Final Exam 2013.5.10 MAT 4233 Modern Abstract Algebra

1. $\det \begin{bmatrix} 7 & 5 \\ 4 & 5 \end{bmatrix} = 35 - 20 = 15$. Since 17 is a prime, $\mathbb{Z}_{17}$ is a field, so since $\det \neq 0$, the matrix is invertible

$15 = -2$, $(-2)^4 = 16 = -1$, $(-2)^8 = 1$, $(-2)^{-1} = (-2)^7 =$

$= (-2)^4(-2)^3 = 8$. check: $15 \cdot 8 = 120 = 17 \cdot 7 + 1$

$$\begin{bmatrix} 7 & 5 \\ 4 & 5 \end{bmatrix}^{-1} = 8 \begin{bmatrix} 5 & -5 \\ -4 & 7 \end{bmatrix} = \begin{bmatrix} 40 & -40 \\ -32 & 56 \end{bmatrix} \equiv \begin{bmatrix} 6 & 11 \\ 2 & 5 \end{bmatrix} \bmod 17$$

2. $D_4 = \{ R_0, R_{90}, R_{180}, R_{270}, H, V, D, D' \}$

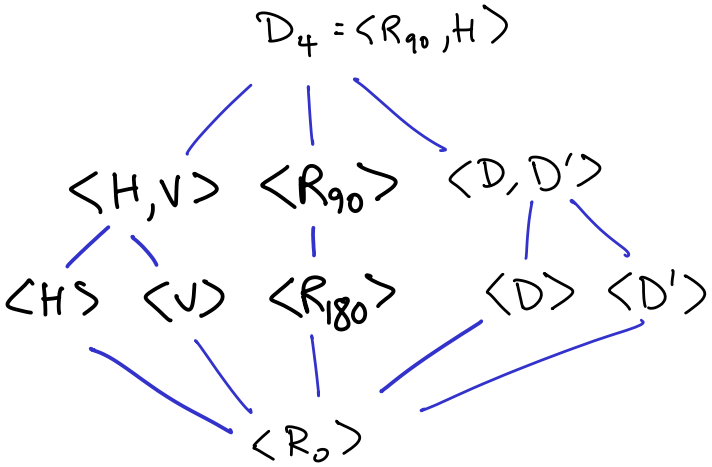
$\langle R_{90} \rangle = \langle R_{270} \rangle = \{R_0, R_{90}, R_{180}, R_{270}\}$

$\langle R_{180} \rangle = \{ R_0, R_{180} \}$

Each flip generates a subgroup of order 2, e.g. $\langle H \rangle = \{R_0, H\}$

$\langle H, V \rangle = \{ R_0, R_{180}, H, V \}$

$\langle D, D' \rangle = \{ R_0, R_{180}, D, D' \}$



$\langle H, V \rangle$ has index 2, so has only 2 cosets, itself and $\{R_{90}, R_{270}, D, D'\}$

3. Given a cyclic group $\langle a \rangle$ define $\phi: \mathbb{Z} \to \langle a \rangle$ by $\phi(k) = a^k$. ϕ is a hom: $\phi(k+\ell) = a^{k+\ell} = a^k \cdot a^\ell = \phi(k)\cdot\phi(\ell)$

ϕ is clearly onto, so if ϕ is injective, ϕ is an iso, so $\langle a \rangle \cong \mathbb{Z}$ and $|a| = \infty$.

If $|a| = n$, $\ker \phi = n\mathbb{Z}$.

[If $\phi(k) = a^k = e$, n divides k, so $k \in n\mathbb{Z}$
Conversely, if $k \in n\mathbb{Z}$, $\exists j \in \mathbb{Z}$ $k = nj$.
Then $\phi(k) = a^k = a^{nj} = (a^n)^j = e^j = e$, so $k \in \ker\phi$.]

By the first isomorphism theorem $\langle a \rangle \cong \frac{\mathbb{Z}}{n\mathbb{Z}_n} = \mathbb{Z}_n$.

4. $H = \{[0,0], [2,0], [0,2], [2,2]\}$

$K = \{[0,0], [2,3], [0,2], [2,1]\}$

$[1,0] + H = \{[1,0], [3,0], [1,2], [3,2]\}$

$[0,1] + H = \{[0,1], [2,1], [0,3], [2,3]\}$

$[1,1] + H = \{[1,1], [3,1], [1,3], [3,3]\}$

$[1,0] + K = \{[1,0], [3,3], [1,2], [3,1]\}$

$[0,1] + K = \{[0,1], [2,0], [0,3], [2,2]\}$

$[1,1] + K = \{[1,1], [3,0], [1,3], [3,2]\}$

$|G/H| = |G/K| = 4$. By the classification theorem for finite abelian groups, the isomorphism class choices are $\mathbb{Z}_4, \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

$2\cdot[1,0] = [2,0] \in H$ $\quad \therefore G/H \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$

$2\cdot[0,1] = [0,2] \in H$

$2\cdot[1,1] = [2,2] \in H$

$[1,0] + K$ has order 4 in G/K, so $G/K \cong \mathbb{Z}_4$

5. $e \in H$, $e \in K$, so $e = e \cdot e \in HK$ and $e \in KH$

If $h, h' \in H$, $k\, k' \in K$, then

$hkh'k' = \underbrace{hh'}_{\in H}\ \underbrace{h'^{-1} k\, h'\, k'}_{\in K \text{ since } K \trianglelefteq G} \in HK$

$khk'h' = \underbrace{k\underbrace{hk'h^{-1}}_{\in K \text{ since } K \trianglelefteq G}}_{\in K}\ \underbrace{h\, h'}_{\in H} \in KH.$

Closure under inverses is automatic since G is finite.

6. Since $k \geq 1$, $p^k > 1$, so let $x \in G$, $x \neq e$.

Then $|x| \neq 1$ and $|x| \mid p^k$ (Lagrange), so $|x| = p^j$ for some $j \geq 1$. Thus $x^{p^j} = e$, but

$e = x^{p^j} = x^{p^{j-1} p} = (x^{p^{j-1}})^p$ and the power is minimal, so $|x^{p^{j-1}}| = p$ ☺

7. If n is not prime, $n = mk$ for some $m, k \in \mathbb{N}$ where $m \neq 1$, $m \neq n$. Then $\langle n \rangle \subsetneq \langle m \rangle \subsetneq \mathbb{Z}$, so $\langle n \rangle$ is not maximal.

If n is prime, let I be an ideal of $\mathbb{Z}$ with $\langle n \rangle \subsetneq I$. Let $k \in \mathbb{Z} \setminus \langle n \rangle$. Then by Bézout

$\exists\, s, t \in \mathbb{Z} \quad 1 = \underbrace{sk}_{\in I} + \underbrace{tn}_{\in \langle n \rangle \subseteq I} \in I$, so $I = R$, so $\langle n \rangle$ is maximal.

Alt: n is prime $\Leftrightarrow \mathbb{Z}_n = \frac{\mathbb{Z}}{\langle n \rangle}$ is a field $\Leftrightarrow \langle n \rangle$ is maximal. ☺

8. Let $M = R \setminus U(R)$ and suppose A is an ideal of R with $M \subsetneq A$. Then A contains a unit, so $A = R$. $\therefore M$ is maximal. If M' is another maximal ideal, $M' \nsubseteq M$, so M' contains a unit, so $M' = R$ ☹. $\therefore M$ is the unique maximal ideal. ☺

Conversely, suppose M is the unique max. ideal. Let $u \in U(R)$. If $u \in M$, $M = R$ ☹, so $U(R) \subseteq R \setminus M$. Conversely, if $x \notin U(R)$, for $\forall\, x' \in R$ $x \cdot x' \neq 1$, so $\langle x \rangle$ is a proper ideal ($\neq R$), so $\langle x \rangle \subseteq$ some maximal ideal, which by uniqueness is M, so $x \in M$. ☺