密码学与信息安全第一次作业

郭嘉　17345019　数学与应用数学

2020 年 4 月 12 日

1.（第一章第 3 题）
只需证明该环中任一元素 α 都存在逆元。
我们取 α、α^2、α^3、α^3...
注意到该环是有限环，则必存在 a,b$\in \mathbb{Z}+$ 使得 $\alpha^a = \alpha^b$(a>b)
交换整环满足消去律，即 $\alpha^{a-b} = 1$
即 α 的逆元为 α^{a-b-1}
得证
2.（第一章第 4 题）
由于 $\underbrace{1+1+...+1}_{ch(\mathbb{F})} = 0$
故对于 $\forall\alpha \in \mathbb{F}, (\underbrace{1+1+...+1}_{ch(\mathbb{F})}) * \alpha = 0$
即 $\underbrace{\alpha+\alpha+...+\alpha}_{ch(\mathbb{F})} = 0$
反之，若 $\underbrace{\alpha+\alpha+...+\alpha}_{n} = 0$ 且 $\alpha \neq 0$
则 n 不可能小于 ch($\mathbb{F}$)
否则 $(\underbrace{1+1+...+1}_{n}) * \alpha = 0$
由于 $\alpha \neq 0$, 故 $\underbrace{1+1+...+1}_{n} = 0$
故 ch($\mathbb{F}$)|n, 这与 n<ch($\mathbb{F}$) 矛盾
综上所述，每个非零元素的阶都是 n
得证
3.（第一章第 5 题）
由有限域的结构定理，所有四阶有限域都同构。
特别的由于容易验证 $x^2 + x + 1$ 是 $\mathbb{F}_2$ 上的二次既约多项式

故有 $\mathbb{F}\cong\mathbb{F}_2/(x^2+x+1)$

故 $\mathbb{F}$ 中的 4 个元素分别为 0,1,a,a+1，其中 $a^2+a+1=0$

（1）如上所述 $\mathbb{F}\cong\mathbb{F}_2/(x^2+x+1)$，故 1+1=0，即 ch（$\mathbb{F}$）=2

（2）如上所述故 $\mathbb{F}$ 中的 4 个元素分别为 0,1,a,a+1，其中 $a^2+a+1=0$，

故 $a^2=-a-1=a+1$ 和 $(a+1)^2=a^2+1=(a+1)+1$

得证

4.（第一章第 12 题）

(1) 由于 $|\mathbb{F}_8^*|$=7

故其中元素的阶要么为 7，要么为 1，若为本原元即为 7，否则为 1

但 φ(7)=6, 故除了乘法单位元 1 外，乘法群中其它元素阶都为 7

(2) 利用 $\alpha^3+\alpha+1=0$

有 $\alpha^3+\alpha^5=(\alpha+1)+(\alpha^3+\alpha)=\alpha^3+1=\alpha$

利用 $(1+\alpha)^7=1$

有 $(\alpha+1)^{-1}=(\alpha+1)^6=\alpha^6+6\alpha^5+15\alpha^4+20\alpha^3+15\alpha^2+6\alpha+1=\alpha^6+\alpha^4+\alpha^2+1=(\alpha+1)^2+(\alpha^2+\alpha)+\alpha^2+1=\alpha^2+\alpha$

5.（第一章第 13 题）

(1) 本章例题中已验证了 x^4+3x^2+1 与 x^4+x^2+1 都是 $\mathbb{F}_2$ 上除了 $x^4+x^3+x^2+x+1$ 外仅有的既约多项式。又 φ(16-1)=8，即本原元有八个，故这八个本原元就是 $x^4+3x^2+1=0$ 与 $x^4+x^2+1=0$ 的所有根。

容易验证 $\alpha+1$ 是 $x^4+3x^2+1=0$ 的一个根，那么 $(\alpha+1)^2=\alpha^2+1$，$(\alpha+1)^4=\alpha^3+\alpha^2+\alpha$，$(\alpha+1)^8=\alpha^3+1$ 是其余的三个根

容易验证 $\alpha^3+\alpha$ 是 $x^4+x^2+1=0$ 的一个根，那么 $(\alpha^3+\alpha)^2=\alpha^2+\alpha$，$(\alpha^3+\alpha)^4=\alpha^3+\alpha+1$，$(\alpha^3+\alpha)^8=\alpha^2+\alpha+1$ 是其余的三个根

上面所说的八个根就是 $\mathbb{F}_{16}$ 的全部本原元

(2) 如 (1) 中所述 $\alpha+1$ 的极小多项式是 $x^4+3x^2+1=0$

6.（第一章第 15 题）

$\mathbb{F}_2$ 上五次既约多项式个数为 $1/5\sum_{d|5}\mu(d)2^{5/d}=6$

$\mathbb{F}_2$ 上五次既约多项式个数为 $1/5\varphi(32-1)=6$

故只需要找 $\mathbb{F}_2$ 上的 6 个五次既约多项式

如例题中的推理，五次项和常数项是必须的，一次项到四次项只能有奇数个，即 1 个或 3 个，但这里总共有 8 个多项式，我们需要排除两个

$(x^3+x^2+1)(x^2+x+1)=x^5+x+1$ 和 $(x^3+x+1)(x^2+x+1)=x^5+x^4+1$ 就是我们所排除的，于是我们可以列出余下 6 个就是所求既约且本原的多

项式

分别为 x^5+x^2+1,x^5+x^3+1,$x^5+x^3+x^2+x+1$,$x^5+x^4+x^2+x+1$,$x^5+x^4+x^3+x+1$,$x^5+x^4+x^3+x^2+1$

7. 补充题 1

$z^{81}-z$ 在 $\mathbb{F}_3$ 上分解得到的所有四次因式就是 $\mathbb{F}_3$ 上所有的四次既约多项式

利用 sagemath：

```
R1.<z> = PolynomialRing(GF(3))
for i in (z^81-z).factor():
  print(i[0])
```

输出结果为：

z

$z+1$

$z+2$

z^2+1

z^2+z+2

$z^2+2*z+2$

z^4+z+2

$z^4+2*z+2$

z^4+z^2+2

z^4+z^2+z+1

$z^4+z^2+2*z+1$

z^4+2*z^2+2

z^4+z^3+2

$z^4+z^3+2*z+1$

$z^4+z^3+z^2+1$

$z^4+z^3+z^2+z+1$

$z^4+z^3+z^2+2*z+2$

$z^4+z^3+2*z^2+2*z+2$

z^4+2*z^3+2

z^4+2*z^3+z+1

$z^4+2*z^3+z^2+1$

$z^4+2*z^3+z^2+z+2$

$z^4 + 2 * z^3 + z^2 + 2 * z + 1$

$z^4 + 2 * z^3 + 2 * z^2 + z + 2$

其中最高次项为 4 的多项式就是所求既约多项式

对于其中的四次多项式 P(x), 取 $\mathbb{F}_3[x]/(P(x))$

若对于 $\forall\ 1 < n < 80$ 都有 $x^n \neq 1$

那么 P(x) 就是本原多项式

利用 sagemath：

```
for i in range(6,len(list((z^81-z).factor()))):
    poly=(z^81-z).factor()[i][0]
    R2.<x> = R1.quotient((poly)*R1)
    flag=1
    for j in range(1,80):
      if x^(j)==1:
      flag=0
      break;
    if flag==1:
      print(poly)
```

输出结果：

$z^4 + z + 2$

$z^4 + 2 * z + 2$

$z^4 + z^3 + 2$

$z^4 + z^3 + z^2 + 2 * z + 2$

$z^4 + z^3 + 2 * z^2 + 2 * z + 2$

$z^4 + 2 * z^3 + 2$

$z^4 + 2 * z^3 + z^2 + z + 2$

$z^4 + 2 * z^3 + 2 * z^2 + z + 2$

这就是我们需要的本原多项式

8. 补充题 2

右推左：

若 $F(x) = \sum_{n \leq x} \mu(n) G(\frac{x}{n})$

则 $\sum_{n \leq x} F(\frac{x}{n}) = \sum_{n \leq x} \sum_{nm \leq x} \mu(m) G(\frac{x}{mn}) = \sum_{a \leq x} G(\frac{x}{a}) \sum_{m|a} \mu(m)$

当 a=1 时第二个和式取 1，对其它 a，第二个和式为 0

故该式最终等于 G(x)，这就完成了右推左。

左推右：

若 $G(x) = \sum_{n \leq x} F(\frac{x}{n})$

则 $\sum_{n\leq x}\mu(n)G(\frac{x}{n})=\sum_{n\leq x}\mu(n)\sum_{nm\leq x}F(\frac{x}{mn})=\sum_{n\leq x}\sum_{nm\leq x}\mu(m)F(\frac{x}{mn})=\sum_{a\leq x}F(\frac{x}{a})\sum_{m|a}\mu(m)$

当 a=1 时第二个和式取 1，对其它 a，第二个和式为 0

故该式最终等于 F(x)，这就完成了左推右。

得证