# August 2012 Algebra Prelim

Sarah Arpin

## 1

Show that there is no simple group of order 120.

*Solution:*
Let $n_p$ denote the number of Sylow $p$-subgroups of a group $G$ such that $|G| = 120 = 2^3 \cdot 3 \cdot 5$. Assume $G$ is simple. We will show that this leads to a contradiction.
Using the Sylow theorems, we see:

$$n_5 \equiv 1 \pmod 5, \text{ and } n_5 | 25 \Rightarrow n_5 = 1 \text{ or } 6$$

If $G$ is simple, then it cannot contain any normal subgroups, and if $n_5 = 1$ the Sylow 5-subgroup of $G$ would be normal (all conjugates of Sylow $p$-subgroups are Sylow $p$-subgroups: if all of $P_5 \in \mathrm{Syl}_5(G)$'s conjugates are equal to itself, $P_5$ is normal, which contradicts $G$ being simple).
Let $G$ act by conjugation on the set of Sylow 5-subgroups of $G$. This action produces a homomorphism $\varphi : G \to S_6$.
This action is nontrivial, so the image of $G$ under $\varphi$ must nontrivially intersect $A_6$, since $\varphi(G)$ cannot consist solely of odd permutations. So $\varphi^{-1}(A_6) \neq \{1\}$.
Since $A_6 \trianglelefteq S_6$, $\varphi^{-1}(A_6) \trianglelefteq G$. If we assume that $G$ is simple, this means $\varphi^{-1}(A_6) = G$, so we have embedded $G$ as a subgroup of $A_6$.
By order considerations, we see that $|A_6 : G| = 3$, which is not possible: if we let $A_6$ act on the left cosets of $G$ in $A_6$ by left multiplication, this action would embed $A_6$ into $S_3$, which is not possible since $A_6$ is simple and $S_3$ is not.
Thus, our original assumption that $G$ is simple must be wrong, so there is no simple group of order 120.

$\square$

## 2

Show that any group of order $104 = 2^3 \cdot 13$ is solvable (without using Burnside's theorem).

*Solution:*
Let $G$ be a group of order 104.
By Sylow analysis, we see that $G$ must have a normal Sylow 13-subgroup, say $P \in \mathrm{Syl}_{13}(G)$.
$P$ is solvable, because $P \cong \mathbb{Z}_{13}$, which is cyclic and cyclic groups are solvable.
If we consider $G/P$, we have a group of order $2^3$. A prime power group of order $p^k$ has a subgroup of order $p^i$ for $i = 0, 1, ..., k-1$, so $G/P$ has a subgroup $H_1$ of order $2^2$, $H_1$ has a subgroup $H_2$ of order 2.
$[G/P : H] = 2$, so $H$ is a normal subgroup of $G/P$.
$[H : H_1] = 2$, so $H_1$ is a normal subgroup of $H$.
$[H_1 : H_2] = 2$, so $H_2$ is a normal subgroup of $H_1$.
$|H_2| = 2$, so $H_2$ is isomorphic to $\mathbb{Z}_2$ and is thus cyclic. Same holds for the other quotients $H_1/H_2$ and $H/H_1$.
Thus, we have the following normal series to show that $G/P$ is solvable:

$$1 \trianglelefteq H_2 \trianglelefteq H_1 \trianglelefteq H \trianglelefteq G/P$$

Since $G/P$ is solvable and $P$ is solvable, $G$ must be solvable as well.

$\square$

## 3

Suppose $R$ is a commutative ring with identity. A proper ideal $I$ in $R$ is said to be a *primary* ideal if whenever elements $a$ and $b$ in $R$ satisfy $ab \in I$ and $a \notin I$, then there exists a positive integer $m$ such that $b^m \in I$.

(a) Show that every prime ideal in $R$ is a primary ideal.

(b) Let $I$ be a primary ideal and let

$$I' = \{a \in R : a^m \in I \text{ for some positive integer } m\}$$

Show that $I'$ is a prime ideal containing $I$.

(c) Show that if $R$ is a PID then any primary ideal of $R$ is a power of a prime ideal.

*Solution:*

(a) If $I$ is a prime ideal then $ab \in I$ implies either $a \in I$ or $b \in I$, which satisfies the necessary condition taking $m = 1$.

(b) By construction, every element $a \in I$ is $a^1 \in I$, so $I \subseteq I'$.
To show that $I'$ is a prime ideal, suppose $ab \in I'$. Then, $(ab)^m \in I$, so $a^m b^m \in I$. Since $I$ is a primary ideal, if $a^m \notin I$, then $b^{mn} \in I$, for some positive integer $n$. If $a^m \in I$, then $a \in I'$. If $a^m \notin I$, then $b \in I'$, by construction. Thus, either $a \in I'$ or $b \in I'$, so $I'$ is a prime ideal.

(c) Suppose $I$ is a primary ideal of $R$. Since $R$ is a PID, we have $I = (a)$ for some $a \in R$.
If $R$ is a PID, then it is also a UFD and we have a factorization of $a$ into a product of irreducibles: $p_1...p_n$.
If $a$ iself is irreducible, then $a = p_1$, and the irreducibles are prime in a PID, so $(a)$ is immediately a prime ideal itself.
$a \in I$, so $p_1...p_n \in I$, which means either $p_1 \in I$ or $(p_2...p_n)^m \in I$, for some positive integer $m$.

*Case 1:* If $p_1 \in I = (a)$, then there exists some $s \in R$ such that $sa = p_1$. This implies $sp_2...p_n = 1$, which means $p_2, ..., p_n$ are units, so $(p_1) = (a) = I$.
*Case 2:* If $(p_2...p_n)^m \in I$, for some positive integer $m$, then there exists $r \in R$ such that $ra = (p_2...p_n)^m$, which implies $rp_1 = (p_2...p_n)^{m-1}$. Howeve