# SOLUTIONS TO LECTURE 2 PROBLEMS

**P5** # 24 of pg. 55 Gallian

$U(12) = \{1, 5, 7, 11\}$ with multiplication modulo 12

| $\cdot$ | 1 | 5 | 7 | 11 |
|---|---|---|---|---|
| 1 | 1 | 5 | 7 | 11 |
| 5 | 5 | 1 | 11 | 7 |
| 7 | 7 | 11 | 1 | 5 |
| 11 | 11 | 7 | 5 | 1 |

$$\left.\begin{aligned}
5(5) &= 25 = 1 \\
5(7) &= 35 = 24+11 = 11 \\
5(11) &= 5(-1) = -5 = 7 \\
7(7) &= 49 = 48+1 = 1 \\
7(11) &= 7(-1) = -7 = 5 \\
11(11) &= (-1)(-1) = 1.
\end{aligned}\right\} \text{Calculations } \underline{\text{mod } 12}$$

– (I'm showing work to give ideas on how to calculate, I'm not suggesting you need to show work here ☺ )–

–( IN CONTRAST, MUCH WORK MISSING IN NEXT PROBLEM BY MOST STUDENTS... )–

**Lemma**: if $m, k \in \mathbb{Z}$ and $g \in G$ where $G$ is a group then $g^m g^k = g^{m+k}$ given that we define $g^0 = e$ where $e$ is the group identity and $g^n = g^{n-1}g$ for $n \in \mathbb{N}$ and $g^{-n} = (g^{-1})^n$ for $n \in \mathbb{N}$. (these def$^{n}$'s were given in lecture)

Proof: fix $m \in \mathbb{Z}$. ① Notice $g^m e = g^m = g^{m+k}$ for $k=0$ thus $g^m g^k = g^{m+k}$ for $k = 0$.

---

② If $m \geq 0$ then $g^m g = g^{m+1}$ by def$^{n}$ hence $g^m g^k = g^{m+k}$ in the case $m \geq 0$ and $k = 1$. Suppose $m < 0$ then $m = -n$ for some $n \in \mathbb{N}$ and

$$\begin{aligned} g^m g = g^{-n} g &= (g^{-1})^n g &&: \text{def}^{n} \text{ of negative power} \\ &= (g^{-1})^{n-1} g^{-1} g &&: \text{def}^{n} \text{ of power in } \mathbb{N}, \\ &= g^{1-n} &&: (g^{-1})^{n-1} = (g)^{-1(n-1)} \\ &= g^{m+1} &&: m = -n. \end{aligned}$$

Hence $g^m g^k = g^{m+k}$ for $m<0$ and $k = 1$.

Inductively suppose $g^m g^k = g^{m+k}$ for some $k \in \mathbb{N}$

Consider, $g^m g^{k+1} = g^m g^k g = g^{m+k} g$ by induct. hypo. hence $g^m g^{k+1} = g^{m+k} g = g^{m+k+1}$ and we conclude by induction on $k$ that $g^m g^k = g^{m+k}$ for all $k \in \mathbb{N}$ in the case $m \geq 0$. It remains to show $g^m g^k = g^{m+k}$ for $k = -1, -2, -3, \ldots$ in the case $m \geq 0$, I'll be a bit less verbose,

$$g^m g^{-1} = g^{m-1} g g^{-1} = g^{m-1} \Rightarrow g^m g^k = g^{m+k} \text{ for } k = -1.$$

Continued

## Proof of Lemma Continued ($m \geq 0$)

We seek to show $g^m g^{-n} = g^{m-n}$ for $n \in \mathbb{N}$.
We already proved $-n = k = -1$ or $n=1$ last page.
Suppose inductively, $g^m g^{-n} = g^{m-n}$ for some $n \in \mathbb{N}$.
Consider,
$$\begin{aligned} g^m g^{-(n+1)} &= g^m (g^{-1})^{n+1} \\ &= g^m (g^{-1})^n g^{-1} \\ &= g^m g^{-n} g^{-1} \\ &= g^{m-n} g^{-1} \quad (*) \end{aligned}$$

There are several cases to consider for $(*)$

(i.) $m-n=0$ then $g^m g^{-(n+1)} = g^0 g^{-1} = g^{-1} = g^{m-n-1}$.

(ii.) $m-n>0$ then $g^m g^{-(n+1)} = g^{m-n-1} g g^{-1} = g^{m-n-1}$

(iii.) $m-n<0$ then
$$\begin{aligned} g^m g^{-(n+1)} = g^{m-n} g^{-1} &= (g^{-1})^{n-m} g^{-1} \\ &= (g^{-1})^{n-m+1} \\ &= g^{-1(n-m+1)} \\ &= g^{m-n-1} \end{aligned}$$

Thus, $g^m g^{-(n+1)} = g^{m-(n+1)}$ and we conclude by induction on $n$, $g^m g^{-n} = g^{m-n}$ $\forall n \in \mathbb{N}$.

– (end of ②) –

---

At this point, we've shown $g^m g^k = g^{m+k}$ for $m \geq 0$ and for each $k \in \mathbb{Z}$. It remains to argue $g^m g^k = g^{m+k}$ for the case $m<0$ and $k \in \mathbb{Z}$.

Proof of Lemma $(m<0)$

③ Suppose $m<0$. Let $m=-n$ for $n \in \mathbb{N}$. Consider,

$$g^m g = g^{-n} g = g^{-(n-1)} g^{-1} g = g^{-(n-1)} = g^{-n+1}$$

thus $g^m g^k = g^{m+k}$ for $k=1$. $\beta$ inductively, $g^m g^k = g^{m+k}$. Consider,

$$g^m g^{k+1} = g^m g^k g = g^{m+k} g \quad (*)$$

There are 3 cases,

(i.) $m+k=0$, $g^m g^{k+1} = g^{m+k} g = g = g^{m+k+1}$.

(ii.) $m+k>0$, $g^m g^{k+1} = g^{m+k} g = g^{m+k+1}$

(iii.) $m+k<0$, $g^m g^{k+1} = g^{m+k} g = (g^{-1})^{-m-k-1} g^{-1} g$

$$= (g^{-1})^{-(m+k+1)}$$

$$= g^{m+k+1}$$

Thus $g^m g^{k+1} = g^{m+k+1}$ for $m<0$ and we conclude $g^m g^k = g^{m+k}$ for $m<0$ and $k \in \mathbb{N}$.

//

$$g^m g^{-1} = g^{-n} g^{-1} = g^{-(n+1)} = g^{m-1} \quad (j=1 \text{ step})$$

Suppose inductively $g^m g^{-j} = g^{m-j}$ for $j \in \mathbb{N}$.

Consider, $g^m g^{-(j+1)} = g^{-n} g^{-j} g^{-1} = g^m g^{-j} g^{-1} = g^{m-j} g^{-1}$ by ind. hypo. Notice $m-j = -n-j < 0$ so thankfully there is one case. $g^{m-j} g^{-1} = g^{-n-j-1} = g^{m-(j+1)}$.

Hence $g^m g^{-j} = g^{m-j}$ for all $j \in \mathbb{N}$ in the case $m<0$. -(ends ③)-

In summary, $g^m g^k = g^{m+k} \; \forall m,k \in \mathbb{Z}$. //

P6

$\boxed{\text{Claim: } |g| = |g^{-1}| \text{ for } g \in G}$ group

PROBLEM 6 (#4 pg. 67 Gallian)

① If $|g| = \infty$ then $g^n \neq e \quad \forall n \in \mathbb{N}$.

Suppose $|g^{-1}| < \infty$ then $\exists k \in \mathbb{N}$ for which

$$(g^{-1})^k = e \Rightarrow g^{-k} = e \Rightarrow g^k g^{-k} = g^k e$$

Hence, using Lemma $g^a g^b = g^{a+b}$ with $a = k$, $b = -k$

we obtain $g^{k-k} = g^k \Rightarrow g^k = e \therefore |g| \leq k$

But, $|g| = \infty$ so we find $\rightarrow\!\leftarrow$ and conclude

$|g^{-1}| \not< \infty$ or, as we hoped, $|g^{-1}| = \infty$.

② If $|g| = n$ then $g^n = e$ and $g^j \neq e$

$\forall j = 1, 2, \ldots, n-1$. Observe, by Lemma

$$g^n = e \Rightarrow g^{-n} g^n = g^{-n} e \Rightarrow g^{-n+n} = g^{-n}$$

Hence $(g^{-1})^n = e \Rightarrow |g^{-1}| \leq n$.

Suppose $(g^{-1})^j = e$ for some $j < n$.

then $g^j (g^{-1})^j = g^j e \Rightarrow g^{j-j} = g^j$

Thus, $e = g^j \Rightarrow |g| \leq j$ yet $|g| = n > j$.

To summarize, $|g| \leq j$ and $|g| > j$ a clear $\rightarrow\!\leftarrow$

thus $(g^{-1})^j \neq e$ for $j < n$ and we

conclude $|g^{-1}| = n = |g|$.

Thus, in all cases, $|g| = |g^{-1}|$ for $g \in G$ //

P7 # 45 pg. 70 of Gallian

Suppose $H \leq \mathbb{R}$ with respect to additive group $\mathbb{R}$. Let $K = \{2^a \mid a \in H\}$. Show $K \leq \mathbb{R}^\times$ where $\mathbb{R}^\times = \mathbb{R} - \{0\}$ with multiplication

Observe $0 \in H$ as $H \leq \mathbb{R}$ and $0$ is identity of $\mathbb{R}$. Moreover, $2^0 = 1$ is identity for $\mathbb{R}^\times$ and we find $2^0 = 1 \in K \neq \phi$. Suppose $x, y \in K$ then $\exists a, b \in H$ for which $x = 2^a$ and $y = 2^b$ thus $xy^{-1} = 2^a(2^b)^{-1} = 2^a 2^{-b} = 2^{a-b}$ and $a - b \in H$ as $H \leq \mathbb{R}$ with addition. Thus, $2^{a-b} \in K$ and so we've shown $x, y \in K \Rightarrow xy^{-1} \in K \therefore K \leq \mathbb{R}^\times$ by one-step subgroup test. //

Remark: details matter.

$\boxed{P8}$ #51 of pg 71 Gallian

Let $G = Gl(2, \mathbb{R})$

(a.) Find $C\left(\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\right)$

(b.) Find $C\left(\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\right)$

(c.) Find $Z(G)$

(a.) $C\left(\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\right) = \left\{ A \in G \,/\, A\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} A \right\}$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

$$\left[\begin{array}{c|c} a+b & a \\ \hline c+d & c \end{array}\right] = \left[\begin{array}{c|c} a+c & b+d \\ \hline a & b \end{array}\right]$$

linear algebra, to be careful.

thus $b = c$, $a = c + d$, $c, d \in \mathbb{R}$.

$A = \left[\begin{array}{c|c} c+d & c \\ \hline c & d \end{array}\right] \in G \Rightarrow \det(A) = d(c+d) - c^2 \neq 0$

$$\boxed{C\left(\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\right) = \left\{ \left[\begin{array}{c|c} c+d & c \\ \hline c & d \end{array}\right] \;\middle|\; c, d \in \mathbb{R},\ d^2 - c^2 + cd \neq 0 \right\}}$$

(b.) $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \Rightarrow \left[\begin{array}{c|c} c & d \\ \hline a & b \end{array}\right] = \left[\begin{array}{c|c} b & a \\ \hline d & c \end{array}\right]$

thus $c = b$, $d = a$ hence we deduce,

$$\boxed{C\left(\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\right) = \left\{ \begin{bmatrix} a & b \\ b & a \end{bmatrix} \;\middle|\; a, b \in \mathbb{R},\ a^2 - b^2 \neq 0 \right\}}$$

(c.) $A \in Z(G)$ only if $AB = BA$ for all $B \in Gl(2, \mathbb{R})$ use (a.) & (b.). Set $B = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$ to force $A = \left[\begin{array}{c|c} c+d & c \\ \hline c & d \end{array}\right]$ for $c, d \in \mathbb{R}$ with $d^2 - c^2 + cd \neq 0$. Set $B = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ to force $A = \begin{bmatrix} a & b \\ b & a \end{bmatrix}$ for $a, b \in \mathbb{R}$, $a^2 - b^2 \neq 0$ continued

P8 continued

We have $\underline{A = \begin{bmatrix} a & b \\ b & a \end{bmatrix} = \left[\begin{array}{c|c} c+d & c \\ \hline c & d \end{array}\right]}$ *

for some $a, b, c, d \in \mathbb{R}$ where $a^2 - b^2 \neq 0$

and $d^2 - c^2 + cd \neq 0$. Notice * yields,

$$
\begin{aligned}
a &= c+d \\
b &= c \\
b &= c \\
a &= d
\end{aligned}
$$

Thus, $a = d$ and $a = c+d \Rightarrow \underline{c = 0} \therefore \underline{b = 0}$.

In summary $A = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} = aI$, $a^2 \neq 0$.

To be safe, we should verify other choices of $B$ do not impose further constraints on the form of $A$. Observe

$$AB = aIB = aBI = B(aI) = BA$$

thus, $\boxed{Z(G) = \{ aI \mid a \neq 0 \}}$