Math 250a hw2

12. **(b)** If $H \cap N = \{e\}$, show that the map $H \times N \to HN$ given by $(x, y) \mapsto xy$ is a bijection, and that this map is an isomorphism iff f is trivial, i.e., $f(x) = \mathrm{id}_N$ for all $x \in H$.

Proof. Call the map ψ.

- ψ is injective. For $x_1, x_2 \in H, y_1, y_2 \in N$, suppose $x_1 y_1 = x_2 y_2$. Then $x_2^{-1} x_1 = y_2 y_1^{-1} \in H \cap N = \{e\}$, so both sides are equal to the identity e. Thus, $x_1 = x_2$ and $y_1 = y_2$.
- ψ is surjective by the definition of HN.

If ψ is a group homomorphism, then for any $x \in H, y \in N$, we have

$$\begin{aligned} \psi((e,y),(x,e)) &= \psi((e,y))\psi((x,e)) \\ \psi((x,y)) &= yx \\ xy &= yx \\ xyx^{-1} &= y \\ f(x) &= \mathrm{id}_N \quad \text{since } y \text{ is arbitrary} \end{aligned}$$

Since x is arbitrary, we have $f(x) = \mathrm{id}_N$ for all $x \in H$.

Conversely, if $f(x) = \mathrm{id}_N$ for all $x \in H$, then for all $y \in N$,

$$\begin{aligned} f(x)(y) &= \mathrm{id}_N(y) \\ xyx^{-1} &= y \\ xy &= yx \quad \forall x \in H, \forall y \in N \end{aligned}$$

Thus, $\psi((x_1, y_1), (x_2, y_2)) = \psi((x_1, y_1))\psi((x_2, y_2))$ for all $x_1 x_2 \in H, y_1, y_2 \in N$, so ψ is a homomorphism. Since it is also a bijection, ψ is an isomorphism. □

Common mistake: the group law of product is defined component-wisely; if elements of H, N do not commute, ψ is not necessarily a homomorphism.

Remark on 19. $t \sim s \iff t \in Gs$ defines an equivalence relation on G. Indeed,

- $s = es, s \in Gs$
- $t = gs \implies s = g^{-1}t \implies s \in Gt$
- $t = gs, s = hr \implies t = ghr \implies t \in Gr$.

Thus, $\{Gs : s \in G\}$ form a partition of G.

20. Let P be a p-group. Let A be a normal subgroup of order p. Prove that A is contained in the center of P.

Here is a collection of solutions.

Proof 1. Since A is normal, for any $x \in P, a \in A$, we have $xax^{-1} \in A$. Thus, P acts on A by conjugation. Let Z denote the center of P and Z_A denote $Z \cap A$. Since the intersection of subgroups is again a subgroup, Z_A is a p-subgroup. By the class formula,

$$|A| = |Z_A| + \sum_{a \in C} \frac{|P|}{|P_a|}$$

where C is a set of representatives for the distinct, nontrivial conjugacy classes and $P_a = \{x \in P : xa = a\}$. Note that $|P_a| \neq |P|$ (otherwise $a \in Z_A$), so $p | \frac{|P|}{|P_a|}$. If $|Z_A| = |A| = p$, then $A = Z_A$ and $A \subset Z$. Otherwise $|Z_A| = 1$ and the class formula modulo p gives $0 \equiv 1 \mod p$, a contradiction. □

Proof 2. Since A is normal, P acts on A by conjugation. The action induces a homomorphism $\phi : P \to \mathrm{Aut}(A) \cong \mathbb{Z}/(p-1)\mathbb{Z}$. The order of $\phi(P)$ divides both $|P|$ and $p-1$. Since P is a p-group, $\phi(P) = \{e\}$, so for all $x \in P, a \in A, xax^{-1} = a$. Thus, A is in the center of P. □

A variation of the above proof maps P into S_{p-1}, the permutation group of $p-1$ objects.

Proof 3. Since $|A| = p$, A is cyclic. Let $A = \langle a \rangle$, for any $x \in P$, there is $k \in \{0, 1, \ldots, p-1\}$ such that $xa = a^k x$. Let p^n be the order of x, then $a = x^{p^n} a = a^{k^{p^n}} x^{p^n} = a^{k^{p^n}}$. Thus, $a^{k^{p^n}-1} = e$, so $k^{p^n} \equiv 1 \mod p$. By Fermat's Little Theorem, $k \equiv 1 \mod p$, so $xa = ax$. Since x is arbitrary, $A \subset Z(P)$. □

24. Let p be a prime number. Show that a group of order p^2 is abelian, and that there are only two such groups up to isomorphism.

Proof. By theorem 6.5, a nontrivial p-group G has a nontrivial center Z (proved by the class formula). If $|Z| = p^2$, then G is abelian. If $|Z| = p$, then both Z and G/Z have order p and thus are cyclic. Let $Z = \langle x \rangle, G/Z = \langle yZ \rangle$ for some representative $y \in G$, Then $G = \left\{ y^j x^i : i, j \in \{0, \ldots, p-1\} \right\}$. Since $x \in Z$,

$$\begin{aligned} y^\ell x^k y^j x^i &= y^{\ell+j} x^{k+i} \\ &= y^j x^i y^\ell x^k \end{aligned}$$

so G is again abelian and $|Z| = p^2$.

Suppose G has an element of order p^2, then G is cyclic and $G \cong \mathbb{Z}/p^2\mathbb{Z}$. Otherwise, pick $x \in G - \{e\}$ so $x^p = 1$, and pick $y \notin \langle x \rangle$ so $y^p = 1$ and $\langle x \rangle \cap \langle y \rangle = \{e\}$. By 12(b), $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \cong \langle x \rangle \langle y \rangle$ is a subgroup of G. Since both have order p^2, we conclude that $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. □

26. (a) Let G be a group of order pq, where p, q are primes and $p < q$. Assume that $q \not\equiv 1 \mod p$. Prove that G is cyclic.

Proof 1. Let P be a p-Sylow subgroup of G and Q be the q-Sylow subgroup of G. By lemma 6.7, $p < q$ implies that Q is normal. Then P acts by conjugation on Q, so there is a homomorphism $f : P \to \mathrm{Aut}(Q) \cong \mathbb{Z}/(q-1)\mathbb{Z}$. Since $p \nmid q-1$, f is trivial. Thus, for all $x \in P, y \in Q$, we have $xy = yx$. Follow the same line as proposition 6.8, G is abelian and, since $p \neq q$, cyclic. □

Proof 2. Let P be a p-Sylow subgroup of G and let N_P be its normalizer. Observe that $P \leq N_P$, so either P is normal, or $P = N_P$. By Sylow's third theorem, the number n_p of p-Sylow subgroups of G is $\equiv 1 \mod p$. The number $n_p = \frac{|P|}{|N_P|} \neq q$, so P is normal. Similarly, let Q be a q-Sylow subgroup of G, then Q is also normal, and $P \cap Q = \{e\}$. By 12(b), $PQ \cong P \times Q \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}/pq\mathbb{Z}$ is cyclic. Since PQ is a subgroup of G of the same order pq, we conclude that $G \cong PQ$. □