EE 605: Error Correcting Codes

Instructor: Saravanan Vijayakumaran

Indian Institute of Technology Bombay

Autumn 2010

Solutions to Assignment 2 — Prepared by Sravan Kumar Jatavath

1. Given, H is a subset of G such that it is non-empty, finite and closed under group operation $\star$.

   Since H is closed under group operation $\star$, $\star$ is a valid binary operation over set H.

   Associative property follows from the fact that G is a group.

   Now, subset H is non-empty.

   Hence $\exists$ at least one element in H, call it 'a'.

   Now, consider a set B, B=$\{a, a \star a, a \star a \star a, \dots\}$

   Because H is closed under $\star$, $a \star a \in H, a \star a \star a \in H$ and so on.

   We see that $B \subseteq H \Rightarrow |B| \leq |H|$

   Since, H is finite, the cardinality of B is finite.

   That means, $a, a\star a, a\star a\star a, \dots$ cannot all be distinct. So there exist positive integers i and j such that

$$\begin{aligned} \underbrace{a \star a \star \dots \star a}_{i \text{ times}} &= \underbrace{a \star a \star \dots \star a}_{j \text{ times}} \\ \Rightarrow \underbrace{a \star a \star \dots \star a}_{(i-j) \text{ times}} &= e \end{aligned}$$

   where e is the identity of the group G. The second equality is obtained by multiplying both sides by $\underbrace{a^{-1} \star a^{-1} \star \cdots \star a^{-1}}_{j \text{ times}}$

   However, $\underbrace{a \star a \star \dots \star a}_{k \text{ times}} \in H$ where $k = i - j > 0$ because H is closed under $\star$.

   This implies that $e \in H$. Since e is the identity of the group G, $a \star e = e \star a = a$ for all $a \in H$.

   Now, only thing left to prove is the existence of inverse. Consider any element a in subset H. We need to prove that there exists $b \in H$ such that $a \star b = b \star a = e$

   If $a = e$, then a is the inverse of itself. Otherwise, by the argument presented earlier, there exists a positive integer k such that $\underbrace{a \star a \star \dots \star a}_{k \text{ times}} = e$. Let $b = \underbrace{a \star a \star \dots \star a}_{k-1 \text{ times}}$.
   Then $a \star b = b \star a = e$. Since $b \in H$, the inverse of every element $a \in H$ exists.

   Hence, H is a subgroup of G.

2. Consider the set of integers $\mathbb{Z}$={...,-2,-1,0,1,2,...} under the operation real addition. It is easy to show that $\mathbb{Z}$ is a group, since addition is associative, closed over integers, 0 is the identity and for a, $-a$ is the inverse.

   Let $\mathbb{Z}^+ = \{1, 2, 3, ...\}$. $\mathbb{Z}^+$ is non-empty, infinite and closed under addition. However, $\mathbb{Z}^+$ is not a subgroup of $\mathbb{Z}$ since there is no identity element.

3. Let H and K be subgroups of a group G.

   One direction: Given H is a subgroup of K or K is a subgroup of H, we want to prove that $H \cup K$ is a subgroup of G.

   $H \cup K = H$ if K subgroup of H or $H \cup K = K$ if H subgroup of K. Since H and K are subgroups of G, $H \cup K$ is a subgroup of G.

   Other direction: Given $H, K, H \cup K$ are subgroups of G, we want to prove that H is a subgroup of K or K is a subgroup of H.

   If H is a subgroup of K, we have nothing to prove. Suppose H is not a subgroup of K. Since H is a subgroup of G, this is possible only if H is not a subset of K. So there exists an element $a \in H$ such that $a \notin K$. Now for any $b \in K$, $a \star b \in H \cup K$. Now $a \star b$ cannot be in K because if it does belong to K then $a \star b \star b^{-1} = a$ belongs to K, which is a contradiction. So $a \star b \in H$ for all $b \in K$. This implies that $a^{-1} \star a \star b = b$ belongs to H. Thus every element of K belongs to H and K is a subgroup of H.

4. Given H and K are subgroups of G. Consider $H \cap K$. We will use a theorem proved in class that subset H is subgroup of G if $H \neq \phi$ and $x, y \in H \Rightarrow xy^{-1} \in H$.

   $H \cap K \neq \phi$ because the identity is in both subgroups.

   Also, for any $x, y \in H \cap K, x, y \in H$ and $x, y \in K$

   $\Rightarrow xy^{-1} \in H$ and $xy^{-1} \in K$

   $\Rightarrow xy^{-1} \in H \cap K$

   Hence, $H \cap K$ is also a subgroup.

5. H is a subgroup of G,

   $\Rightarrow O(H) \mid O(G)$

   $\Rightarrow O(H) \mid n$

   $(n - 1)$ does not divide n for $n > 2$.

   $\Rightarrow O(H) \neq n - 1$

   Hence, G cannot have subgroup H such that $|H| = n - 1$.

6. $\mathbb{Z}_n = \{0, 1, 2, ..., n - 1\}$ with operation addition modulo n.

   Let P be the subgroup of $\mathbb{Z}_n$. $P \neq \phi$, since it is a group. If $P = \{0\}$, the P is cyclic. Suppose $P \neq \{0\}$. By the well-ordering property of the integers, there exists a smallest non-zero element in this subgroup P. Let it be s. We claim that P is cyclic with generator s, i.e. every element of P is a multiple of s modulo n. Suppose this is not true. Then there exists an integer $m \in P$ such that m is not divisible by s. Then we can write $m = qs + r$ where $0 < r < s$ and q is a positive integer representing the quotient. Since $s \in P$, $qs \bmod n = \underbrace{s + \cdots + s}_{q \text{ times}} \mathrm{mod} n \in P$. Since m and $qs \bmod n$ belong to P, $r = m - qs \bmod n \in P$ where $-qs$ is the additive inverse of $qs \bmod n$ in P. This is a contradiction since $0 < r < s$ and s was chosen to be the smallest non-zero element of P.

Thus, every subgroup of $\mathbb{Z}_n$ is cyclic.

7. $\phi : G \to H$ is an isomorphism between G and H.

   $\Rightarrow \phi(x *_g y) = \phi(x) *_H \phi(y), \quad x, y \in G$

   $\Rightarrow \phi(x *_g O_g) = \phi(x) *_H \phi(O_g)$

   $\Rightarrow \phi(x) = \phi(x) *_H \phi(O_g)$

   $\Phi : G \to H \Rightarrow$ Let $\phi(x) = h \in H$

   $h = h *_H \phi(O_g)$

   Similarly, $h = \phi(O_g) *_H h$ (similar to above)

   $\Rightarrow O_H = \phi(O_g)$

8. All finite cyclic groups are isomorphic to $\mathbb{Z}_n$.

   Proof: Let G be a finite cyclic group. We need a one-to-one and onto function $h : G \to Z_n$ such that $h(x \oplus y) = h(x) * h(y), \forall x, y \in G$.

   Let g be the generator element of G and $i \cdot g$ denote $\underbrace{g \oplus g \oplus ... \oplus g}_{\text{i times}}$ for every integer $i > 0$. Since G is cyclic, every element in G can be written as $i \cdot g$ for some positive integer i. Since G is finite there exists a smallest positive integer n such that $n \cdot g = 0$.

   Define $h : G \to \mathbb{Z}_n$ as $h(i \cdot g) = i$. It can be shown that h is one-to-one and onto.

   For any $x, y \in G$, $x = i \cdot g$ and $y = j \cdot g$ for some positive integers i and j less than n. Also $x \oplus y = i \cdot g + j \cdot g = (i + j \bmod n) \cdot g$. This proves that $h(x \oplus y) = h(x) * h(y)$ since both sides are equal to $(i + j) \bmod n$.

9. All finite cyclic groups are isomorphic to $\mathbb{Z}_n$ and $\mathbb{Z}_n$ is abelian. So all finite cyclic groups have to be abelian. Suppose this is not true. Then there exists a finite cyclic group G with elements x and y such that $x \star y \neq y \star x$. Since G is isomorphic to $\mathbb{Z}_n$, there is a one-to-one and onto function $h : G \to \mathbb{Z}_n$ such that $h(x \star y) = h(x) \star h(y)$. Since $\mathbb{Z}_n$ is abelian, $h(x) \star h(y) = h(y) \star h(x)$. This implies $h(x \star y) = h(y \star x)$. Since h is one-to-one $x \star y = y \star x$. This contradicts our assumption that G is not abelian.

10. $x \in G$, $m, n \in \mathbb{Z}$. To prove that if $x^n = 1$ and $x^m = 1$, then $x^d = 1$ where $d = \gcd(m, n)$. Using Bezout's theorem, $d = \gcd(m, n)$= am + bn for some integers $a, b \in \mathbb{Z}$. Then

$$x^d = x^{am+bn} = (x^m)^a (x^n)^b = 1$$

    Let n be the order of x. This means $x^n = 1$ and $x^i \neq 1$for $i = 1, 2, ..., n - 1$. Given that $x^m = 1$, $x^{\gcd(m,n)} = 1$. Then $\gcd(m, n) \geq n$ since n is the smallest positive integer such that $x^n = 1$. However,$d = \gcd(m, n) \leq n$, since a divisor of a positive integer is less than or equal to it. Thus $\gcd(m, n) = n$ and n divides m.