Math 101 Fall 2013
Homework #6
Due Wednesday October 30, 2013

1. Prove Cauchy's Theorem: If p is a prime dividing $|G|$, then G contains an element x of order p. (Since $\langle x\rangle$ is a subgroup of G of order p, we also obtain a *partial* converse to LaGrange's Theorem.)

ANS: Suppose that $p \mid |G|$. Then G has a nontrivial p-Sylow subgroup P. Since P has order p^α for $\alpha \geq 1$, any nontrivial element $y \in P$ has order p^j for $1 \leq j \leq \alpha$. If $j = 1$, then we're done. If not, $x = y^{p^{j-1}}$ will do: clearly $x^p = (y^{p^{j-1}})^p = y^{p^j} = 1$. On the other hand, if $x^i = 1$, then $y^{ip^{j-1}} = 1$ and $p^j \mid ip^{j-1}$. Thus $p \mid i$. In short, $|x| = p$ and we're done.

2. Let H and K be finite subgroups of G.

(a) Prove that
$$|HK| = \frac{|H||K|}{|H \cap K|}.$$
(Suggestion: show that the number of distinct left K cosets in HK is equal to the index $H \cap K$ in H.)

(b) Show that if $H \subset N_G(K)$, then HK is a subgroup of G.

(c) Suppose that $H \lhd G$, $K \lhd G$ and $H \cap K = \{1\}$. Show that $HK \cong H \times K$. (Suggestion, if $h \in H$ and $k \in K$, then consider $hkh^{-1}k^{-1}$.)

ANS: (a) Not that $HK = \bigcup_{h\in H} hK$. Furthermore $h_1K = h_2K$ exactly when $h_2^{-1}h_1 \in K$. Of course, this is equivalent to saying $h_2^{-1}h_1 \in H \cap K$ or that $h_1H \cap K = h_2H \cap K$. Thus HK consists of $[H : H \cap K]$ many distinct K-cosets. Thus
$$|HK| = [H : H \cap K] \cdot |K| = \frac{|H|}{|H \cap K|}|K|.$$
Hence the result.

(b) Since $H \subset N_G(K)$, we have $HK \subset KH$. But then
$$(HK)(HK) \subset KHK \subset HK,$$
says HK closed under multiplication and
$$(HK)^{-1} = KH \subset HK$$

says HK is closed under inversion. Hence HK is a subgroup.

(c) Note that $hkh^{-1}k^{-1} \in H \cap K$. Hence $hkh^{-1}k^{-1} = 1$ and $hk = kh$ for any $h \in H$ and $k \in K$. Thus the map $(h, k) \mapsto hk$ is a homomorphism of $H \times K$ onto the subgroup HK. But if $hk = 1$, then $h = k^{-1} \in H \cap K$. Hence $h = 1 = k$, and the map is an isomorphism.

3. Let F be a finite field and $F^\times$ the multiplicative group of units (a.k.a. the nonzero elements). We want to show that $F^\times$ is cyclic.

(a) Let $G = \mathbf{Z}_{n_1} \times \mathbf{Z}_{n_2} \times \cdots \times \mathbf{Z}_{n_k}$ be a finite abelian group with $n_j \mid n_{j-1}$ for $2 \le j \le k$ and $n_j \ge 2$. If we view the operation in G as multiplication with identity 1, how many solutions to $x^{n_1} = 1$ there are in G? (If you write the operation in G additively and use 0 for the identity, this is the same as asking how many solutions to $n_1 \cdot x = 0$ are there?)

(b) Use that fact that in $F[x]$ a polynomial of degree n can have at most n zeros to show that $F^\times$ must be cyclic as claimed.

ANS: (a) Considering G as a $\mathbf{Z}$-module with invariant factors n_i, we saw (long ago) in lecture that the exponent of G is n_1. Hence $n_1 \cdot x =$ has $|G| = n_1 n_2 \cdots n_k$ solutions.

(b) Now let $G = F^\times$. As an abelian group, it must have an invariant factor decomposition $n_1, \dots, n_k$ as above. Therefore, every element of $F^\times$ (now thought of multiplicatively) is a solution to $x^{n_1} - 1$. But over a field, the polynomial $x^{n_1 - 1}$ can have at most n_1 solutions. Hence $k = 1$ and $F^\times$ is cyclic.

4. Suppose that $|G| = pqr$ with $p < q < r$ primes. Let P, Q and R be a p-Sylow subgroup, a q-Sylow subgroup and a r-Sylow subgroup, respectively. Show that at least one of P, Q and R is normal in G.

ANS: Suppose $n_r > 1$. Then $n_r = 1 + kr$ with $k \ge 1$. But we also have $n_r \mid pq$. Since n_r is greater than p and q, we must have $n_r = pq$. On the other hand, if $n_q > 1$, then $n_q \mid pr$ says the only prime factors of n_q can be p and r. But $n_q > p$, so this forces $n_q \ge r$. Finally, $n_p > 1$ and $n_p \mid qr$ forces $n_p \ge q$.

Thus G has at least $n_r(r-1)$ elements of order r, and $n_q(q-1)$ elements of order q and $n_p(p-1)$ elements of order p. These are all distinct: all nonidentity elements of a group of prime order are generators. So since we also have $1 \in G$,

$$\begin{aligned} pqr = |G| &\le n_r(r-1) + n_q(q-1) + n_p(p-1) \\ &\le pq(r-1) + r(q-1) + q(p-1) + 1 \\ &\le pqr - pq + rq - r + pq - q \\ &= pqr + rq - r - q \end{aligned}$$

which, since $3 \le q < r$, is

$$< pqr + 3r - 2r = |G| + r.$$

Of course, this is a contradiction.

So at least one of n_r, n_q or n_p is 1.

Comment: Justin Troyka gave the following clever argument that in fact $R \lhd G$. First just counting distinct elements of order r and q, we get

$$\begin{aligned} |G| &\le n_r(r-1) + n_q(q-1) \\ &\le pq(r-1) + r(q-1) \\ &\le pq(r-1) + rp \\ &\le pqr - pq + rp \\ &> pqr - pq + pq = pqr. \end{aligned}$$

This is a contradiction and forces at least one of Q and R to be normal. Suppose to the contrary, $R \ntriangleleft G$. Then by the above $Q \lhd G$ and QR is a subgroup of index p in G. Hence QR is normal in G. Since the index of R in RQ is q and since q is the smallest prime dividing $|QR$, R is normal in QR. But then it is the unique r-Sylow subgroup of QR and is characteristic in QR. But then, since $QR \lhd G$, R would be normal in G.

5. Let $|G| = 105$. Suppose that G has a normal 3-Sylow subgroup. Show that $G \cong \mathbf{Z}_{105}$,

ANS: Let P, Q and R be Sylow subgroups of order 3, 5 and 7, respectively. We have $P \lhd G$ by assumption. We know from lecture that $Q \lhd G$ and $R \lhd G$. Hence QR is a subgroup by part 2b above. Since $Q \cap R = \{1\}$, $|QR| = 35$ and has no elements of order 3. Hence $P \cap QR = \{1\}$. Hence $P(QR)$ is a subgroup of G of order 105 and is equal to G. But by 2c, $QR \cong Q \times R$. Since QR has index 3, it is normal in G and $G \cong P \times QR \cong P \times Q \times R$. The latter is cyclic of order 105.