Notes for 27 Feb (Wednesday)

1 The road so far...

1. Reproved Fermat's and Euler's theorems. Used the ideas to prove related results for squarefree integers.
2. Proved the Frobenius property ("Freshman's dream.")
3. Defined Ring Homomorphisms.

2 Ring homomorphisms

A ring homomorphism satisfies the following properties

1. $T(0) = 0$. Indeed, $T(a) = T(a+0) = T(a) + T(0)$ and hence $T(0) = 0$ (because addition forms a group).
2. The image of T is a subring of S. Indeed, $0, 1$ are in the image and it is closed under addition and multiplication. Moreover, $T(r) + T(-r) = T(0) = 0$ and hence $-T(r) = T(-r)$. So it is closed under additive inverses too. Hence it is a subring.
3. The image of the group of units of R is inside the group of units of S. Indeed, $T(a)T(a^{-1}) = T(1) = 1$. (By the way, just as a subring is defined as a subset such that the addition and multiplication operations make it into a ring, a subgroup of a group is a subset such the multiplication operation makes it into a group. It is easy to see that a subset is a subgroup iff it is closed under multiplication, inverses, and the identity belongs to it.)

Here are examples and non-examples :

1. The identity map is always a homomorphism.
2. If $S \subset R$ is a subring, then the inclusion map is a homomorphism.
3. The map $T(x) = 2x$ is not a ring homomorphism from $\mathbb{Z}$ to itself because $T(1) \neq 1$ (for instance). In fact, if $T : \mathbb{Z} \to \mathbb{Z}$ is any ring homomorphism, then if $n > 0$, $T(n) = T(n.1) = T(1) + T(1) + \ldots = n$. Hence, $T(-n) = -n$ and T is the identity.
4. The Frobenius map is a ring homomorphism.
5. The map $T : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ given by $T(n) = [n]_m$ is a ring homomorphism.

6. There is no ring homomorphism from $\mathbb{Z}/m\mathbb{Z}$ to $\mathbb{Z}$ for $m \geq 2$. Indeed, $0 = T([m]) = T([1] + [1] + \ldots) = mT([1]) = m$ which is a contradiction.

Likewise, before we proceed further with ring homomorphisms, a group homomorphism $T : G \to H$ is a function such that $T(1_G) = 1_H$, $T(a * b) = T(a) * T(b)$. These two properties imply that $T(a^{-1}) * T(a) = T(1) = 1 = T(a) * T(a^{-1})$. Hence $T(a)^{-1} = T(a^{-1})$.

Back to rings : A ring homomorphism is $1-1$ iff $T(r) = 0 \Rightarrow r = 0$. Indeed, one way is obvious. For the other way, $T(a) = T(b) \Rightarrow T(a-b) = 0$ and hence $a = b$. Here is a definition :

If $T : R \to S$ is a ring homomorphism, then the set of all $r \in R$ such that $T(r) = 0$ is called the kernel of T. The kernel is not a subring of R unless $T(1) = 0$. However, $T(a.r) = 0 \ \forall \ r \in ker(T) \ and \ a \in R$. Moreover, $T(r_1 + r_2) = 0$ if $r_1, r_2 \in ker(T)$.

In general, it is not hard to prove that if $T : R \to S$ is a ring homomorphism, and $s \in Im(T)$, then $\{r : T(r) = s\}$ is in 1-1 correspondence with the kernel. Lastly, if R is a field and $1_S \neq 0_S$ then T is 1-1. Indeed, if $r \neq 0$, then $T(r) = 0 \to T(r^{-1})T(r) = 0 \to T(1) = 1 = 0$ which is not possible.

Now we look at all homomorphisms with domain $\mathbb{Z}$.

Theorem 1. *The function $f : \mathbb{Z} \to R$ where R is a given commutative ring, defined by $f(n) = n.1_R := 1_R + (n-1)1_R \ \forall \ n \in \mathbb{Z}$ (defined inductively by adding 1_R to itself n times for positive n) is a homomorphism, and it is the only homomorphism.*

Proof. Indeed, $f(1) = 1_R$ by definition. Note that $f(a+b) = (a+b).1_R = a.1_R + b.1_R$ by associativity of addition and induction. Also, $f(ab) = (ab).1_R$. Now, $a.1_R b.1_R = a.1_R(1_R + 1_R + \ldots) = a.1_R + a.1_R + \ldots = ab.1_R$ by distributivity and associativity respectively. Hence f is a homomorphism.

If f is any homomorphism, $f(1) = 1_R$ by definition and $f(0) = 0_R$ as a property. Also, $f(n) = f(1 + (n-1)) = f(1) + f(n-1)$ for any positive integer n by definition. By induction, $f(n) = n1_R$. Since $f(-n) = -f(n) = -n1_R$ when $n > 0$. Hence it is the only homomorphism. □

So, here are a couple of more examples.

1. $f : \mathbb{Z} \to \mathbb{Q}$ is simply the inclusion homomorphism.

2. $f : \mathbb{Z} \to \mathbb{Z}_m$ given by $f(n) = n[1]_m = [n]_m$ is a homomorphism that is not 1-1. Indeed, the kernel is $f(n) = [0]_m$ iff $n = mk$. It is onto though.

The last example motivates the following definition : Let $f : \mathbb{Z} \to R$ be the only homomorphism (R is a commutative ring). If f is 1-1, it is said to have characteristic 0. If not, the smallest natural number > 0 in $ker(f)$ is called the characteristic of the ring R.