哈爾濱工業大學 HARBIN INSTITUTE OF TECHNOLOGY

信息安全数学基础

举例

手写板

讲课视频

例

设$(Z,+,0)$中Z为整数集，$+$为整数的加法，0为整数零，易验证

- $(Z,+,0)$中有$(a+b)+c=a+(b+c)$，故G1成立；
- 又有$a+0=0+a=a$，故G2成立；
- 最后有$a+(-a)=(-a)+a=0$，这里$(-a)$表示与a对应的负整数，因而G3成立；
- 再$a+b=b+a$，故G4成立。

从而$(Z,+,0)$为交换群。

哈爾濱工業大學 HARBIN INSTITUTE OF TECHNOLOGY

信息安全数学基础

手写板

讲课视频

举例

例

设$(Z,+,0)$中Z为整数集，$+$为整数的加法，0为整数零，易验证

- $(Z,+,0)$中有$(a+b)+c=a+(b+c)$，故G1成立；
- 又有$a+0=0+a=a$，故G2成立；
- 最后有$a+(-a)=(-a)+a=0$，这里$(-a)$表示与a对应的负整数，因而G3成立；
- 再$a+b=b+a$，故G4成立。

从而$(Z,+,0)$为交换群。

哈爾濱工業大學 HARBIN INSTITUTE OF TECHNOLOGY

信息安全数学基础

手写板

讲课视频

举例

例

设$(Z,+,0)$中Z为整数集，$+$为整数的加法，0为整数零，易验证

- $(Z,+,0)$中有$(a+b)+c=a+(b+c)$，故$G1$成立；
- 又有$a+0=0+a=a$，故$G2$成立；
- 最后有$a+(-a)=(-a)+a=0$，这里$(-a)$表示与a对应的负整数，因而$G3$成立；
- 再$a+b=b+a$，故$G4$成立。

从而$(Z,+,0)$为交换群。

哈爾濱工業大學 HARBIN INSTITUTE OF TECHNOLOGY

信息安全数学基础

举例

手写板

讲课视频

例

设$(Z,+,0)$中Z为整数集，$+$为整数的加法，0为整数零，易验证

- $(Z,+,0)$中有$(a+b)+c=a+(b+c)$，故$G1$成立；
- 又有$a+0=0+a=a$，故$G2$成立；
- 最后有$a+(-a)=(-a)+a=0$，这里$(-a)$表示与a对应的负整数，因而$G3$成立；
- 再$a+b=b+a$，故$G4$成立。

从而$(Z,+,0)$为交换群。

哈爾濱工業大學 HARBIN INSTITUTE OF TECHNOLOGY

信息安全数学基础

手写板

讲课视频

举例

例

设$(Z,+,0)$中Z为整数集，$+$为整数的加法，0为整数零，易验证

- $(Z,+,0)$中有$(a+b)+c=a+(b+c)$，故G1成立；
- 又有$a+0=0+a=a$，故G2成立；
- 最后有$a+(-a)=(-a)+a=0$，这里$(-a)$表示与a对应的负整数，因而G3成立；
- 再$a+b=b+a$，故G4成立。

从而$(Z,+,0)$为交换群。

哈尔滨工业大学 HARBIN INSTITUTE OF TECHNOLOGY

信息安全数学基础

手写板

讲课视频

举例

例

设$(Q^*,\cdot,1)$中Q^*为零以外的所有有理数的集合，$\cdot$为有理数乘法，1为整数1，则$(Q^*,\cdot,1)$满足$G1,G2,G3$和$G4$。故$(Q^*,\cdot,1)$为交换群。

例

设$GL_n(R)$为n阶实数可逆方阵的集合，$\cdot$为两矩阵的乘法，I为单位阵，则$(GL_n(R),\cdot,I)$为群。$GL_n(R)$称为实数域R上n阶一般线性群。

哈爾濱工業大學 HARBIN INSTITUTE OF TECHNOLOGY

信息安全数学基础

举例

手写板

讲课视频

例

设$(Q^*,\cdot,1)$中Q^*为零以外的所有有理数的集合，$\cdot$为有理数乘法，1为整数1，则$(Q^*,\cdot,1)$满足$G1,G2,G3$和$G4$。故$(Q^*,\cdot,1)$为交换群。

例

设$GL_n(R)$为n阶实数可逆方阵的集合，$\cdot$为两矩阵的乘法，I为单位阵，则$(GL_n(R),\cdot,I)$为群。$GL_n(R)$称为实数域R上n阶一般线性群。

哈爾濱工業大學 HARBIN INSTITUTE OF TECHNOLOGY

信息安全数学基础

手写板

讲课视频

举例

例 (希尔密码)

在希尔密码(Hill Cipher)中加密变换为

$$(y_1y_2\cdots y_m) = (x_1x_2\cdots x_m)M \bmod 26 \tag{1.1}$$

这里密钥$M \in GL_m(Z_{26}), x_i, y_i \in Z_{26}, Z_{26} = \{0, 1, \cdots, 25\}$，$x_i$*为明文，*$y_i$*为密文。（式1.1右边的行向量*$(x_1, x_2, \cdots, x_m)$*与矩阵*$M$*乘是先进行通常的实数行向量与实数矩阵乘再对所得行向量的每一分量取模26）*

加密过程

字母$AB\cdots Z$分别对应$0, 1, \cdots, 25$，加密前先将明文字母串变换为Z_{26}上的数字串，然后再按上述表达式每次m个数字的将明文数字串变换为密文数字串，最后将密文数字串变换为密文字母串。

哈爾濱工業大學 HARBIN INSTITUTE OF TECHNOLOGY

信息安全数学基础

手写板

讲课视频

举例

例 (希尔密码)

在希尔密码(Hill Cipher)中加密变换为

$$(y_1y_2\cdots y_m)=(x_1x_2\cdots x_m)M mod\,26 \tag{1.1}$$

这里密钥$M\in GL_m(Z_{26}), x_i, y_i\in Z_{26}, Z_{26}=\{0,1,\cdots,25\}$，$x_i$*为明文，*$y_i$*为密文。（式1.1右边的行向量*$(x_1,x_2,\cdots,x_m)$*与矩阵*$M$*乘是先进行通常的实数行向量与实数矩阵乘再对所得行向量的每一分量取模26）*

加密过程

字母$AB\cdots Z$分别对应$0,1,\cdots,25$，加密前先将明文字母串变换为Z_{26}上的数字串，然后再按上述表达式每次m个数字的将明文数字串变换为密文数字串，最后将密文数字串变换为密文字母串。

哈爾濱工業大學 HARBIN INSTITUTE OF TECHNOLOGY

信息安全数学基础

手写板

讲课视频

补充：

定理

设$\mathbf{A}=(a_{ij})$为一个定义在$\mathbf{Z}_{26}$上的$n\times n$矩阵，若$\mathbf{A}$在$mod\,26$上可逆，则有：

$$\mathbf{A}^{-1}=(det\mathbf{A})^{-1}\mathbf{A}^{*}(mod\,26)$$

这里，$\mathbf{A}^{*}$是$\mathbf{A}$的伴随矩阵。