查阅资料，思考并回答下述问题：  
IT-EX07-线性码  
1. 解释群、 阿贝尔群、 环、 交换环、 含幺环、 除环、 域。

答：

**群**：群表示一个拥有满足[封闭性](http://baike.baidu.com/view/585152.htm" \t "http://baike.baidu.com/_blank)、[结合律](http://baike.baidu.com/view/120414.htm" \t "http://baike.baidu.com/_blank)、有[单位元](http://baike.baidu.com/view/689605.htm" \t "http://baike.baidu.com/_blank)、有[逆元](http://baike.baidu.com/view/699065.htm" \t "http://baike.baidu.com/_blank)的[二元运算](http://baike.baidu.com/view/1454408.htm" \t "http://baike.baidu.com/_blank)的[代数结构](http://baike.baidu.com/view/550738.htm" \t "http://baike.baidu.com/_blank)；

**阿贝尔群**（Abelian Group），又称交换[群](http://baike.baidu.com/view/48541.htm" \t "http://baike.baidu.com/view/_blank)或加群，是这样一类群：它由自身的集合G和[二元运算](http://baike.baidu.com/subview/1454408/1454408.htm" \t "http://baike.baidu.com/view/_blank) \* 构成。它除了满足一般的群公理，即运算的封闭性、[结合律](http://baike.baidu.com/subview/120414/120414.htm" \t "http://baike.baidu.com/view/_blank)、G 有[单位元](http://baike.baidu.com/subview/689605/689605.htm" \t "http://baike.baidu.com/view/_blank)、所有G的元素都有逆元之外，还满足[交换律](http://baike.baidu.com/subview/120407/120407.htm" \t "http://baike.baidu.com/view/_blank)；

**环**：一个集合R叫做一个环，假如

① R是一个加群，即R对于一个叫做加法的代数运算来说作成一个交换群； ② R对于另一个叫做乘法的代数运算来说是闭的；

③这个乘法适合结合律；

④两个分配率成立；

**交换环**：一个环R叫做交换环，假如ab=ba，不管a,b是R的哪两个元;

**含幺环**：环R中乘法存在单位元，则称R为含幺环；

**除环**：一个环R叫做一个除环，假如

①R至少包含一个不等于零的元；

②R有一个单位元；

③R的每一个不等于零的元有一个逆元；

**域**：一个交换除环叫做一个域；

2. 给出最小规模的域实例。

答：设一个域中只有0,1元素，代数运算定于如下

|  |  |  |
| --- | --- | --- |
| × | 0 | 1 |
| 0 | 0 | 0 |
| 1 | 0 | 1 |

3. 解释线性空间。

答：设F是一个域。一个F上的向量空间是一个集合V和两个运算：

向量加法: V + V → V, 记作 v + w, ∃ v, w∈V

标量乘法: F × V → V, 记作 a·v, ∃a∈F, v∈V

符合下列公理 (∀ a, b ∈ F 及 u, v, w ∈ V)：

向量加法结合律：u + (v + w) = (u + v) + w；

向量加法交换律：v + w = w + v；

向量加法的单位元：V 里有一个叫做零向量的 0，∀ v ∈ V , v + 0 = v；

向量加法的逆元素：∀v∈V, ∃w∈V，使得 v + w = 0；

标量乘法分配于向量加法上：a(v + w) = a v + a w；

标量乘法分配于域加法上: (a + b)v = a v + b v；

标量乘法一致于标量的域乘法: a(b v) = (ab)v；

标量乘法有单位元: 1 v = v, 这里 1 是指域 F 的乘法单位元。

4. 解释线性码、 生成矩阵、 校验矩阵。

答：

①线性码是指，其中，H是有限域上的行满秩矩阵；

②生成矩阵：由矩阵G和原始信息符号分组，生成有待发送的符号分组，则称G为码的生成矩阵。

③校验矩阵：一个矩阵是校验矩阵，若其满足:其n列对应n个符号；不能出现全0的列；有n-k行，对应n-k个独立方程式、对应n-k个校验符号；其秩为n-k。

5. 如何利用生成矩阵编码?

答：有一个长度为k比特的串b，产生一个码字w，其长度为n 比特，G为生成矩阵，w=bG,w的首个k bits是信息比特，剩余的比特是校验比特。

6. 如何利用校验矩阵译码?

答：首先生成校验矩阵，它是陪集的串列，然后给出最小重量的矢量和它的校验子，当接收到的串不是码字时，计算它的校验子，从对应的陪集中将最小重量的矢量加到损坏的串中从而恢复未损坏的码字。

7. 对于线性码而言，证明码的最小 Hamming 距离等于非零码字的最小 Hamming 重量。

证明：根据线性分组码的封闭性可知，任意两个码字的和仍为码中的码字。根据码字之间的距离的定义，两个码字和的非零符号的个数即为它们之间的距离，而两个码字和的非零符号的个数又是新码字的重量。所以，线性分组码的最小距离必为它的非零码字的最小重量。

8. 编码的数学本质在于:设计消息空间和码空间之间的算子，使得低维空间变成高维空间的子空间，并要求扩距:象空间的最小距离大于原象空间的距离。 请以实例予以解释。

答：如





码字组成的矩阵为，这就从低维空间变成了高维空间，象空间的最小距离大于原象空间的距离。

9. 简述线性码的非零码字最小重量与码的检错能力之间的关系。

答：最小距离：线性分组码的最小距离就是其非零码字的最小重量。

检错能力：为检测e个错码，要求最小码距 d0 ≥ e + 1;

10.简述线性码的非零码字最小重量与码的纠错能力之间的关系。

答：

最小距离：线性分组码的最小距离就是其非零码字的最小重量。

纠错能力：为纠正t个错码，要求最小码距 d0 ≥ 2t+ 1;

为纠正t个错码，同时检测e个错码，则要求最小码距d0 ≥ e + t+1；

（答案提交方式：电子稿，电子邮箱infosecynu2015@163.com)