Cyclic Codes

Kyle Cook & Jacob Hauck

November 7, 2019

1 Review of Ideals

Definition 1.1. *Let R be a ring with operations $+$ and $\cdot$. An ideal I of R is a subset of R satisfying the following properties:*

1. *I is a subgroup of R under $+$*
2. *for any $r \in R$ and any $i \in I$, $ri \in I$*

Definition 1.2. *Let R be a ring and I a two sided ideal of R. We can define an equivalence relation $\sim$ on R as follows:*

$$a \sim b \iff a - b \in I$$

The equivalence class of the element a in R is given by

$$[a] = a + I := \{a + r | r \in I\}$$

The set of all equivalence classes is denoted R/I; it becomes a ring, the factor ring, or quotient ring of R modulo I, if one defines

$$(a + I) + (b + I) = (a + b) + I$$
$$(a + I)(b + I) = (ab) + I$$

In practice one must check these definitions are well defined.

Definition 1.3. *Let $a \in R$. The set $\langle a \rangle = \{ra | r \in R\}$ is an ideal of R generated by a. Ideals with such a generator element are called Principal Ideals.*

Definition 1.4. *An integral domain is a nonzero commutative ring in which the product of any two nonzero elements is nonzero.*

Theorem 1.5. *In an integral domain, every nonzero element a has the cancellation property, that is, if $a \neq 0$, then $ab = ac \implies b = c$*

Definition 1.6. *A principal ideal domain is an integral domain in which every ideal is a principal ideal.*

Definition 1.7. *I is a maximal ideal of a ring R if there are no other ideals contained between I and R.*

Theorem 1.8. *Given a ring R and a proper ideal I of R, that is $I \neq R$, I is a maximal ideal of R if any of the following equivalent conditions hold:*

1. *There exists no other proper ideal J or R so that $I \subset J$.*
2. *For any ideal J with $I \subseteq J$, either $J = I$ or $J = R$.*
3. *The quotient ring R/I has no nontrivial ideals.*

Definition 1.9. *Given a field $\mathbb{F}$ we define the ring of polynomials in x over $\mathbb{F}$, $\mathbb{F}[x]$, as the set of all polynomials $p = p_0 + p_1x + p_2x^2 + \cdots p_kx^k$ where p_i are coefficients in $\mathbb{F}$*