16.1

Let p be prime, $n \in \mathbb{N}$ such that $p \le n \le p^2 - 1$. The p-Sylow subgroup of S_n will have order p^k for some $k \in \mathbb{Z}$. Moreover, $p^k \mid |S_n| = n!$. Note $\exists$ an i $(1 \le i < p-1)$ such that $p^i \parallel n!$. $(ip \le n < (i+1)p)$. Then if P a p-Sylow subgroup of S_n, $|P| = p^i$, $P \cong \mathbb{Z}/p^i$ or $\mathbb{Z}/p^2 \times \mathbb{Z}/p^{i-2}$. In general, $P \cong \prod_i \mathbb{Z}/p$.

16.2

Let n be prime, $n = p(p-1)$. By 14.3 and Sylow (2), if P_g a p-Sylow subgroup, $P = \langle g\,(p+j \;\; p+j+1 \; \cdots \; p+j+i)\,g^{-1} \rangle$ where $j \in \mathbb{Z}$, $g \in S_n$, i from 16.1. So there are i disjoint p-cycles. Thus the number of distinct sets of i disjoint p-cycles is equal to the number of p-Sylow subgroups since any set of i disjoint p-cycles is the generator of a p-Sylow subgroup. Thus # of p-Sylow subgroups

$$= \frac{(p(p-1))!}{(p-1)!\; p^{p-1}}$$

dividing $(p-1)!$ because cycle order doesn't matter and we have p different representations in each cycle.

16.3

Let G be a group w/ order 42. Then $|G| = 7 \cdot 3 \cdot 2$.

By Sylow (1), $\exists\, P_7 \le G$ with $|P_7| = 7$. Furthermore, by Sylow (3), $n_7 \mid 3 \cdot 2$ so $n_7 \in \{1, 3, 2, 6\}$. By Lagrange, $[G : P_7] = \{1, 2, 3, 7\}$.

Also, $n_7 \equiv 1 \bmod 7$ so $n_7 \in \{1, 8, 15, 22, 29, 36\}$. Thus $n_7 = 1$.

Hence $N_G(P_7) = G$ so $P_7 \trianglelefteq G$. ∎

16.4

Let $H, K \le G$, $HK \le G$. We will show for $h \in H$, $k \in K$, hk is duplicated <u>exactly</u> $|H \cap K|$ times (including hk itself). Suppose $h_1 \in H \cap K$. Then $h_1^{-1} \in K$ so

$$hk = \underbrace{(h\,h_1)}_{\in H}\underbrace{(h_1^{-1}\,k)}_{\in K} \qquad (*)$$

Thus hk is duplicated <u>at least</u> $|H \cap K|$ times.

However, if $hk = h'k'$ for some $h' \in H$, $k \in K'$, then $(h^{-1})h' = k(k')^{-1} =: g \in H \cap K$ so $h' = hg$ and $k' = g^{-1}k$, so $h'k'$ was accounted for in $(*)$. ∎

17.2

Suppose a group G has order 99. Then $|G| = 3^2 \cdot 11$. By Sylow (1), $\exists$ an 11-Sylow subgroup $P_{11} \leq G$. By Sylow (3), $n_{11} \equiv 1 \bmod 11$ and $n_{11} \in \{1, 3, 9\}$. So $n_{11} = 1$. Thus $|N_G(P_{11})| = \frac{|G|}{n_{11}} = |G|$ so $N_G(P_{11}) = G$. $\square$

17.1 $\updownarrow$ Sorry about being out of order.

Notice

2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

- prime order: 2, 3, 5, 7, 11, 13, 17, 19
- normal by Ex 17.6: $2\cdot 3$, $2 \cdot 5$, $2\cdot 7$, $3 \cdot 5$
- $n_1 = 1$ by Sylow (3): $2^2 \cdot 1$, $2^3 \cdot 1$, $3^2 \cdot 1$, $4^2 \cdot 1$

$|G|$: $3^2 \cdot 2$, $2^2 \cdot 5$

- 18 has a 3-Sylow group of order 9, $n_3 \equiv 1 \bmod 3$ but $n_3 \in \{1, 2\}$ so $n_3 = 1$. Similar for $|G| = 20$, which has $P_5 \trianglelefteq G$.

$2^2 \cdot 3$

If $|G| = 12$, $\exists P_3 \leq G$ with order 3. By Sylow (3), $n_3 \equiv 1 \bmod 3$ and $n_3 \in \{1, 2, 4\}$. So $n_3 \in \{1, 4\}$. If $n_3 = 1$, we're done. Suppose $n_3 = 4$. Then there are $4 \cdot 2 = 8$ distinct order 3 elements. $\Rightarrow n_3 \in \{1, 4, \dots\}$

Similarly, $\exists P_2 \leq G$ with order 4. By Sylow (3), $n_2 \equiv 1 \bmod 2$, $n_2 \mid 3$. Notice that $12 - 8 = 4$ elements of G have order not equal to 3. Since $|P_2| = 4$ $\forall P_2 \leq G$, P_2 must be unique! Thus $n_2 = 1$. $\square$

18.1

Let k be a field. Consider the following:

a) Let $A,B \in GL_n(k)$, $AB=BA$. Then if $Bv=\lambda v$ for some $v\in k^n$, $\lambda \in k$, $BAv = ABv = A\lambda v = \lambda A v$. Thus A preserves the eigenspace of B.

b) Let $A \in GL_n(k)$ and $A\vec{v} = \lambda_v \vec{v}$ $\forall \vec{v}\in k^n$, then $A\vec{e}_i = \lambda_i \vec{e}_i$ for $1\le i\le n$. Let $\vec{x} = \sum_1^n \vec{e}_i$. Then $A\vec{x} = \lambda'$ for some $\lambda' \in k$. Then $\lambda'(\vec{e}_1 + \dots + \vec{e}_n) = A\vec{x} = \sum_1^n A\vec{e}_i = \lambda_1 \vec{e}_1 + \dots + \lambda_n \vec{e}_n \Rightarrow (\lambda'-\lambda_1)\vec{e}_1 + \dots + (\lambda'-\lambda_n)\vec{e}_n = \vec{0}$. But $\{\vec{e}_i\}$ linearly independent so $\lambda_i = \lambda'$ $\forall i$, so $A\vec{v} = \lambda'\vec{v}$ $\forall \vec{v}\in k^n$.

Suppose $A \in Z(GL_n(k))$.

Let $\vec{v}_1 \overset{\neq}{\in} k^n$ ($\vec{v}_1 \neq 0$). We can extend $\vec{v}_1$ to an ordered basis (Gram-Schmidt) $\mathcal{B} = \{\vec{v}_1, \dots, \vec{v}_n\}$. Next, let B be the linear map which defined by $\begin{cases} \vec{v}_1 \mapsto \vec{v}_1 \\ v_i \mapsto \vec{v}_i + \vec{v}_{i-1} & i \neq 1 \end{cases}$. Note that $B = \begin{bmatrix} 1 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 1 & & \ddots & 0 \\ \vdots & 0 & 1 & 1 & \ddots & 0 \\ \vdots & \vdots & 0 & \ddots & \ddots & 1 \\ & & & 0 & 0 & 1 \end{bmatrix}_{\mathcal{B}}$. Then if $\vec{x} = (x_1, \dots, x_n)_{\mathcal{B}}$,

$$Bx = \begin{bmatrix} x_1 + x_2 \\ x_2 + x_3 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} + \begin{bmatrix} x_2 \\ \vdots \\ x_n \\ 0 \end{bmatrix} \Rightarrow \vec{x} \in \operatorname{span}\{\vec{v}_1\} \text{ iff } \vec{x} \text{ an eigenvector (w/ eigenvalue 1).}$$

By assumption, $AB=BA$. By (a), $A: \vec{v}_1 \mapsto \lambda \vec{v}_1$ for some $\lambda \in k$. Since $\vec{v}_1$ arbitrary, every $\vec{v}\in k^n$ an eigenvector of A, and by (b), $A\vec{v} = \lambda\vec{v}$ for some $\lambda \in k^\times$ and for all $\vec{v}\in k^n$. $\Rightarrow A = \lambda I_n$. ∎

18.2

Let p be prime, note $SL_2(F_p) = \ker(\det_{GL_2(k)\to k^\times}) = \{M \in GL_2(k) : \det M = 1$

Take $S = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $T = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$, and notice $S,T \in SL_2(F_p)$. Suppose $M \in Z(SL_2(F_p))$. Then

$MS = SM \Rightarrow \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} \Rightarrow \begin{bmatrix} a & a+b \\ c & c+d \end{bmatrix} = \begin{bmatrix} a+c & b+d \\ c & d \end{bmatrix} \Rightarrow \begin{matrix} c=0 \\ a\equiv d \bmod p \end{matrix}$

$MT = TM \Rightarrow$ ... similar computation ... $\Rightarrow b = 0$

So $M = \lambda I_2$ for some $\lambda \in \mathbb{Z}/p$. But $\det M = 1$, so we must restrict $\lambda^2 \equiv 1 \bmod p$. Thus

$$Z(SL_2(F_p)) = \begin{cases} I_2 & \text{if } p=2 \\ \pm I_2 & \text{otherwise} \end{cases}.$$

18.3

Note that $SL_2(F_p)$ is the kernel of the surjective group homomorphism $\det: GL_n(k) \to k^\times$. Then

$$|SL_2(F_p)| \cdot |p^\times| = |GL_2(F_p)| \Rightarrow |SL_2(F_p)| = \frac{p(p-1)^2(p+1)}{p-1} = p(p-1)(p+1)$$

(Ex 18.5)

By Lagrange,

$$|PGL_2(F_p)| = \left|\frac{SL_2(F_p)}{Z(SL_2(F_p))}\right| = \frac{|SL_2(F_p)|}{|Z(SL_2(F_p))|} = \begin{cases} \dfrac{p(p-1)(p+1)}{2} & \text{if } p>2 \\ \\ p(p-1)(p+1) & \text{if } p=2. \end{cases}$$

18.4 Find the number of p-Sylow subgroups of $SL_2(F_p)$.

Note that $|SL_2(F_p)| = p(p-1)(p+1)$ (by 18.3). Then, if $p=2$, $|SL_2(F_2)| = 2\cdot 3$, so $SL_2(F_2)$ has a normal 3-Sylow subgroup by Cauchy.

Suppose otherwise that $p>2$. Notice $\tilde{x} := \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ has order p. Thus $\langle \tilde{x} \rangle$ is a p-Sylow subgroup of $SL_2(F_p)$. From Sylow (3), $n_p \mid (p-1)(p+1)$ and $n_p \equiv 1 \bmod p$ so $n_p = 1$ or $p+1$. Computing the normalizer $N(\langle \tilde{x} \rangle) = \{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(F_p) \mid \begin{bmatrix} a & b \\ c & d \end{bmatrix} g = g \begin{bmatrix} a & b \\ c & d \end{bmatrix} \}$, note:

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

Thus

$$N(\langle \tilde{x} \rangle) = \{ u \in SL_2(F_p) \mid u \text{ upper triangular} \}$$

and

$$p\cdot(p-1) = |N(\langle \tilde{x} \rangle)|$$

since there are $p(p-1)$ upper triangular matrices in $SL_2(F_p)$

So

$$n_p = \frac{|SL_2(F_p)|}{|N(\langle \tilde{x} \rangle)|} = \frac{p(p-1)(p+1)}{p(p-1)} = \underline{p+1}.$$

18.5 Find the number of p-Sylow subgroups of $PGL_2(F_p)$.

If $p=2$, $Z(SL_2(F_p)) = \{I_2\}$ so $PGL_2(F_2) = SL_2(F_2)$. Thus $\underline{n_p = p+1}$ by 18.4.

Suppose $p>2$. Then $Z(SL_2(F_p)) = \{\pm I_2\}$ (=: Z for sake of notation)

Consider the quotient map $\varphi : SL_2(F_p) \to PGL_2(F_p)$, defined by $\varphi(M) = \{M, -M\}$, $M \in SL_2(F_p)$.

Then, taking $\langle \tilde{x} \rangle$ to be the p-Sylow subgroup of $SL_2(F_p)$ in 18.4,

$$\varphi(\langle \tilde{x} \rangle) = \langle Z\tilde{x} \rangle$$

is a p-Sylow subgroup of $PGL_2(F_p)$. From a nearly identical calculation as in 18.4,

$$|N(\langle Z\tilde{x} \rangle)| = \frac{p(p-1)}{2}$$

since $Zg = Z(-g)$ for $g \in SL_2(F_p)$. Thus,

$$n_p = \frac{|PGL_2(F_p)|}{|N(\langle Z\tilde{x} \rangle)|} = \frac{p(p-1)(p+1)}{2} \cdot \frac{2}{p(p-1)} = \underline{p+1}.$$