Notes for 28 Feb (Thursday)

1 The road so far...

1. Properties of ring homomorphisms.
2. Classified all the ring homomorphisms from $\mathbb{Z}$ to a commutative ring.
3. Defined the characteristic of a commutative ring.

Lemma 1.1. *If $f : \mathbb{Z} \to R$ is a homomorphism and m is the characteristic, then $ker(f) = \{0, m, -m, 2m, -2m, \ldots\}$.*

Proof. If $n \in ker(f)$, i.e., $f(n) = 0_R$, then $n = mq + r$ where $0 \leq r < m$. Thus, $f(n) = f(m)f(q) + f(r) = 0_R + r.1_R = 0_R$ which means that unless $r = 0$ we have a contradiction. □

Denote by $m\mathbb{Z}$ the set of multiplies of m.

Lemma 1.2. *Let R be a commutative ring with no zero divisors and $0 \neq 1$. Then if the characteristic is not 0, it is a prime.*

Proof. If the characteristic is m, then $m.1_R = 0_R$. If m is not a prime, then $m = pq$ for some prime p. Then $pq.1_R = (p.1_R)(q.1_R) = 0_R$. Since there are no zero divisors, $p.1_R = 0$ or $q.1_R = 0$. We have a contradiction because m is the smallest such integer. □

Every field therefore has either characteristic 0 or p where p is a prime. Every finite field obviously has characteristic p. Here are examples of finite fields (it is easy to see that the polynomial ring over $\mathbb{Z}_p$ is an example of ring with positive characteristic).

1. $\mathbb{Z}_p$ where p is a prime has characteristic p.
2. Let $\mathbb{F}_4 = \{0, 1, \omega, b\}$ defined by $0.x = x.0 = 0$, $0 + x = x + 0 = x$, $1.x = x.1 = x$, $1 + 1 = 0$, $1 + \omega = \omega + 1 = b$, $1 + b = b + 1 = \omega$, $\omega + b = b + \omega = 1$, $\omega.b = b.\omega = 1$, $\omega.\omega = b$, $b.b = \omega$. Clearly, this defines a finite field. Its characteristic is clearly 2.

Def : A ring homomorphism is said to be an isomorphism if it is a bijection. Two rings are said to be isomorphic if there is an isomorphism between them.
Firstly, the inverse of a ring isomorphism is a ring homomorphism. (HW) It is easy to see that if the characteristic of a commutative ring is 0, then $f : \mathbb{Z} \to R$ defined by $f(n) = n.1_R$ is an isomorphism to its image.

Theorem 1. *Let R be a commutative ring and $f : \mathbb{Z} \to R$ be a homomorphism. If f is not injective, and $m\mathbb{Z} \subset ker(f)$ then f induces a homomorphism from $\mathbb{Z}_m$ onto its image defined by $g([a]_m) = f(a) = a.1_R$. If $ker(f) = m\mathbb{Z}$, then the induced homomorphism is an isomorphism onto its image.*

As consequences,

1. Let R be a commutative ring with no zero divisors. If R has characteristic 0, it has a subring isomorphic to $\mathbb{Z}$. If it has characteristic p, then it has a subring isomorphic to $\mathbb{Z}_p$.
2. If d divides m, then $f : \mathbb{Z} \to \mathbb{Z}_d$ induces a homomorphism from $\mathbb{Z}/m\mathbb{Z}$ to $\mathbb{Z}_d$. Also, a homomorphism between the groups of units.

Now we prove the above theorem.

Proof. We need to prove that g is well-defined. Indeed, if $[a] = [a']$, i.e. $a = a' + km$ then $f(a) = f(a') + f(km) = f(a') + 0$ because $km \in ker(f)$. This map is a homomorphism because $g([1]) = f(1) = 1$, $g([a]+[b]) = g([a+b]) = f(a+b) = f(a)+f(b) = g([a])+g([b])$. Likewise, for multiplication. The kernel of this homomorphism is $[a]$ such that $g([a]) = 0$, i.e., $a \in ker(f)$. If $ker(f) = m\mathbb{Z}$, then $[a] = [0]$ and hence g is an isomorphism. □

The following theorem defines the Frobenius endomorphism in general.

Theorem 2. *If R is a commutative ring with prime characteristic p and a, b are elements of R then $(a+b)^p = a^p+b^p$, i.e., $f_p(a) = a^p$ is a homomorphism (a homomorphism between the same objects is called an endomorphism).*

Proof. Note that the Binomial theorem $(a+b)^n = \sum_{r=0}^{n} \binom{n}{r} a^r b^{n-r}$ is true for commutative rings by induction. Hence, $(a+b)^p = a^p + b^p + \sum_{r=1}^{p-1} \binom{p}{r} a^r b^{p-r} = a^p + b^p$ because p divides $\binom{p}{r}$ when $1 \leq r \leq p-1$. □

It is clear from the above that if $\mathbb{F}$ is a finite field of characteristic p (indeed, $1-1$ implies onto because $\mathbb{F}$ is finite) then the Frobenius endomorphism is an isomorphism. (An isomorphism between the same objects is called an Automorphism.) Moreover,

Lemma 1.3. *If R is a ring of characteristic p, then $\forall\ a, b \in R$ and every $n > 0$, $(a+b)^{p^n} = a^{p^n} + b^{p^n}$.*

Proof. The composition of any number of homomorphisms is a homomorphism (easy to prove). Therefore, $(a+b)^{p^n} = f_{p^n}(a) + f_{p^n}(b) = a^{p^n} + b^{p^n}$. □