof.

**5.** Suppose that that $R$ is a principal ideal domain. Show that every irreducible element is prime.
*Hint:* Suppose that $x$ is irreducible and $x|(ab)$ but $x \not| a$. Consider the ideal $(x, a)$. Now use the fact that $R$ is a principal ideal domain.

**Solution:** Following the hint, we suppose that $x$ is irreducible, $x|(ab)$ but $x \not| a$. Because $R$ is a principal ideal domain, we have $(x, a) = (g)$ for some $g \in R$. Thus $g|x$ or in other words, $gr = x$ for some $r \in R$. But by the irreducibility of $R$, we have that either $g$ is a unit or $r$ is a unit. If $r$ is a unit, then $(g) = (x)$ and so $a \in (g) = (x)$ which implies that $x|a$. Therefore $g$ is a unit and $(x, a) = R$. In particular $1 = sx + ta$ for some $s, t \in R$. It follows that $b = bsx + bat$. $x$ divides $bsx$ (obviously) and divides $bat$ as well. This completes the proof.

**6.** Prove that the ring $k[[x]]$ is a PID. This is hard(ish).

**Solution:** One first should show that an element in $f \in k[[x]]$ is a unit if and only if it has non-zero constant term. I'll leave this as an exercise still. I claim the ideals of $k[[x]]$ are simply the ideals $(x^n)$ for $n \geq 0$, or $(0)$. This has a remarkable consequence though. For any power series $f = a_n x^n + a_{n+1}x^{n+1} + \dots$, there is a unit $u \in k[[x]]$ such that $uf = x^n$ (again, I'll leave to you to verify).

Now, for each ideal $I \neq 0$, consider the smallest $n$ such that $I$ has a powerseries $f$ whose first term is of degree $n$. I claim that $I = (x^n)$ for that same $n$. Certainly $(x^n) = (f) \subseteq I$. But for every element $g \in I$, whose first term is of degree $m_g$, we have $g \in (x^{m_g})$. By assumption $n \leq m_g$ and so $g \in (x^n)$ as well. Thus $I \subseteq (x^n)$ which completes the proof.