# 作业七 （12月8日课堂上交）

1. 本题中，自然数的定义（包括上面的加法、乘法等）是课程中通过Peano公理所定义的，整除、素数的概念也是依照课程中的定义。可以直接使用的，仅限于课件中和以往作业中证明过的结论（课件中练习中待证明的结论不可以直接使用）。

i) 证明自然数乘法的消去率：对于自然数 $m, n, k$ ，如果 $k \neq 0$ 且 $m \cdot k = n \cdot k$ ，则 $m = n$ 。

ii) 证明：若自然数 $m$ 和 $n$ 满足 $m \cdot n = 0$ ，则 $m = 0$ 或者 $n = 0$ 。

iii) 证明：对于非零自然数 $m, n$ 和素数 $p$ ，如果 $p|(m \cdot n)$，则 $p|m$ 或者 $p|n$ 。

iv) 证明：假定 $m$ 是大于等于 $2$ 的自然数，则 $m = p_1^{k_1} \cdots p_s^{k_s}$ ，其中 $p_1, \cdots, p_s$ 是互不相等的素数，并且 $r_1, \cdots, k_s$ 都是大于等于 $1$ 的自然数。如果不考虑其中互不相等素数排列的次序，$m$ 的如上分解（称为素因子分解）还是唯一的。

注：iv）中所证明之结论，也被称为唯一分解定理。不仅仅是自然数（或者整数），只要能够做带余除法（Euclidean性），并且满足 ii）中所证明之性质，都有类似的唯一分解定理（比如关于 $x$ 的实系数多项式全体）。其证明方法，和上面 iv) 的证明方法，本质上是一样的。

2. 根据课上所学内容，完成如下：

i) 在群 $G$ 中，若将 $a$ 的逆元记为 $a^{-1}$ ，将 $b$ 的逆元记为 $b^{-1}$ 。证明（或者更准确的说，验证）：$a \cdot b$ 的逆元是 $b^{-1} \cdot a^{-1}$ 。

ii) 证明：群 $G$ 的左乘，的确是个群 $G$ 在集合 $G$ 上的作用。其中左乘定义如下（作为集合， $X = G$）：

$$G \times X \longrightarrow X, \ \ (g, x) \mapsto g \cdot x \ \ \forall\, g \in G, x \in G \text{ 。}$$

iii) 群 $G$ 的右乘，是不是个群 $G$ 在集合 $G$ 上的作用？若是，给出证明；若否，给出证明。这里右乘定义为（作为集合， $X = G$ ）：

$$G \times X \longrightarrow X, \ \ (g, x) \mapsto x \cdot g \ \ \forall\, g \in G, x \in G \text{。}$$

iv) 假定

$$G \times X \longrightarrow X, \, (g, x) \mapsto g(x) \ \ \forall\, g \in G, x \in X$$

给出了群 $G$ 在集合 $X$ 上的作用。对于 $G$ 的任意子群 $H$ ，证明

$$H \times X \longrightarrow X, \, (h, x) \mapsto h(x) \ \ \forall\, h \in H, x \in X$$

给出了群 $H$ 在集合 $X$ 上的作用。

## 参考答案

1.

i) 证明：

由于 $k \neq 0$ ，不妨假定 $k > 0$ （否则若 $k < 0$ ，令 $k$ 为 $-k$ 即可）。由于 $k > 0$ ，存在 $p \in \mathbb{N}$ ，使得 $k = p^+$ 。

因为 $mk = nk$ ，我们有 $(m - n)k = 0$ 。需要证明 $m - n = 0$ 。若不然，则 $m - n > 0$ 或者 $m - n < 0$ 。

如果 $m - n > 0$ ，则存在 $s \in \mathbb{N}$ ，使得 $m - n = s^+$ 。因此

$$0 = (m - n) \cdot k = s^+ \cdot k = k \cdot s^+ = k \cdot s + k = ks + p^+ = (ks + p)^+ \text{。}$$

这与Peano公理中 “$0$ 不是任何自然数的后继”矛盾。

如果 $m-n<0$ ，即 $n-m>0$ ，我们可以用类似的方法得到矛盾。

由于 $m-n>0$ 和 $m-n<0$ 均不可能成立，由三歧律，有 $m-n=0$ ，即 $m=n$ 。证毕。 □

ii) 证明：我们使用反证法。

假定 $m\cdot n=0$ 且自然数 $m$ 与 $n$ 均不为 $0$ ，则存在自然数 $p,q$ ，使得 $m=p^+,n=q^+$ 。

因此

$$0=mn=mq^+=mq+m=mq+p^+=(mq+p)^+\ ,$$

这与Peano公理中 “$0$ 不是任何自然数的后继”矛盾，证毕。 □

iii) 证明：采用反证法。

假定有非零自然数 $m,n$ 和素数 $p$ ，使得 $p|(m\cdot n)$ ，并且 $p\nmid m$ ，$p\nmid n$ 。

因为 $p$ 为素数， $p$ 的因子只有 $1$ 和 $p$ 。因为 $p\nmid m$ ，因此 $\gcd(p,m)=1$ 。同理， $\gcd(p,n)=1$ 。

根据课件中的结论（将辗转相除倒过来走），由于 $\gcd(p,m)=1$ ，存在整数 $a,b$ ，使得

$$ap+bm=1\text{ 。}$$

同理，存在整数 $a',b'$ ，使得

$$a'p+b'n=1\text{ 。}$$

将这两个等式两边分别相乘，得到

$$aa'p^2+ab'np+bma'p+bb'mn=1\text{ 。}$$

注意到 $p|aa'p^2$ ，$p|ab'np$ ，$p|bma'p$ ，因此

$$p|\left(aa'p^2+ab'np+bma'p\right)\text{ 。}$$

根据题设，$p|(m\cdot n)$ ，因此 $p|bb'mn$ 。故

$$p|\left(aa'p^2+ab'np+bma'p+bb'mn\right)\text{ 。}$$

换言之，$p|1$ ，矛盾（为什么？）。证毕。

iv) 这里给出证明框架供参考。

关于素因子分解的存在性，只需要对 $m$ 不断进行分解，直到出现的每个因子都是素数为止。因为每次分解后，因子都是严格变小的，因此有限步后肯定会停止在“每个因子都是素数”的阶段。这样得到的就是素因子分解。

关于素因子分解的唯一性，假定关于 $m$ 有两个素因子分解。我们反复利用 iii) 中的结论以及 i) 中证明的乘法消去律对两边进行“消去公共素因子”的操作。每次这样的操作后得到的自然数值，一定严格小于原来的自然数。因此有限步后一定会停止。

2.

i) 只需要验证

$$(b^{-1}a^{-1})\cdot(ab)=b^{-1}\cdot(a^{-1}a)\cdot b=b^{-1}\cdot e\cdot b=b^{-1}\cdot b=e$$

以及

$$(ab)\cdot(b^{-1}a^{-1})=a\cdot(b\cdot b^{-1})\cdot a^{-1}=a\cdot e\cdot a^{-1}=a\cdot a^{-1}=e$$

即可。

ii) 按照定义逐条验证即可。

iii) 未必。

这是因为

$$g(h(x))=g(x\cdot h)=(x\cdot h)\cdot g=x\cdot(h\cdot g)$$

而

$$(g\cdot h)(x)=x\cdot(g\cdot h)$$ 。

一般的， $h\cdot g$ 和 $g\cdot h$ 未必相同，因此 $x\cdot(h\cdot g)$ 未必等于 $x\cdot(g\cdot h)$ 。当然，如果 $G$ 是交换群，$g\cdot h$ 始终等于 $h\cdot g$ ，因此对于交换群，右乘也是个作用。但是对于非交换群，右乘不是个作用。

iv) 根据定义逐条验证即可。