Lecture 4

As advertised, we finish chapter 2 this week and next week start chapter 3, which is the hardest chapter on groups we will do.

2.3

Cyclic groups are among the most basic building blocks of groups. In particular, for $x \in G$, the subgroup $< x >$ generated by $x = \{x^n | n \in \mathbb{Z}\}$ is cyclic by definition. The subgroup is finite if and only if $|x|$ is finite because $| < x > | = |x|$.

The book does a thorough job of explaining cyclic groups, so I have nothing to add to the discusion. However, I do want you to see the proof of a hard problem.

2.3.21: Let p be an odd prime and let n be a positive integer. Using the Binomial Theorem, we see $(1+p)^{p^{n-1}} = 1 + \binom{p^{n-1}}{1}p + ... + \binom{p^{n-1}}{i}p^i + ... + p^{p^{n-1}}$. For $i \geq n$ the power of p is greater than or equal to n, so we need not worry about the binomial coefficient. What we need is a lemma:

Lemma: $\binom{p^s}{i}$ is divisible by p^{s-i+1} for $i = i, 2, ..., s-1$.

Proof: By symmetry of the binomial coefficient, we may assume that $i \leq s - i$. If $i = 1$, $\binom{p^s}{1} = p^s = p^{s-1+1}$. Assume $\binom{p^s}{i-j}$ is divisible by $p^{s-i+j+1}$ for $j = 1, 2, ..., i-1$. Note that $\binom{p^s}{i} = p^s!/(i!(p^s - i)!) = p^{s-i}p^i(p^s-1)(p^s - 2)\dots(p^s - i + 1)/i!$. $i! = p^t m$ where $(p, m) = 1$. Since $\binom{p^s}{i}$ is an integer and p is a prime, we need only show that there are enough factors of p in $p^i(p^s-1)(p^s-2)...(p^s-i+1)$. We proceed by induction on i. If $i = 1$, then $1! = 1$ divides every integer. Assume that j divides $p^j(p^s-1)(p^s-2)...(p^s-j+1)$ for $j = 1, 2, ..., i-1$. If $(i, p) = 1$, then the number of factors of p in $i!$ equals the number of factors of p in $(i-1)$, which has at most as many factors of p as in $p^{i-1}(p^s-1)(p^s-2)...(p^s-i)$ which equals the number of factors of p in $p^{i-1}(p^s-1)(p^s-2)...(p^s-i+1)$ since p does not divide i. Thus $i!$ divides $p^i(p^s-1)(p^s-2)...(p^s-i+1)$.

If $(i, p) \neq 1$, $i = p^t m$, where $(p, m) = 1$. Again, we need only show that there are enough factors of p. We know that $i-1$ divides $p^{i-1}(p^s-1)(p^s-2)...(p^s-i)$.

Since p is odd, p does not divide $i-1,\ i-2,\ ...\ i-p+1$. Thus, the number of factors of p in $(i-1)!$ is the same as the number of factors of p in $(i-j)!,\ j=2,...,p-1$ and is t less than the number of factors of p in $i!$. But by induction $(i-p+2)!$ divides $p^{i-p+1}(p^s-1)(p^s-2)...(p^s-i+p)$, which has $i-p+1+a+t+1=i-p+a+2$ factors of p where a is the number of factors of p in $(p^s-1)(p^s-2)...(p^s-i+1)$. Furthermore, $p^i(p^s-1)(p^s-2)...(p^2-i+1)$ has $i+a$ factors of p, so has $p-2$ more. So we have gained $p-2$ factors of p for $m=1,2,...,p-1$ or $(p-1)(p-2)=p^2-3p+2$ total. Since $p\geq 3,(p-1)(p-2)\geq 2$, and we have enough more. This proves the lemma.

For the first part of the problem, $s=n-1$, so for $i\geq 1$, $\binom{p^{n-1}}{i}p^i = p^{n-1+i+1+b}=p^{n+b}\equiv 0 \mod p^n$. So $(1+p)^{p^{n-1}}\equiv 1 \mod p^n$.

For the second part, $s=n-2$, so $(1+p)^{p^{n-2}}=1+p^{p^{n-1}}+$ higher order terms in p. Thus $(1+p)^{n-2}\equiv 1+p^{n-1}\not\equiv 1 \mod p^n$.

Similarly $(1+p)^{p^i}=1+p^{p^i}+...\not\equiv 1 \mod p^n$. Therefore, the order of $1+p$ is $p^{n-1}\in(\mathbb{Z}/p^n\mathbb{Z})^\times$.

2.4

I can't think of anything to add to the theory the book presents as it is basically one definition and an equivalent statement of that definition. But using the definition or its equivalent can be daunting. Thus I'm simply going to work some more examples in hopes of making the idea clearer.

2.4.5: Prove that S_3 is generated by any two elements of order 2.

Proof: Let $(ij),\ (jk)$ be any two elements of S_3 of order 2. Then $(ij)(jk)=(ijk),\ (jk)(ij)=(ikj),\ (ijk)(ij)=(ik)$. Thus $<(ij),\ (jk)>=S_3$.

2.4.10: Prove that the subgroup A of $SL_2(\mathbb{F}_3)$ generated by $\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}$ and $\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$ is isomorphic to Q_8.

Proof: $a^4=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}^4=\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}^2=I$. Also, $b^4=\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}^4=$

$\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}^2 = I$ since $2^2 = 1 \in \mathbb{F}_3$. Thus $|a| = |b| = 4$. Note that $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}$. Thus, $ab = -ba$. Since Q_8 has generators $i,\ j$ with relations $i^4 = j^4 = 1$ and $ij = -ji$, there is a homomorphism $\phi : Q_8 \to A$. Since $|ab| = 4$ by computation, $|A| = 8$. Since ϕ takes generators to generators, ϕ is onto. Since $|A| = |Q_8|,\ \phi$ is an isomorphism.

2.4.13: Prove that the multiplicative group of positive rational numbers $\mathbb{Q}^\times$ is generated by $A = \{1/p | p \text{ is a prime}\}$.

Proof: By the fundamental theorem of arithmetic, every integer q can be written uniquely as $p_1^{n_1}...p_b^{n_b}$ where $p_1 < p_2 < \cdots < p_b$ are primes. Therefore, $1/q$ is in the subgroup generated by A. Since $< A >$ is a group, it is closed under inverses, whence $a \in < A >$ for every positive integer a. Lastly, $< A >$ is closed under multiplication, so $a/q \in < A > \quad \forall a, q \in \mathbb{Z}^\times$. Therefore, $< A > = \mathbb{Q}^\times$.

2.5

Recall that the normalizer of a subgroup H in G, $N_G(H)$, contains H, so we need only check all the subgroups of G containing H to see which is the normalizer. Note that $N_G(G) = G$ as G is the biggest subgroup of G. Also, $N_G(1) = G$ since every element commutes with 1.

Similarly, $C_G(H)$ is a subgroup. If H is abelian, $H \subseteq C_G(H)$. If H is not abelian, then $H \not\subseteq C_G(H)$, but $Z(H) \subseteq C_G(H)$. The lattice will tell us which subgroups are possible.

Again, I think the best thing I can do to be helpful is to work some problems.

2.5.6c: Use the given lattice to find the centralizers of each element of S_3. Since $< (1\ 2\ 3) > = < (1\ 3\ 2 >$ is commutative and S_3 is not, $C_G((1\ 2\ 3)) = C_G((1\ 3\ 2)) = < (1\ 2\ 3) >$. Since $(i\ j)$ commutes only with itself, $C_G((i\ j)) = < (i\ j) >$.

2.5.8a: Compute the normalizer of each subgroup of S_3. From the lattice diagram on the top of page 69, we see that there are four proper, non-trivial subgroups for which to compute the normalizer.

$H =< (1\ 2\ 3) >$: The only possible normalizers are H and G. Since $(1\ 2)(1\ 2\ 3)(1\ 2) = (1\ 3\ 2)$ and $S_3 =< (1\ 2),\ (1\ 2\ 3) >,\ N_G(H) = G$.

$H =< (1\ 2) >$: Again the only choices are H and G. Since $(1\ 3)(1\ 2)(1\ 3) = (2\ 3) \notin H,\ N_G(H) = H$.

Similar computations show that $N_G(< (1\ 3) >) =< (1\ 3) >$ and $N_G(< (2\ 3) >) =< (2\ 3) >$.