第六章作业解答

3. 自然数集N 上的二元代数运算 * 定义为 $x * y = x^y$，* 是否满足结合律？是否满足交换律？

解：都不满足。

4. 设 * 是集合S上的二元代数运算，且满足结合律，设x，y是S中任意元素，如果 $x * y = y * x$，则 $x = y$。试证明 * 满足等幂律。

证明：由于对S中任意的x，y和z，有 $x*(y*z)=(x*y)*z$，故 $x*(x*x)=(x*x)*x$，于是有 $x*x=x$。

2. 举例说明不要求可除条件而要求消去条件，即要求由 $a\chi=ay$ 可推出 $\chi=y$，由 $\chi\cdot a=y\cdot a$ 可推出 $\chi=y$，则G不见得是一个群，若G有限怎么样？

解：例如，全体自然数在普通乘法下，适合消去律，但不是群。若 $G=\{a_1，a_2，\ldots a_n\}$，用a右乘G中各元素得 $a_1a，a_2a，\ldots，a_na$ 必不相同（无限也不相同），否则若 $a_ia=a_ja$ $(i\neq j)$，由消去条件有 $a_i=a_j$，矛盾。所以 $G=\{a_1a，a_2a，\ldots，a_na\}$(因为有限)。对任意 $b\in G$，必有 a_i，使 $a_ia=b$，因之方程 $xa=b$ 有解。同理可知 $ay=b$ 有解。故G是群。

1. 计算（1 2 3）（2 3 4）（1 4）（2 3）。

解：（1 2 3）（2 3 4）（1 4）（2 3）=（1 3）（2 4）。

I，(1)(2)(3)(4)，(1)等等

5. 证明n个元素的所有偶置换作成群（叫做n次交代群）。写出四次交代群中的元素。n次交代群的元数为何？

证明：注意到偶置换×偶置换=偶置换。易知偶置换成群。

A_4：(1)，(1 2 3)，（1 3 2），（1 2 4），（1 4 2），

（1 3 4），（1 4 3），（2 3 4），（2 4 3），（1 2）（3 4），（1 3）（2 4），（1 4）（2 3），$\frac{1}{2}$ n!。

8. 求证循环群的子群仍是循环群。

证明：若循环群G由其中元a生成。H是的子群，但不是单位元群。则H中必含有幂 $m>0$ 的元 a^m。因为若 $m<0$，a^m 的逆元 a^{-m} 也在H内，而 $-m>0$。假定 a^m 是H中的最小正幂，显然H包含 a^m 的任意乘幂。假如又有H中任意元 a^S，由 $S=tm+r$。$0\leq r<m$ 知 $a^r=a^{S-tm}=(a^S)\cdot(a^m)^{-t}$ 是H中元，但m最小。而 $0\leq r<m$，故 $r=0$，因此有 $a^S=(a^m)^t$ 这表明H中任意元 a^S 也是 a^m 的乘幂，而知H为 a^m 生成的循环群。

10. 求证若G的元数是一个质数，则G必是循环群。

证明：设G的元数为质数P，任取G中非单位元a，则(a)是G的一个循环子群，设a的周期为r，则(a)的元数为r，因此r|P。但P是质数。显然r=P，所以G=(a)，即G是由a生成的循环群。

2. 设σ是G到G'上的同态映射。τ是G'到G"上同态映射，说明τσ是G到G"上的同态映射。并说明τσ的核为 $\sigma^{-1}\tau^{-1}(1")$，其中1"是G"的壹。

证明：首先由题意，τσ是G到G"上的映射。

对任意 $a\in G$，$b\in G$，有 $\tau\sigma(a\bullet b)=\tau(\sigma(a\bullet b))=\tau(\sigma(a)\bullet\sigma(b))=\tau(\sigma(a))\bullet\tau(\sigma(b))=\tau\sigma(a)\bullet\tau\sigma(b)$，故τσ为同态映射。因此τσ是G到G"上的同态映射。

1”在τσ下在G中原像集是$\sigma^{-1}\tau^{-1}(1”)$，$\tau\sigma(\sigma^{-1}\tau^{-1}(1”))=1”$，所以τσ的核为$\sigma^{-1}\tau^{-1}(1”)$。

3. 设σ是G到G’上的同态映射。H是包含σ的核N的G的正规子群。H’＝σ（H），求证H’是G’的正规子群。并证明“第一同构定理”：$\frac{G}{H}\cong\frac{G'}{H'}$。

证明：由题意可知H’是G’的子群。对任g’∈G’，必有g∈G，使σ(g)=g’。所以由$gHg^{-1}\subseteq H$，而$\sigma(gHg^{-1})=\sigma(g)\sigma(H)\sigma(g)^{-1}\subseteq\sigma(H)=H'$。所以$g'H'g'^{-1}\subseteq H'$。这表明H’是G’的正规子群。

因H’是G’的正规子群。故有同态映射τ，使G’~$\frac{G'}{H'}$，其核为H’，1”为$\frac{G'}{H'}$的壹。又在σ下，G～G’，故在τσ下G～$\frac{G'}{H'}$同态核为$\sigma^{-1}\tau^{-1}(1”)=\sigma^{-1}(H')$。因为H⊇N，所以$\sigma^{-1}(H')=H$。故τσ的核为H，因此$\frac{G}{H}\cong\frac{G'}{H'}$.

4. 设H和N都是G的正规子群，H⊇N。证明由第一同构定理推出：$\frac{G}{H}\cong\frac{G/N}{H/N}$。

证明：因为N是G的正规子群，则有同态映射σ使G～G/N，看σ（H）在G/N中所有的映象。注意到G/N中元素是G中对N来看的陪集N_{a1}, N_{a2}, …, 其中代表$a_i\in G(i=1,2,\ldots,)$。因此H中任意元在G/N中的映象也是N的陪集，代表元应取自上面属于H的各a_i。可见H在G/N中的象正是H/N。根据第一同构定理，H/N是G/N的正规子群，并且G/H≅$\frac{G/N}{H/N}$。

2. 列举I/12I的所有理想。

解：

$\{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4},\bar{5},\bar{6},\bar{7},\bar{8},\bar{9},\overline{10},\overline{11}\}$;

$\{\bar{0},\bar{2},\bar{4},\bar{6},\bar{8},\overline{10}\}$;

$\{\bar{0},\bar{3},\bar{6},\bar{9}\}$;

$\{\bar{0},\bar{4},\bar{8}\}$;

$\{\bar{0},\bar{6}\}$;

$\{\bar{0}\}$

5. A，B是理想N在环R中的两个剩余类。命P为所有ab的集合，a∈A,b∈B，则自然P⊆AB，举例说明P不见得等于AB。

解：对整数环I，取理想5I，I/5I=$\{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4}\}$

令A=$\bar{0}$={0，5，10，…，}，B=$\bar{2}$={2，7，12，…}。则AB=$\bar{0}$.
因此，5∈AB，但5∉P，故P≠AB。

1. 在R_{17}中$\frac{3}{4}$等于什么?

解：在R_{17}中$4\times13\equiv1(\bmod 17)$，故$4^{-1}=13$，$\frac{3}{4}=3\times4^{-1}=2\times13=39\equiv5(\bmod 17)$。

2. 在R_5中$\sqrt{-1}$等于什么?

解：R_5中$-1=4$，$\sqrt{4}=\pm2$，$-2=3$，故R_5中$\sqrt{-1}$是2或3。

6. 在R_2上分解x^4+x^3+x+1为质因式的乘积。

解：$x^4+x^3+x+1=(x+1)^2(x^2+x+1)$

3. 求证x^3-3x+1在R_0上不可约。

证明：三次多项式若可约必有一次因式，必有有理根，用可能的根±1试之均不是，故不可约。

4. 求证：x^5+3x^2-1在R_0上不可约

证明：在R_2上看$f(x)=x^5+x^2+1$。

$f(0)=1,f(1)=1$,故无一次因子。

注意R_2上二次质式只有x^2+x+1,而$x^5+x^2+1=(x^2+x+1)(x^3-x^2)=1$，故无二次因子。

所以x^5+3x^2-1在R_2上不可约，从而在R_0上必不可约。

5. 求证 $x^4+3x^3+3x^2-5$在R_0上不可约。

证明：

在R_2上看，$x^4+3x^3+3x^2-5=(x+1)(x^3+x+1)$；

而x^3+x+1在R_2上是质式（需证明）；

又因为：R_0上最高质因式次数大于等于R_2上最高质因式次数，所以，R_0上最高质因式次数为3或4。

若R_0上最高质因式次数为4，则$f(x)$在R_0上不可约；若在R_0上最高质因式次数为3，则必有一次质因式。

但±5与±1均不是上式的根。故上式无一次质因式，故在R_0上不可约。

1. 求$\Phi_{72}(x)$

解：$\Phi_{72}(x)=x^{24}-x^{12}+1$

1. GF（9）中的元素可表为$a+b\varphi$的形式，其中a,b为0，1或－1，试列出其乘法表。

解：

·	0	1	φ	1-φ	-1-φ	-1	-φ	-1+φ	1+φ
0	0	0	0	0	0	0	0	0	0
1	0	1	φ	1-φ	-1-φ	-1	-φ	-1+φ	1+φ
φ	0	φ	1-4	-1-φ	-1	-φ	-1+φ	1+φ	1
1-φ	0	1-φ	-1-4	-1	-φ	-1+φ	1+φ	1	φ

-1-φ	**0**	**-1-**φ	**-1**	**-**φ	**-1+**φ	**1+**φ	**1**	φ	**1-**φ
-1	**0**	**-1**	**-**φ	**-1+**φ	**1+**φ	**1**	φ	**1-**φ	**-1-**φ
-φ	**0**	**-**φ	**-1+**φ	**-1+**φ	**1+**φ	**1**	φ	**-1-**φ	**-1**
-1+φ	**0**	**-1+**φ	**1+**φ	**1+**φ	**1**	φ	**1-**φ	**-1**	**-**φ
1+φ	**0**	**1+**φ	**1**	**1-**φ	**1-**φ	**-1-**φ	**-1**	**-**φ	**-1+**φ