M7210 Lecture 28 Friday October 26, 2012

Commutative Rings III

We assume all rings are commutative and have multiplicative identity (different from 0).

Units and zero-divisors

Definition. Let A be a commutative ring and let $a \in A$.

i) a is called a *unit* if $a \neq 0_A$ and there is $b \in A$ such that $ab = 1_A$.

ii) a is called a *zero-divisor* if $a \neq 0_A$ and there is non-zero $b \in A$ such that $ab = 0_A$. A (commutative) ring with no zero-divisors is called an *integral domain*.

Remark. In the zero ring $Z = \{0\}$, $0_Z = 1_Z$. This is an annoying detail that our definition must take into account, and this is why the stipulation "$a \neq 0_A$" appears in *i*). The zero ring plays a very minor role in commutative algebra, but it is important nonetheless because it is a valid model of the equational theory of rings-with-identity and it is the final object in the category of rings. We exclude this ring in the discussion below (and occasionally include a reminder that we are doing so).

Fact. In any (non-zero commutative) ring R the set of zero-divisors and the set of units are disjoint. *Proof*. Let $u \in R \setminus \{0\}$. If there is $z \in R$ such that $uz = 0$, then for any $t \in R$, $(tu)z = 0$. Thus, there is no $t \in R$ such that $tu = 1$.

Fact. Let R be a ring. The set $U(R)$ of units of R forms a group.

Examples. The units in $\mathbb{Z}$ are 1 and -1. In $\mathbb{Z}[i]$, the units are $1, i, -1, -i$. In a field, all non-zero elements are units. If A is a domain, the units of $A[x]$ are the units of A, because when A is a domain, the degree of the degree of the product of two polynomials is the sum of the degrees of each separately). In $\mathbb{Z}/n\mathbb{Z}$, the units are the residues of the integers that are prime to n. Every other non-zero element of $\mathbb{Z}/n\mathbb{Z}$ is a zero-divisor.

Example. A is *not* a domain, then there may be units in $A[x]$ that are not in A. For example, if $A = \mathbb{Z}/4\mathbb{Z}$, then

$$\left(\overline{1} + \overline{2}\,x\right)^2 = \overline{1} + \overline{4}\,x + \overline{4}\,x^2 = \overline{1},$$

Exercise 1. Show that $\overline{1} + \overline{p}x$ is a unit in $\mathbb{Z}/p^n\mathbb{Z}$. What are the units in $(\mathbb{Z}/4\mathbb{Z})[x]$? What are the units in $(\mathbb{Z}/p^n\mathbb{Z})[x]$?

Definition/Exercise. Let R be a ring. Two elements $s, t \in R$ are said to be *associates* if there is a unit $u \in R$ such that $s = ut$. Show that being associates is an equivalence relation. Show that equivalence classes may be multiplied unambiguously.

Fact. Every field is an integral domain. *Proof*. All non-zero elements of a field are units, so there are no zero-divisors.

Exercise 2. A finite integral domain is a field.

Exercise 3. Suppose D is an integral domain that contains a field F. Suppose further that D is finite-dimensional over F. Can you conclude that D is a field?

Proposition. *Every integral domain is a subring of a field.*

Comment. More important than the fact itself is the way we construct a field from any integral domain. This is described in the proof.

Proof. Let A be an integral domain, and let $S = A \setminus \{0_A\}$ We define a relation $\sim$ on $A \times S$ as follows:

$$(a_1, s_1) \sim (a_2, s_2) :\Leftrightarrow \; a_1 s_2 = a_2 s_1.$$

We will show this is an equivalence relation. It is obviously reflexive and symmetric. In order to prove transitivity, we use the fact that if a product of elements of A is 0, then one of the factors is zero. Suppose $a_1 s_2 = a_2 s_1$ and $a_2 s_3 = a_3 s_2$ Multiplying the first equation by s_3 and the second by s_1, we get $a_1 s_2 s_3 = a_3 s_1 s_2$, so $(a_1 s_3 - a_3 s_1) s_2 = 0$. But by assumption, $s_2 \neq 0$, so $a_1 s_3 = a_3 s_1$. We denote the equivalence class of (a, s) by $\frac{a}{s}$, and the set of all equivalence classes is denoted $S^{-1}A$. We now define addition on $S^{-1}A$ by

$$\frac{a_1}{s_1} + \frac{a_2}{s_2} := \frac{a_1 s_2 + a_2 s_1}{s_1 s_2},$$

and multiplication by

$$\frac{a_1}{s_1} \cdot \frac{a_2}{s_2} := \frac{a_1 a_2}{s_1 s_2}.$$

These operations make $S^{-1}A$ into a ring that contains a copy of A, namely $\{\, \frac{a}{1} \mid a \in A \,\}$. The proof is routine, but requires a lot of checking; see the exercise below. Every non-zero element of $S^{-1}A$ has an inverse, since if $a \neq 0$, then

$$\frac{a}{s} \cdot \frac{s}{a} = \frac{as}{as} = 1_{S^{-1}A}.$$

Thus $S^{-1}A$ is a field that contains A. /////

Exercise 4. Finish the proof.

Exercise 5. The field constructed in the proof is called the fraction field of A. Show that the embedding of A in its fraction field has the following universal property. If $\phi : A \to F$ is any *injective* ring homomorphism and F is a field, then there is a unique extension of ϕ to the fraction field of A.

Ideals and Prime and Maximal Ideals

Warm-up. Suppose A is a ring. Then for all $a \in A$, $a 0_A = 0_A$.

Reminder. Let A be a commutative ring. A subgroup of the additive group of A with the property that

$$\text{for all } a \in A, \text{ and all } y \in I,\ ay \in I \tag{1}$$

is called an *ideal*.[1]

Fact. The kernel of any ring homomorphism is an ideal. If $I \subseteq A$ is an ideal, the set of (additive) cosets of I has a multiplication defined unambiguously by $(a + I)(b + I) = ab + I$, and with this operation A/I is a ring and $a \mapsto a + I$ is a ring homomorphism.

[1] If A is not assumed commutative, this is called a *left ideal.* An ideal must be closed under both "out-in" and "in-out" multiplication, i.e., it must satisfy (1) and also for all $a \in A$, and all $y \in I$, we must have $ya \in I$.