AM 106: Applied Algebra	**Salil Vadhan**

Lecture Notes 19

November 13, 2018

1 Homomorphisms

- Reading: Gallian Ch. 15.
- **Def:** A mapping $\varphi : R \to S$ between two rings is a *ring homomorphism* iff $\varphi(a+b) = \varphi(a) + \varphi(b)$ and $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in R$. If φ is a bijection (one-to-one and onto), we call φ a *ring isomorphism* and write $R \cong S$.
- **Ring Analogues of Familiar Facts about Homomorphisms:**
  - The *image* $\mathrm{Im}(\varphi) \stackrel{\text{def}}{=} \varphi(R) = \{\varphi(r) : r \in R\}$ is a subring of S.
  - The *kernel* $\mathrm{Ker}(\varphi) \stackrel{\text{def}}{=} = \{r \in R : \varphi(r) = 0\}$ is an ideal of R.
  - $R/\mathrm{Ker}(\varphi) \cong \mathrm{Im}(\varphi)$.
  - φ is one-to-one (and thus establishes an isomorphism between R and $\mathrm{Im}(\varphi)$) iff $\mathrm{Ker}(\varphi) = \{0\}$.
- **Examples and non-examples:**
  - $\varphi : \mathbb{Z} \to \mathbb{Z}_n$, $\varphi(x) = x \bmod n$.
  - $\varphi : \mathbb{Z} \to \mathbb{Z}_m \times \mathbb{Z}_n$, $\varphi(x) = (x \bmod m, x \bmod n)$.
  - $\varphi : R \to R/I$, $\varphi(a) = a + I$.
  - $\varphi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}[i]$, $\varphi(a,b) = a + bi$.
  - $\varphi : M_n(\mathbb{R}) \to \mathbb{R}$, $\varphi(M) = \det M$.

- $\varphi : \mathbb{R}[x] \to \mathbb{R}$, $\varphi(p) = p(11)$.

- $\varphi : \mathbb{R}[x] \to \mathbb{C}$, $\varphi(p) = p(i)$.

-

- $\varphi_1 \circ \varphi_2$, where φ_1, φ_2 ring homomorphisms.

- $\varphi : \mathbb{Z}[x] \to \mathbb{Z}_{17}$, where $\varphi(p) = p(0) \bmod 17$.

- $\varphi : \mathbb{Z} \to R$, $\varphi(n) = 1 + 1 + \cdots + 1$ (n times).

- **Corollary of Last Example:** A ring of characteristic 0 contains a subring isomorphic to $\mathbb{Z}$. A ring of finite characteristic n contains a subring isomorphic to $\mathbb{Z}_n$.