往年期末考卷重点题目

试卷见附件2018年卷子，2019年卷子，下面的证明只给出大概思路而不是严格的证明。

2018

7. （1）$< G, * >$是有限阶群，$|G| \geq 2$且$\forall a \in G, a^2 = e$成立，试证明$\exists n \in \mathbb{Z}, |G| = 2^n$

   证明：这里提供一个思路

   首先证明G是交换群，由于$\forall a \in G, a^2 = e \Leftrightarrow a = a'$成立，所以对$\forall a, b \in G$，有$ab = (ab)' = b'a' = ba$，即$G$是交换群

   由于$|G| \geq 2$，所以可以取$g \in G, g \neq e$，由g生成的子群$H = \{e, g\}$是G的二阶正规子群（其正规性由G的交换性可以得到）

   然后对于商群G/H，可以看到$|G| = 2 \times |G/H|$对于$\forall aH \in G/H, (aH)^2 = a^2H = eH = H$，所以$G/H$中元素除单位元$H$之外也均为二阶元，与$G$具有相同的性质，所以又可以做如上的商群同态，如此反复下去直到某个商群只剩下单位元，由于G有限阶，所以这一过程必定在有限步终止，所以$|G| = 2^n$。

2019

1. 已知存在一些正整数 n，满足：
   (1)$2^n - n$ 是 3 的整数倍；

   (2)$3^n - n$ 是 5 的整数倍；

   (3)$5^n - n$ 是 2 的整数倍；
   求同时满足条件 (1)(2)(3) 的 n 的最小值？

   解：本题看上去比较唬人，是一个指数与线性混合的方程，然而只要稍加分析其实很容易解决。

   首先考虑条件(3)，注意到5^n是一个奇数，所以若要$5^n \equiv n(mod\ 2)$，等价于有$n \equiv 1(mod\ 2)$成立。

   再考虑条件(1)，由于$2 \equiv -1(mod\ 3) \Rightarrow 2^n \equiv (-1)^n(mod\ 3)$成立，又因为$n$是奇数，所以有$n \equiv 2^n \equiv (-1)^n \equiv -1 \equiv 2(mod\ 3)$

   条件(2)稍微有些难处理，我们先考察3^k模5意义下的余数:

$$
\begin{aligned}
3^0 &\equiv 1(mod\ 5)\\
3^1 &\equiv 3(mod\ 5)\\
3^2 &\equiv 4(mod\ 5)\\
3^3 &\equiv 2(mod\ 5)\\
3^4 &\equiv 1(mod\ 5)\\
3^5 &\equiv 3(mod\ 5)\\
3^6 &\equiv 4(mod\ 5)\\
3^7 &\equiv 2(mod\ 5)
\end{aligned}
$$

   可以看到的是其余数每隔4个重复出现一次，即以4为周期。

   另一方面，n模5意义下的余数显然以5为周期循环，所以从1开始，3^n与n的余数对应关系(或者说$3^n - n$模5的余数)以4和5的最小公倍数20为周期循环。

   所以我们使用最粗暴的枚举法，检查n取0到19时模5的余数如下

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
$n\ mod\ 5$	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4
$3^n\ mod\ 5$	1	3	4	2	1	3	4	2	1	3	4	2	1	3	4	2	1	3	4	2

于是可以看到$3^n \equiv n(mod\ 5) \Leftrightarrow n \equiv 7, 13, 14, 16(mod\ 20)$，由于之前有要求$n$为奇数，得$n \equiv 7, 13(mod\ 20)$，与前面得到的$n \equiv 1(mod\ 2)$，$n \equiv 2(mod\ 3)$联合求解，由于$2, 3, 20$的最小公倍数为60，所以可以看到只要验证60以内的情况就可以了，最终求得解47满足题意。

2. 证明：若两个正整数 a,b 互素，则存在正整数 m,n，使得$a^m + b^n \equiv 1(mod\ ab)$

   证明：由于a, b互素，所以有

$$
\begin{aligned}
& a^m + b^n \equiv 1(mod\ ab) \\
\Leftrightarrow & \begin{cases} a^m + b^n \equiv 1(mod\ a) \\ a^m + b^n \equiv 1(mod\ b) \end{cases} \\
\Leftrightarrow & \begin{cases} b^n \equiv 1(mod\ a) \\ a^m \equiv 1(mod\ b) \end{cases}
\end{aligned}
$$

   由欧拉定理，只需要取$m = \varphi(b), n = \varphi(a)$即可。

补充题目

1. 证明非平凡群G没有非平凡子群的充分必要条件是G为素数阶循环群。

   证明:

   "⇒"

   由于G非平凡，所以G有至少一个非单位元$a \neq e$，而G没有非平凡子群，所以考虑a生成的子群(a)，由于$a \notin \{e\}$，所以$(a) \neq \{e\}$，所以$(a) = G$，于是G是循环群

   若G是无限阶，则$G = \{e, a, a^{-1}, a^2, a^{-2}, \cdots\}$，则显然$H = \{e, a^2, a^{-2}, a^4, a^{-4}, \cdots\}$是$G$的非平凡子群，不合题意，故$G$是有限阶。

   设$G = \{e, a, a^2, \cdots, a^{n-1}\}$，显然$a$的阶是$n$，所以$a^m$的阶是$\frac{n}{(n,m)}, m = 1, 2, \cdots, n-1$，又因为$G$没有非平凡子群，所以$G$中非单位元的阶都是$n$，所以$(n, m) = 1, m = 1, 2, \cdots, n-1$，所以$|G| = n$为素数。

   "⇐"

   显然

2. 设A是有限群G的一个非空子集，证明：$AA \subseteq A \Leftrightarrow A \leq G$。

   证明：

   "⇐"显然

   “⇒”

   乘法封闭性显然。

   有逆：对于$\forall a \in A$，由于$AA \subseteq A$，知道$a^k \in A$对$k \in \mathbb{Z}^+$成立，又因为A是有限集合，所以必定存在$n \in \mathbb{Z}^+$使得$a^n = e$，于是$a^{n-1} = a'$，可以知道a在A中有逆，A是G子群。

3. 设A,B都是G的子群，则当且仅当$AB = BA$时，AB是G的子群

   证明：

   "⇐"

   若$AB \leq G$，则对于$\forall ab \in AB$，$\exists a_1 b_1 \in AB, ab = (a_1 b_1)'$成立，于是有$ab = (a_1 b_1)' = b_1' a_1' \in BA$。所以$AB \subseteq BA$

   另一方面，对于$\forall ba \in BA$，有$ba = (a'b')' \in AB$。于是$BA \subseteq AB$

   综上所述，$AB = BA$成立。

"$\Rightarrow$"

若$AB=BA$，则对于$\forall a_1b_1,a_2b_2\in AB$，有$a_1b_1(a_2b_2)'=a_1b_1b_2'a_2' \overset{def}{=} a_1ba_2'$，由于$AB=BA$所以存在$a_3b_3\in AB$使得$a_3b_3=ba_2'$成立，于是$a_1ba_2'=a_1a_3b_3 \overset{def}{=} ab_3\in AB$，所以$AB\leq G$。

4. 若$G_1\trianglelefteq G, G_2\trianglelefteq G_1$，那么是否有$G_2\trianglelefteq G$?为什么？

   否，令$G=A_4$，$G_1=\{e,(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\}$，$G_2=\{e,(1,2)(3,4)\}$即得($(1,2,3)^{-1}G_2(1,2,3)\neq G_2$)。

5. 试证:设A是G的一个子群，H是G的正规子群，那么有$AH/H\cong A/(A\cap H)$。

   证明:

   $AH=a_1H\cup a_2H\cup\cdots(a_1,a_2,\cdots\in A)$，对$a_i,a_j\in A$，有$a_iH=a_jH\Leftrightarrow a_i'a_j\in H\Leftrightarrow a_i'a_j\in A\cap H\Leftrightarrow a_i(A\cap H)=a_j(A\cap H)$，所以可以定义映射$\varphi: AH/H\rightarrow A/(A\cap H),\varphi(aH)=a(A\cap H))$。显然它是同态。

   若对于$a\in A,\varphi(aH)=(A\cap H)$则有$a\in A\cap H$成立，所以$aH=H$成立，即$ker(\varphi)=\{H\}$，所以是同构映射。

6. 设H是群G的正规子群，$a\in G$，试证：如果a的阶与H在G中的指数互素，则$a\in H$。

   证明：

   设$[G:H]=m$，则$a^m\in H$。（习题结论，使用自然同态证得）

   又设a的阶是l，则$a^l=e\in H$，$(l,m)=1$，所以由裴蜀定理知$a=a^{\alpha m+\beta l}\in H$。

7. 设G是有限群，H是其正规子群，A是其子群，试证：若A在G中的指数与H的阶互素，则H是A的正规子群。

   证明：

   由于A在G中的指数$[G:A]=\frac{|G|}{|A|}$与H的阶互素，所以由裴蜀定理，$\exists\alpha,\beta,s.t.\ \alpha\frac{|G|}{|A|}+\beta|H|=1$成立，即$\alpha|G|+\beta|H||A|=|A|$

   另外由$|HA|=\frac{|H||A|}{|H\cap A|}$公式知道$|H||A|=|HA||H\cap A|$成立。

   此外由于H是正规子群，所以易得$AH=HA$成立，所以由第三题结论，HA是G的子群，$|HA|\mid|G|$成立

   综上可知$|HA|\mid|A|$成立，另一方面，由于HA是数个A陪集的交，所以$|A|\mid|HA|$成立，所以$|A|=|HA|$成立，又因为$A\subseteq HA$，所以$A=HA$成立，所以$H\leq A$成立，又因为H是G的正规子群，所以也是A的正规子群。

8. 设A,B是G的两个正规子群，若他们的阶互素，则A,B的任意元素可交换。

   证明：

   考察$A\cap B$，若其中有非单位元的元素a，由于A,B都是有限阶的，所以这个元素也是有限阶且阶大于1，考察子群(a)，它非平凡子群且同时是A,B的子群，这与A,B阶互素矛盾，所以$A\cap B=\{e\}$成立。

   还记得作业习题中关于换位元的讨论吗？对于$\forall a\in A,b\in B$，考察换位元$a'b'ab$，容易看到由于A,B是正规子群，所以$a'b'ab=(a'b'a)b=a'(b'ab)\in A\cap B$成立，所以$a'b'ab=e$，即$ab=ba$成立。