Ex: We saw last time that  

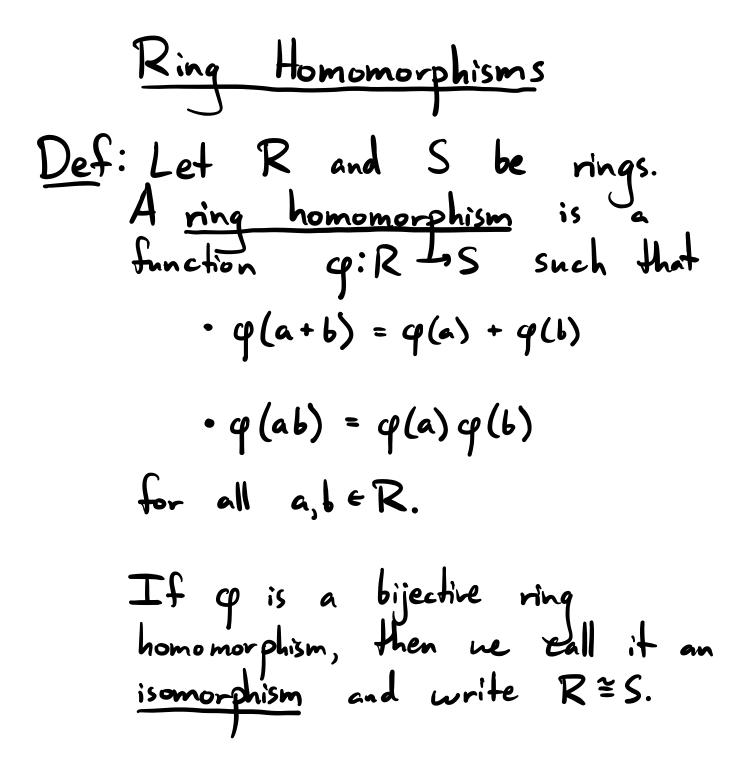
$$Z_n^{\times} = U(n) = \{a \in \mathbb{Z}_n \mid gcd(a, n) = 1\},\$$
  
and that every non-zero element  
of  $Z_n$  which isn't a unit is a  
zero divisor. Thus

Thum: Let R be a finite integral  
domain. Then R is a field.  
  
Proof: We must show 
$$R^{x} = R \setminus \{0\}$$
.  
Certainly,  $R^{x} \in R \setminus \{0\}$ . So take  
 $a \in R \setminus \{0\}$ .  
Define the "multiply by a" map  
 $f: R \rightarrow R$   
 $x \mapsto ax$ .  
  
Since R is an integral domain  
and  $a \neq 0$ , we have  
 $ax_{1} = ax_{2} \implies x_{1} = x_{2}$   
for any  $x_{1}, x_{2} \in R$ . So f is  
injective.

Since R is finite, f is also  
surjective.  
Thus, 
$$I \in R$$
 is in the range of  
f. That is,  
 $I = f(b) = ab$   
for some  $b \in R$ . Thus,  $b = a^{-1}$   
and so  $a \in R^{\times}$  is a unit.

Def: Let 
$$R = (R, +, \cdot)$$
 be a ring.  
A subset  $S \subseteq R$  is a subring if  
 $\cdot S$  is closed under +,  
 $\cdot S$  is closed under  $\cdot$ ,  
 $\cdot (S, +, \cdot)$  is also a ring.

Then S is a subjroup of 
$$(R, +)$$
.  
Then S is a subjroup of  $(R, +)$ .  
 $\cdot (S, +)$  is a subgroup of  $(R, +)$ .  
 $\cdot S$  is closed under  $\cdot$   
Proof: This is just a restatement of  
the definition.  
Ex:  $Z \in Q \subseteq R \subseteq C$   
Ex: For  $n \in \mathbb{N}$ ,  $nZ \subseteq Z$ .  
Ex: For  $n \in \mathbb{N}$ ,  $nZ \subseteq Z$ .  
Ex:  $\{n \times n \text{ upper triangular matrices}\} \subseteq M_{*}(R)$   
Note: No special notation for subrings.  
We just use  $\subseteq$ .



Def: Let 
$$q: R \rightarrow S$$
 be a ring  
homomorphism. The image of  $q$   
is  
 $q(R) = {q(r) | r \in R} \leq S$   
and the kernel of  $q$  is  
ker  $q = {r \in R | q(r) = 0} \in R$ .



Def: Let R be a ring. An ideal  
in R is a subring 
$$I \subseteq R$$
 such  
that for all  $a \in I$ ,  $r \in R$ , we have  
 $ra \in I$  and  $ar \in I$ .

So kernels are ideals!