第一周作业参考解答及补充

作业

1. (习题 1.1.6)

设 $p>2$ 是素数, $\mathbb{F}_p=\{\bar{0},\bar{1},\bar{2},\cdots,\overline{p-1}\}$ 是 $\mathbb{Z}$ 的模 p 剩余类域. 试计算:

(1) $\bar{2}$ 在 $\mathbb{F}_p$ 中的逆元 $\bar{2}^{-1}$;

(2) $\overline{p-1}\cdot\overline{p-2}$;

(3) $\overline{p-2}$ 在 $\mathbb{F}_p$ 中的逆元 $\overline{p-2}^{-1}$.

proof

(1) 只需找到能被 2 整除的 $1+kp(k\in\mathbb{Z})$. 由于素数 $p>2$, $p+1$ 即可. i.e. $\bar{2}^{-1}=\overline{\frac{1}{2}(p+1)}$.

(2) $\overline{p-1}\cdot\overline{p-2}=\overline{-1}\cdot\overline{-2}=\bar{2}$.

(3) 由 (1), $\overline{p-2}^{-1}=\overline{-2}^{-1}=\overline{-\frac{1}{2}(p+1)}=\overline{\frac{1}{2}(p-1)}$.

□

2. (习题 1.2.1)

设 R 是一个环, 试证明下述结论:

(1) (加法消去律) 如果 $a+c=b+c$, 则 $a=b$;

(2) $\forall a\in R$, 有 $a\cdot 0_R=0_R$;

(3) $-(-a)=a,\quad a(b-c)=ab-ac\quad(\forall a,b,c\in R)$;

(4) $-(a+b)=(-a)+(-b)\quad(\forall a,b\in R)$;

(5) $a(-b)=(-a)b=-(ab)\quad(\forall a,b\in R)$;

(6) $(-a)(-b)=ab\quad(\forall a,b\in R)$;

(7) $\forall a\in R,m,n\in\mathbb{Z}$, 有 $(m+n)a=ma+na,(mn)a=m(na)$;

(8) $\forall a,b\in R,n\in\mathbb{Z}$, 有 $n(a+b)=na+nb,n(ab)=a(nb)$;

(9) $\forall a,b\in R,m,n\in\mathbb{Z}$, 有 $(ma)\cdot(nb)=mn(a\cdot b)=(mna)\cdot b$;

(10) (二项式定理) $\forall a,b\in R$, 设 $ab=ba$, n 是正整数, 则

$$(a+b)^n=\sum_{i=0}^{n}\binom{n}{i}a^{n-i}b^i.$$

proof

(1) 两边同加 $-c$.

(2) 由于

$$a\cdot 0_R=a\cdot(0_R+0_R)=a\cdot 0_R+a\cdot 0_R.$$

再用一下负元消去即可, $0_R\cdot a=0_R$ 同理.

(3) 前一个为负元定义 (教材 p9 的注记); 后一个先由分配律,

$$a(b-c)=ab+a(-c),$$

又由于

$$a(-c)+ac=a(c+(-c))=a\cdot 0_R\overset{(2)}{=}0$$

得 $a(-c)=-ac$, 这也是 (5) 的证明. 这里要注意仅使用 $-a\overset{(*)}{=}-1_R\cdot a$ 也无法将负号提到前面, 需要 R 是交换环或者说明 $-1_R\cdot a=a\cdot(-1_R)=-a$.

$(*)$ 的证明如下

$$-1_R\cdot a+a=-1_R\cdot a+1_R\cdot a=(-1_R+1_R)\cdot a=0_R\cdot a\overset{(2)}{=}0_R.$$

右乘 -1_R 同理.

(4) 利用 $-a=-1_R\cdot a$ 和分配律展开即可.

(5) 见 (3).

(6) (3) 和 (5) 的推论.

(7) (7)-(9) 和习题 1.1.1 的 (6) 类似, 首先需要明确定义, 教材在这里并没有强调递归定义, 事实上, 这种和 $\mathbb{Z}$ 有关的东西都应该由递归定义给出, 相对应的证明要用归纳法. (就算不用归纳法, 至少要把正负整数分开证, 很多同学直接用一行证明, 这是不行的)

严格来说, 这是定义了一个映射

$$\mathbb{Z}\times R\to R,(n,a)\mapsto na,$$

其中

$$0a:=0_R,\ (n+1)a:=na+a,\ n\in\mathbb{N},$$

以及

$$na \coloneqq -((-n)a),\ n < 0.$$

(注意 na 不是 R 上的乘法, 有同学甚至写了 $\mathbb{Z} \subseteq R$ 然后直接乘法分配律, R 中是否有整数是不知道的)

由该定义可以验证对任意整数 $n \in \mathbb{Z}$ 均有 $(n+1)a = na + a$ 以及 $na = -((-n)a)$, 这样在使用这两个等式的时候不用再区分正负了.

回到原题, 对任意的 $m \in \mathbb{Z}$, 先用归纳法证明 $n \in \mathbb{N}$ 的情形, 负整数的情形可以结合定义得到.

$n = 0$ 根据定义左右均为 ma, 假设对 n 有 $(m+n)a = ma + na$, 根据定义有

$$(m+n+1)a = (m+n)a + a = ma + na + a = ma + (n+1)a.$$

由归纳法知

$$(m+n)a = ma + na, \quad \forall m \in \mathbb{Z}, n \in \mathbb{N} \tag{i}$$

当 $n < 0$ 时, 存在 $k \in \mathbb{Z}_{>0}$ 使得 $m + kn < 0$,

$$\begin{aligned}(m+n)a &= (m + kn - (k-1)n)a \\ &\overset{\text{(i)}}{=} (m+kn)a + (-(k-1)n)a \\ &= -(-m-kn)a + (n-kn)a \\ &\overset{\text{(i)}}{=} -((-m)a + (-kn)a) + na + (-kn)a \\ &\overset{(4)}{=} ma + (kn)a + na + (-kn)a = ma + na.\end{aligned}$$

第二个式子可直接利用第一个证明, $m = 0$ 根据定义左右均为 0_R, $m > 0$ 有,

$$\begin{aligned}(mn)a &= \left(\sum_{i=1}^{m} n\right) a \\ &= \sum_{i=1}^{m} (na) \\ &= m(na).\end{aligned}$$

$m < 0$ 利用 $mn = (-m)(-n)$, 做同样的操作.

(8) 对 n 归纳, 由于加法有交换律,

$$\begin{aligned}(n+1)(a+b) &= n(a+b) + a + b \\ &= na + nb + a + b \\ &= (n+1)a + (n+1)b.\end{aligned}$$

得

$$n(a+b) = na + nb, \quad \forall n \in \mathbb{N}$$

当 $n < 0$ 有

$$n(a+b) = -(-n(a+b)) = -((-n)a + (-n)b) \overset{(4)}{=} na + nb.$$

第二个等式使用分配律, $n = 0$ 根据定义左右均为 0_R, $n > 0$,

$$n(ab) = \sum_{i=1}^{n} ab = a \sum_{i=1}^{n} b = a(nb).$$

$n < 0$, 用 $n = -(-n)$, $n(ab) = -a((-n))b \overset{(5)}{=} a(nb)$. 同样的也会有 $n(ab) = (na)b$.

(9) (7) 和 (8) 的推论,

$$\begin{aligned}(ma)\cdot(nb) &\overset{(8)}{=} m(a\cdot(nb)) \\ &\overset{(8)}{=} m(n(ab)) \\ &\overset{(7)}{=} mn(ab) \\ &\overset{(8)}{=} (mna)\cdot b.\end{aligned}$$

(10) 对 n 归纳,

$$\begin{aligned}(a+b)^n\cdot(a+b) &= \left(\sum_{i=0}^{n}\binom{n}{i}a^{n-i}b^i\right)\cdot(a+b) \\ &= \sum_{i=0}^{n}\binom{n}{i}a^{n-i}b^i a + \sum_{i=0}^{n}\binom{n}{i}a^{n-i}b^{i+1} \\ &\overset{ab=ba}{=} \sum_{i=0}^{n}\binom{n}{i}a^{n-i+1}b^i + \sum_{i=0}^{n}\binom{n}{i}a^{n-i}b^{i+1} \\ &= a^{n+1} + \sum_{i=1}^{n}\left(\binom{n}{i}+\binom{n}{i-1}\right)a^{n-i+1}b^i + b^{n+1} \\ &= \sum_{i=0}^{n+1}\binom{n+1}{i}a^{n+1-i}b^i.\end{aligned}$$

□

注:

(7)-(9) 中实际上需要用归纳法证明的只有

$$n(a+b)=na+nb,$$
$$(m+n)a=ma+na,$$
$$(mn)a=m(na),$$

这三条加上 $1a=a$, 是在说任何一个 Abel 群都是 $\mathbb{Z}$-模 (见教材 5.1 节). 再反过来看 1.1.1 的 (6), 加上 $(ab)^n=a^nb^n$, 也是在说 K^* 是 $\mathbb{Z}$-模, 因为 K^* 关于域的乘法是 Abel 群.

另一方面, 可以先定义

$$N:\mathbb{Z}\to R,\quad n\mapsto n1_R$$

这是一个自然的环同态 (使用归纳法证明)

$$N(m+n)=N(m)+N(n);$$
$$N(mn)=N(m)\cdot N(n).$$

然后利用这个环同态得到 (注意用到的 $n(ab)=(na)b$ 的证明是直接使用分配律的, 因此不存在循环论证. N 表示使用了这个环同态, dis 表示使用了分配律, ass 表示使用了结合律):

$$n(a+b)=n(1_R(a+b))=(n1_R)(a+b)\overset{dis}{=}(n1_R)a+(n1_R)b=na+nb.$$

$$\begin{aligned}(m+n)a&=(m+n)(1_Ra)=((m+n)1_R)a\overset{N}{=}(m1_R+n1_R)a\overset{dis}{=}(m1_R)a+(n1_R)a\\&=ma+na.\\(mn)a&=(mn)(1_Ra)=(mn1_R)a\overset{N}{=}(m1_Rn1_R)a\overset{ass}{=}(m1_R)((n1_R)a)\\&=(m1_R)(na)=m(1_R(na))=m(na).\end{aligned}$$

这个同态是唯一的, 因为我们要求环同态要把 1 映到 1, 因此 $\mathbb{Z}$ 在 Ring 中是始对象 (initial object), Ring 表示环范畴. 因此 $\mathbb{Z}$ 可以认为是任意环 R 的一个子环, n 可看作是 R 中的元素 $n1_R$. 所以此后在没有歧义的情况下, 默认 0 就指零元, 1 指幺元.

3. (习题 1.2.9)

设 $m>0$ 是任意整数, $\mathbb{Z}_m=\{\bar{0},\bar{1},\cdots,\overline{m-1}\}$ 是 $\mathbb{Z}$ 的模 m 剩余类环. 试证明: $\bar{a}\in\mathbb{Z}_m$ 可逆当且仅当 $(a,m)=1$(即: a 与 m 互素).

proof

$\overline{a}\in\mathbb{Z}_m$ 可逆,

$$
\begin{aligned}
&\iff \exists\overline{b}\in\mathbb{Z},\quad \overline{a}\overline{b}=\overline{1}\\
&\iff ab=1+km,\quad k\in\mathbb{Z},\\
&\iff (a,m)=1.\quad \text{(Bézout's Identity)}
\end{aligned}
$$

□

注:

一般用记号 $\mathbb{Z}/m\mathbb{Z}$ 表示模 m 剩余类环.(理想和商环, 教材 2.1 节 p25)
若 $(a,m)=1$, 则 $\overline{a}$ 是加法群 $(\mathbb{Z}/m\mathbb{Z},+)$ 的生成元, 即 $\overline{a}$(在加法群) 的阶是 m.

4. (习题 1.2.10)

设 R 是仅有 n 个元素的环, 试证明对任意 $a\in R$ 有

$$
na:=\underbrace{a+a+\cdots+a}_{n}=0.
$$

proof

该题的证明归结为一句话: 加法群的阶 $(R,+)$ 为 n, 故 $na=0$. □

注:

有限群 G 内任一元素 a, 有 $|a|\Big||G|$(Lagrange 定理, 教材 4.1 节 p70 推论 4.1.3), 因此必有 $a^{|G|}=e$, 在这道题就是 $na=0$.
有些同学没有说明使用了 Lagrange 定理, 也没有证明这些子集 $b+\langle a\rangle=\{b+ma\mid m\in\mathbb{Z}\}$, $b\in R$(这里的 $\langle a\rangle$ 是对于加法群 $(R,+)$ 而言, 由 a 生成的子群, $\langle a\rangle=\{ma\mid m\in\mathbb{Z}\}$) 确实构成了 R 的一个分划 (partition), 而是直接使用/推出这些结论, 我觉得这样的证明是不完整的. 至少要说明一下

$$
b+\langle a\rangle\cap b'+\langle a\rangle\neq\varnothing \implies b+\langle a\rangle=b'+\langle a\rangle
$$

这个证明不难, 由交集非空

$$
\begin{aligned}
&\exists x\in b+\langle a\rangle\cap b'+\langle a\rangle\\
\implies& \exists m_1,m_2\in\mathbb{Z},\ x=b+m_1a=b'+m_2a\\
\implies& b=b'+(m_2-m_1)a\in b'+\langle a\rangle\\
\implies& \forall z\in b+\langle a\rangle,\ z=b+ma=b'+(m+m_2-m_1)a\in b'+\langle a\rangle\\
\implies& b+\langle a\rangle\subseteq b'+\langle a\rangle
\end{aligned}
$$

同理 $b'+\langle a\rangle\subseteq b+\langle a\rangle$, 因此 $b+\langle a\rangle=b'+\langle a\rangle$.

另外, " 设 r 是使得 $ra = 0_R$ 的最小正整数" 是需要说明的 (这个 r 就是 a 的阶).

先要说明 $\exists k \in \mathbb{Z}_{>0}$ 使得 $ka = 0_r$, 也就是说 $|a| < \infty$. 用反证法, 假设这样的正整数不存在, 则

$$\langle a \rangle = \{ma \mid m \in \mathbb{Z}\}$$

中必两两互不相等 (否则不妨设 $i < j$ 使得 $ia = ja$, 即 $(j-i)a = 0_R$, 矛盾).

而 R 中只有 n 个元素, 这样就已经矛盾了. 因此存在 $k \in \mathbb{N}$ 使得 $ka = 0_R$. 也就是说 $\{m \in \mathbb{N} \mid ma = 0_R\} \subseteq \mathbb{N}$ 非空. 由 $\mathbb{N}$ 的良序性, 存在一个最小的 r 使得 $ra = 0_R$. 这样 $\langle a \rangle = \{0, a, 2a, \cdots, (r-1)a\}$ 恰有 r 个元素 (如果还不放心这里面是否有相等元素, 在用一次反证就可以了, 和上面证两两不等类似).

5. (习题 1.3.2)

设 R 是一个环, $U(R)$ 表示 R 中所有可逆元集合, 试证明: $U(R)$ 关于环 R 的乘法是一个群 (称为 R 的单位群).

proof

(1) 这里首先需要验证运算的封闭性, $\forall a, b \in U(R)$, 有 $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = 1$, 故 $ab \in U(R)$ 且 $(ab)^{-1} = b^{-1}a^{-1}$.

很多同学漏了这一条, 这里的乘法是 R 上的乘法限制在 $U(R)$ 上, 即

$$\cdot : U(R) \times U(R) \to R,\ (a, b) \mapsto ab \in R,$$

(2) $1 \in U(R)$, 因为 $1 \cdot 1 = 1$ 的确可逆;

(3) 由于乘法是 R 上的乘法, 故结合律成立;

(4) 若 $a \in U(R)$, 则由习题 1.1.1 的 (3), $a^{-1} \in U(R)$ 且 $(a^{-1})^{-1} = a$;

□

6. (习题 1.3.5)

写出对称群 S_3 的乘法表.

proof

记 $\mathrm{id}_{S_3} = e$, 令 $a = (12), b = (123)$, 有 $a^2 = e, b^3 = e, abab = e \iff ba = ab^2$.

乘法表如下:

	e	a	b	b^2	ab	ab^2
e	e	a	b	b^2	ab	ab^2
a	a	e	ab	ab^2	b^2	b
b	b	ab^2	b^2	e	a	ab
b^2	b^2	ab	e	b	ab^2	a
ab	ab	b^2	a	ab^2	e	b
ab^2	ab^2	b	ab	a	b^2	e

$\square$

注:

可以看到 S_3, 若取 $a=(1\,2)$, $b=(1\,2\,3)$, 则 S_3 可以由 a,b 生成, 即考虑所有可能的乘积, 一般可以表示为 $S_3=\langle a,b\rangle$, $a=(1\,2)$, $b=(1\,2\,3)$.
若不给 a,b 加任何限制, 便得到一个自由群 (free group)$F(\{a,b\})$. 一般地, 任意一个集合 A 都可以生成一个自由群 $F(A)$, A 就是生成元组成的集合. 可以证明任何一个群都同构于某个自由群的商群, 而对应的正规子群便是由生成元满足的某些关系确定 (将 A 看成字母表, Σ_A 表示单词的集合, 这些关系可以表示为一些满足 $w=e$ 单词 $w\in\Sigma_A$). 把这些 w 组成的集合记为 $\mathscr{R}$, A 和 $\mathscr{R}$ 将唯一确定一个群 G, $(A\mid\mathscr{R})$ 称为 G 的一个展示 (presentation). 以 S_3 为例, S_3 的一个展示为 $(\{a,b\}\mid a^2,b^3,abab)$.
由于这本教材没有讲自由群, 所以想要了解的话需要查阅别的教材.

7. (习题 1.3.11)

证明:$GL_2(\mathbb{R})$ 中的元素 $x=\begin{pmatrix}0&1\\-1&0\end{pmatrix}$, $y=\begin{pmatrix}0&1\\-1&-1\end{pmatrix}$ 的阶分别是 4 和 3. 但 xy 是无限阶元.

proof

用 I_n 表示 n 阶单位阵, 计算可得

$$x^2=\begin{pmatrix}-1&0\\0&-1\end{pmatrix}, x^3=\begin{pmatrix}0&-1\\1&0\end{pmatrix}, x^4=\begin{pmatrix}1&0\\0&1\end{pmatrix}=I_2.$$

故 $|x|=4$, 同理,

$$y^2=\begin{pmatrix}-1&-1\\1&0\end{pmatrix}, y^3=\begin{pmatrix}1&0\\0&1\end{pmatrix}=I_2.$$

$|y| = 3$. 最后是 xy,

$$xy = \begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix}, (xy)^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, (xy)^3 = \begin{pmatrix} -1 & -3 \\ 0 & -1 \end{pmatrix}, \cdots$$

可以用归纳法证明

$$(xy)^n = (-1)^n \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \neq I_2, \forall n \in \mathbb{Z}_{\geqslant 1}.$$

故 $|xy| = \infty$. □

8. (习题 1.3.12)

证明群的任意多个子群的交仍是子群.

proof

设 G 是群, 记 I 为指标集, $H_i < G, \forall \in I$. 验证 $H = \bigcap\limits_{i \in I} H_i < G$:

$$\begin{aligned} \forall a, b \in H = \bigcap_{i \in I} H_i &\implies \forall i \in I,\ a, b \in H_i \\ &\implies ab^{-1} \in H_i, \quad \forall i \in I \\ &\implies ab^{-1} \in \bigcap_{i \in I} H_i = H. \end{aligned}$$

□

注:

很多同学认为"任意多"是有限个, 即只考虑 $H = \bigcap\limits_{i=1}^{n} H_i$, 也有同学考虑了 $H = \bigcap\limits_{i=1}^{\infty} H_i$, 这也是不够的, 这里是允许不可数无穷的.

课上的补充内容

1. (子群的判定)

设 G 是一个群, $\varnothing \neq S \subseteq G$, 则 $S < G$(S 是 G 的子群的记号) 当且仅当

$$\forall a, b \in S \iff ab^{-1} \in S.$$

2. (Bézout's Identity)

对 $m, n \in \mathbb{Z}$,

$$(m, n) = 1 \iff \exists u, v \in \mathbb{Z} \quad mu + nv = 1.$$