MATH 115, SUMMER 2012
LECTURE 9

JAMES MCIVOR

- decided to spend an extra lecture on algebra since it's so great.

1. Review of Last Time

- rings = number system w/ add, subtract, and multiply, but not always divide (if so, call it a field)
- main examples: $\mathbb{Z}$ vs $\mathbb{Z}/m$.
- **key difference**: in $\mathbb{Z}/m$, some things add or multiply to zero! Ex: 2 times 3 = 0 in $\mathbb{Z}/6$.
- other interesting things to look for in a ring: **units and zerodivisors**.
- EXAMPLES: in $\mathbb{Z}$, units are ± 1 and there are NO zerodivisors. In $\mathbb{Z}/m$, units are a s.t. $(a, m) = 1$ while zero divisors are a s.t. $(a, m > 1$.
- **Homomorphisms** These are the types of functions between rings that are of interest.
- write definition. examples: square map $\mathbb{Z} \to \mathbb{Z}$ cube map $\mathbb{Z} \to \mathbb{Z}$ same for $\mathbb{Z}/2$ and $\mathbb{Z}/3$.

2. Isomorphism

Sometimes, two rings are considered "the same", even though they may look different.

Definition 1. An **isomorphism** from a ring R to a ring S is a homomorphism $\phi\colon R \to S$ which has an inverse, i.e., for which there exists another homomorphism $\psi\colon S \to R$ such that $\phi \circ \psi$ is the identity map on S and $\psi \circ \phi$ is the identity map on R.

Definition 2. An **isomorphism** $R \to S$ is a ring homomorphism which is both one-to-one and onto (or injective and surjective).

Examples:
- Let R be the ring consisting of three elements a, b, c. The addition and multiplication are defined by the following tables: (draw table)
- from the addition table we see that a is the additive identity, while c is the multiplicative identity.

We already know another ring with three elements, namely $\mathbb{Z}/3 = \{0, 1, 2\}$. They are probably "the same".
- to prove they're isomorphic, must write down an isom between them, say $R \to \mathbb{Z}/3$
- must send 1 to 1 (by def) and 0 to 0 (by short proof), so $a \mapsto 0$ and $c \mapsto 1$. To make it one-to-one and onto, must send b to 2. Easy to see that it really is one-to one and onto.

- could also construct an inverse map $\mathbb{Z}/3 \to R$, by sending $0 \mapsto 1$, $1 \mapsto c$ and $2 \mapsto b$.

- (sort of random, but needed later) **define ideals** in an arbitrary ring - same def as ideals in $\mathbb{Z}$.

- usually, not all ideals are principal, as they are in $\mathbb{Z}$. EXAMPLE: the ideal $(2, x) \subset \mathbb{Z}[x]$.

3. Applications

Why introduce this abstract stuff? I think it makes many arguments clearer, and illuminates connections between various different things. Hopefully you'll come to agree (turn to the dark side!).

Any statement about congruences mod m can be interpreted as a statement about the ring $\mathbb{Z}/m$.

- What does the number $\phi(m)$ have to do with the ring $\mathbb{Z}/m$?

- Fermat's Little Thm. Remember that this says that if p is prime and $a \neq 0$, then $a^{p-1} \equiv 1 \mod p$. In other words, for any nonzero element a of $\mathbb{Z}/p$, if we raise it to the $p-1$ power, we get 1. We've seen that for p prime, p is a field, so everything is a unit (except 0). Since a is a unit, i.e., it has an inverse, so we know that a times something will give us 1. The interesting thing is that a times another power of a actually gives us 1.

- Chinese Remainder Theorem for Rings.

This is the most important application of our discussion of rings. Before explaining it, we need to say what is a product of rings. If R and S are rings, their **product** is denoted $R \times S$. It is the set of ordered pairs whose first element lives in R and whose second element lives in S:

$$R \times S = \{(r, s) \,|\, r \in R, s \in S\}$$

So far this is just a set, but we can give it a ring structure by defining multiplication as follows: to add/multiply two ordered pairs, you add/multiply the R-part and the S-part separately:

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2), \quad (r_1, s_1) \cdot (r_2, s_2) = (r_1 \cdot r_2, s_1 \cdot s_2),$$

The additive identity element is $(0, 0)$, and the multiplicative identity element is $(1, 1)$.

Example 3.1. Take $R = \mathbb{Z}/3$ and $S = \mathbb{Z}/4$. We can write out their elements explicitly:

$$\mathbb{Z}/3 = \{0, 1, 2\}, \quad \mathbb{Z}/4 = \{0, 1, 2, 3\}$$

To compute $(0, 2) + (1, 3)$, we get $(1, 1)$, because in the second factor, $2 + 3 = 5 \equiv 1 \mod 4$. Similarly, $(2, 2) \cdot (2, 1) = (1, 2)$, because on the first factor, $2 \cdot 2 = 4 \equiv 1 \mod 3$.

Now, the Chinese Remainder Theorem can be restated as follows:

Theorem 1 (Chinese Remainder Theorem Revisited)**.** *If m and n are coprime, then the rings $\mathbb{Z}/m \times \mathbb{Z}/n$ and $\mathbb{Z}/mn$ are isomorphic.*

Let's see this in our example of $R = \mathbb{Z}/3$, $S = \mathbb{Z}/4$. The theorem says $\mathbb{Z}/3 \times \mathbb{Z}/4 \cong \mathbb{Z}/12$. Let's write out the isomorphism explicitly. The array on the left lists elements of $\mathbb{Z}/3 \times \mathbb{Z}/4$ and the array on the right lists the elements of $\mathbb{Z}/12$ that they map to.

$$\begin{array}{cccc} (0,0) & (0,1) & (0,2) & (0,3) \\ (1,0) & (1,1) & (1,2) & (1,3) \\ (2,0) & (2,1) & (2,2) & (2,3) \end{array} \quad \longmapsto \quad \begin{array}{cccc} 0 & 9 & 6 & 3 \\ 4 & 1 & 10 & 7 \\ 8 & 5 & 2 & 11 \end{array}$$

So, for example, the element $(2,3) \in \mathbb{Z}/3 \times \mathbb{Z}/4$ maps to $5 \in \mathbb{Z}/12$.

-explain how to check that this is a homomorphism, and also an isomorphism.

4. An Application

Theorem 2. *If $f(x) \equiv 0 \mod m_1$ has a_1 solutions (mod m_1) and $f(x) \equiv 0 \mod m_2$ has a_2 solutions (mod m_2), and if a_1, a_2 are relatively prime, then $f(x) \equiv 0 \mod m_1 m_2$ has $a_1 a_2$ solutions mod $m_1 m_2$.*

Proof. Use CRT □