Solutions for exercises to Lecture 1

1. $C_n = \langle x \rangle$ with $x^n = e$.
If we take $\zeta = \exp(2\pi i/n) \in \mathbb{C}^*$ then all n^{th} roots of 1 have the form ζ^i $0 \le i \le n-1$. Thus the mapping

$$x^i \longmapsto \zeta^i$$

sets up an isomorphism between C_n and μ_n.
It's not natural since we had to choose ζ: cyclic group C_n comes with a generator, μ_n not. In fact the most obvious map is ~~a bijection~~

$$C_n \longrightarrow \mathrm{Maps}(\mu_n, \mathbb{C})$$
$$x^i \longmapsto (\omega \longmapsto \omega^i) \quad \text{for all } \omega \in \mu_n.$$

That doesn't involve any choices.

2. Brute force does it, but that's not going to help for $GL(n, \mathbb{F}_q)$.
Here's a better way:
$A \in \mathrm{Mat}(n, \mathbb{F}_q)$ is invertible $\iff$ the columns of A form a basis of $\mathbb{F}_q^n$.
So $|GL_n(\mathbb{F}_q)| = \#$ bases of $\mathbb{F}_q^n$. This is easy to calculate:

- for the first ~~column~~ vector we can choose any non-zero element, so there are $|\mathbb{F}_q^n \setminus \{0\}| = q^n - 1$ choices
- for the second vector we can choose any vector that is not a linear combination (ie scalar multiple) of the first, so there are $|\mathbb{F}_q^n \setminus \mathbb{F}_q| = q^n - q$ choices
- for the third vector we can choose any vector that is not a linear combination of the first two, so there are $|\mathbb{F}_q^n \setminus \mathbb{F}_q^2| = q^n - q^2$ choices

... etc.

So we end up with ~~q~~

$$|GL(n,\mathbb{F}_q)| = (q^n-1)(q^n-q)(q^n-q^2)\cdots(q^n-q^{n-1})$$

When $n=2$ we get $(q^2-1)(q^2-q)$, just as we said in lectures. To get $SL(n,\mathbb{F}_q)$ we must make sure that the determinant is 1. To do this note that there is an action of $\mathbb{F}_q^\times$ on $GL(n,\mathbb{F}_q)$ given by ~~sending~~ $\lambda \bullet A = \begin{pmatrix}\lambda & \cdots & 0\\ \vdots & \ddots & \\ 0 & & 1\end{pmatrix} A$ $\lambda \in \mathbb{F}_q, A \in GL$.

Then $\det(\lambda \bullet A) = \lambda \det A$ and so in each $\mathbb{F}_q^\times$-orbit on $GL(n,\mathbb{F}_q)$ there is exactly one matrix whose determinant is 1. So

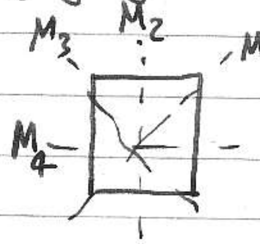
$$|SL(n,\mathbb{F}_q)| = \#\,\mathbb{F}_q^\times\text{-orbits in } GL(n,\mathbb{F}_q)$$

$$= \frac{|GL(n,\mathbb{F}_q)|}{|\mathbb{F}_q^\times|} = (q^{n-1}+q^{n-2}+\cdots+q+1)(q^n-q)\cdots(q^n-q^{n-1})$$

If $n=2$ we get $|SL(2,\mathbb{F}_q)| = (q+1)(q^2-q)$.

3. C_n is abelian, so Each element is a conjugacy class on its own.

4. $D_4 = \{e, r, r^2, r^3, M_1, M_2, M_3, M_4\}$



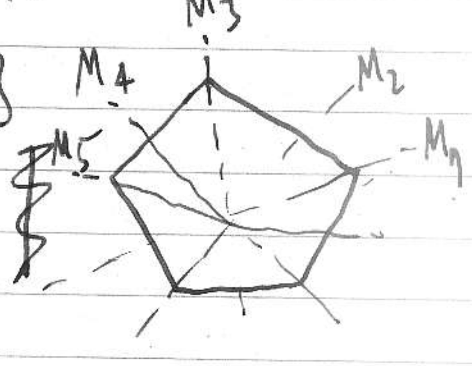
r - rotation by $\pi/2$ anticlockwise

M_i - reflection in axis shown

ccls are

$\{e\}, \{r^2\}, \{r, r^3\}, \{M_1, M_3\}, \{M_2, M_4\}$

$D_5 = \{e, r, r^2, r^3, r^4, M_1, M_2, M_3, M_4, M_5\}$



ccls are

$\{e\}\ \{r, r^4\}\ \{r^2, r^3\}, \{M_1, \ldots, M_5\}$

In general there are two types of behaviour depending on whether n is even or odd.

<u>n odd</u>: $\{e\}$, $\{r^i, r^{n-i}\}_{i\neq 0}$ (this is obvious: $C_{D_n}(r^i) = \langle r\rangle$ $\therefore$ the ccl of r^i has 2 elements)

$\{M_1, \dots, M_n\}$ – all form 1 ccl: to get from M_i to M_{i+2} conjugate by r, and then observe $i \mapsto i+2 \mapsto i+4 \mapsto \dots$ covers all reflections since n is odd)

<u>n even</u>: same arguments as above give

$\{e\}$, $\{r^{n/2}\}$, $\{r^i, r^{n-i}\}_{i\neq 0, n/2}$

$\{M_1, M_3, \dots, M_{n-1}\}$, $\{M_2, M_4, \dots, M_n\}$.

5. $|GL_2(\mathbb{F}_2)| = 6$ by (2), and $GL_2(\mathbb{F}_2)$ is not abelian so it must be that $GL(2,\mathbb{F}_2) \cong S_3$ (so we know to expect 3 ccls as S_3 has 3; (by the way, $GL(2,\mathbb{F}_2)$ acts on $\mathbb{F}_2^2$ by matrix mult^n and in fact on $\mathbb{F}_2^2 \setminus \{0\}$, a ~~space~~ set with 3 elements – it's this that realises $GL(2,\mathbb{F}_2)$ as permutations on 3 elements).)

$$\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix}\right\}, \left\{\begin{pmatrix}1&1\\0&1\end{pmatrix}, \begin{pmatrix}1&0\\1&1\end{pmatrix}, \begin{pmatrix}0&1\\1&0\end{pmatrix}\right\}, \left\{\begin{pmatrix}1&1\\1&0\end{pmatrix}, \begin{pmatrix}0&1\\1&1\end{pmatrix}\right\}.$$

6. Conjugacy classes are given by cycle type in S_n. In the specific examples of $n=4$ and $n=5$ we get representatives:

$n=4$: e; (12); (123); $(12)(34)$; (1234)

$n=5$: e; (12); (123); $(12)(34)$; (1234); $(12)(345)$; (12345)

7. $N = \{e, (12)(34), (13)(24), (14)(23)\}$. $\left|S_4/N\right| = 24/4 = 6$.

$\therefore$ it's either C_6 or S_3. It's obviously not C_6 (since it's not abelian, since S_4 has no elements of order 6, ...)

$$\therefore \; S_4/N \cong S_3.$$

8\. There are two left cosets H, gH (for some $g \notin H$)

" " " right " H, Hg (" " ")

$\therefore$ $Hg = gH$ and so left cosets = right cosets.

$\therefore$ $H \trianglelefteq G$.

9\. This is a brute for calculation:

$A = (a_{ij})$ $B = (b_{ij})$

$$Tr(AB) = \sum_{k=1}^{n} (AB)_{kk} = \sum_{k=1}^{n} \left(\sum_{l=1}^{n} a_{kl} b_{lk} \right)$$

$$= \sum_{l=1}^{n} \left(\sum_{k=1}^{n} b_{lk} a_{kl} \right)$$

$$= \sum_{l=1}^{n} (BA)_{ll} = Tr(BA).$$

If A, B are conjugate, then $A = XBX^{-1}$ for some $X \in GL(n, F)$ and so

$$Tr(A) = Tr(XBX^{-1}) \overset{\text{by above.}}{=} Tr(X^{-1}XB) = Tr(B)$$

10\. take $v_1, v_2 \in V$ and $\lambda, \mu \in F$. Then $v_1 = u_1 + w_1$, $v_2 = u_2 + w_2$ with $u_i \in U$, $w_i \in W$ $(i = 1, 2)$ and then

$$\lambda v_1 + \mu v_2 = \underset{\overset{\Uparrow}{U}}{(\lambda u_1 + \mu u_2)} + \underset{\overset{\Uparrow}{W}}{(\lambda v_1 + \mu v_2)}$$

Now we calculate

$$\pi_U(\lambda v_1 + \mu v_2) = \lambda u_1 + \mu u_2$$

whilst

$$\lambda \pi_U(v_1) + \mu \pi_U(v_2) = \lambda u_1 + \mu u_2$$

$\therefore$ π_U is linear i.e $\pi_U \in \mathrm{End}(V)$.

Clearly $\mathrm{im}\,\pi_U \subseteq U$ since $\pi_U(v) \in U$ $\forall v \in V$. On the other hand given $u \in U$ we have that $u \in V$ since $U \leq V$ and so $\pi_U(u) = u$. Therefore $U \subseteq \mathrm{im}\,\pi_U$. Hence $\mathrm{im}\,\pi_U = U$.

Suppose ~~...~~ $v \in \ker \pi_U$. Writing $v = u + w$ we see that $0 = \pi_U(v) = u$ $\therefore$ $v = w$ and we deduce that $W \supseteq \ker \pi_U$.

Obviously if $v \in W \subseteq V$ then $\pi_U(v) = 0$ and so we get $\ker \pi_U \supseteq W$. Hence $\ker \pi_U = W$.

Let $v \in V$ with $v = u + w$

$$\pi_U^2(v) = \pi_U(\pi_U(v)) = \pi_U(u) = u = \pi_U(v) \quad \therefore \pi_U^2 = \pi_U$$