P412

1、①、Z（2^-1）对+构成一个阿贝尔群：先证明其成群：

1、封闭性：Z 是整数的集合，整数的加法运算仍为整数，所以满足封闭性。

2、单位元，存在 m=0，n=0，使得(0+0*2^1/2)+(m+n*2^1/2)=(m+n*2^1/2)+(0+0*2^1/2)=m+n*2^1/2。

3、逆元：对于任何 m，n,都存在-m,-n 使得(m+n*2^1/2)+（-m-n*2^1/2)=（-m-n*2^1/2)+（m+n*2^1/2)=0+0*2^1/2

4、结合律：(m1+n1*2^1/2)+（(m2+n2*2^1/2)+（m3+n3*2^1/2))=(（m1+n1*2^1/2)+(m2+n2*2^1/2))+(（m3+n3*2^1/2))=(m1+m2+m3)+(n1+n2+n3)*2^1/2

再整明交换律也成立：（m1+n1*2^1/2）+（m2+n2*2^1/2)=（m2+n2*2^1/2)+(m1+n1*2^1/2)=(m1+m2)+(n1+n2)*2^1/2。

所以，Z(2^1/2)对+构成一个阿贝尔群。

②、再证明 Z(2^1/2) 对 * 构成半群：（m1+n1*2^1/2）*(m2+n2*2^1/2)=(m2+n2*2^1/2)*(m1+n1*2^1/2)=m1*m2+2*n1*n2+(m1*n2+m2*n1)*2^1/2。

③、证明其满足左右分配律：(m1+n1*2^1/2) *((m2+n2*2^1/2) + (m3+n3*2^1/2))=（m1+n1*2^1/2）*（m2+n2*2^1/2）+（m1+n1*2^1/2）+（m3+n3*2^1/2）=m1m2+m1m3+2n1n2+2n1n3+m1n2*2^1/2+m1n3*2^1/2

(（m2+n2*2^1/2）+（m3+n3*2^1/2）)*（m1+n1*2^1/2）=（m2+n2*2^1/2）*（m1+n1*2^1/2）+（m3+n3*2^1/2）*（m1+n1*2^1/2）=m1m2+m1m3+2n1n2+2n1n3+m1n2*2^1/2+m1n3*2^1/2

所以（Z（2^1/2），+，*）是一个环。

3、因为其不满足封闭性：(m1+n1*2^1/3)*(m2+n2*2^1/3)=m1m2+(m1n2+m2n1)*2^1/3+n1n2*2^2/3,不在Q（2^1/3）中。

9、e是R的左单位元，则e*a=a(a属于R)，往证a*e=a。若a*e=b(b∈R,且b≠a)

e*e=b,e*e=e,b≠e，矛盾。所以a*e=a。即e也是右单位元，所以e是单位元。

10、a-1/b=（ab-1）/b,它的逆元为b/ab-1=b*(ab-1)。所以a-1/b的逆元为b乘上（ab-1）的逆元，因为b和ab-1的逆元均在R中，所以根据封闭性，b*（ab-1）也在R中，得证。同理，(a-b^-1) ^-1-a^-1=1/(a-1/b)-1/a=1/((ab-1)/b)-1/a=b/(ab-1)-1/a=1/(aba-a),根据封闭性，它也在R中。且（a-b^-1）^-1-a^-1=(aba-a)^-1，所以(（a-b^-1）^-1-a^-1)^-1=aba-a。得证。

P417

1、F仅有4个元素，其中包含0，且非零元素构成一个群，则这个群为3阶群，元素为{e,a,a^-1}。

①、则只需证a+a=0,根据推论13.2.1，则a^-1+a^-1=0。根据封闭性，a+a=0或e或a或a^-1。若 a+a=a,a*a^-1=(a+a)*a^-1=e+e=e,显然不成立，同理 a^-1+a^-1≠a^-1。若a+a=a^-1,a*a^-1=0,a*(a+a)=a*a+a*a=a^-1+a^-1=0,若成立，则根据推论13.2.1，阶应为2，则a+a应为0，矛盾，所以a+a≠a^-1,同理，a^-1+a^-1≠a。若a+a=e，根据上面的结

论，a^-1+a^-1=e。a*e=a(a^-1+a^-1)=a*a^-1+a^a-1=e+e,a*e=a,a=e+e,a=4a^-1,8a^-1=e,矛盾。所以只能 a+a=0。所以阶为 2，特征数为 2。

② 、x^2=x+e：x=a, a^2=a+e 因为乘法群为三阶群，所以 a^-1=a^2,即证 a+e=a^-1。

在加法群中：a+e 显然≠a 或 e，假设 a+e=0,a=-e,a^2=e,a^-1=e,矛盾。所以只剩下 a+e=a^-1 一种可能，即 a+e=a^2,同理可得 a^-1+e=(a^-1)^2。

③ 、

+	0	e	a	a^{-1}
0	0	e	a	a^{-1}
e	e	0	a^{-1}	a
a	a	a^{-1}	a	e
a^{-1}	a^{-1}	a	e	a^{-1}

*	0	e	a	a^{-1}
0	0	0	0	0
e	0	e	a	a^{-1}
a	0	a	a^{-1}	e
a^{-1}	0	a^{-1}	e	a