Final (Solution)

M551 – Abstract Algebra

December 7th, 2011

1. Let p be a prime and G be a *non-abelian* group of order p^3. Prove that $G/Z(G) \cong Z_p \times Z_p$ [where $Z(G)$ is the center of G and Z_p is a multiplicative cyclic group of order p].

Proof. Since G is a p-group, the center is non-trivial. Since G is not abelian, the center is not the whole group. So, $|Z(G)|$ is either p or p^2. If $|G| = p^2$, then $G/Z(G)$ is of order p, and thus cyclic. But this implies that G is abelian, and hence a contradiction. Therefore, $|Z(G)| = p$ and $|G/Z(G)| = p^2$.

Thus, we have $G/Z(G)$ is isomorphic to either Z_{p^2} or to $Z_p \times Z_p$. If the former, then it is cyclic, which would imply, again, that G is abelian, and hence a contradiction. Thus, $G/Z(G) \cong Z_p \times Z_p$. $\square$

2. Let G be a finite *simple* group. Show that if p is the *largest* prime dividing $|G|$, then there is no subgroup $H \leq G$ such that $1 < |G : H| < p$.

Proof. Let $n \stackrel{\text{def}}{=} |G : H|$, and assume that $1 < n < p$. Also, let $\Omega \stackrel{\text{def}}{=} \{g_1H, \dots, g_nH\}$ be the set of cosets of H in G. Then, G acts on Ω by left multiplication. The representation $\phi : G \to S_\Omega \cong S_n$ is faithful, as G is simple.

Since $p \mid |G|$, by Cauchy's Theorem, there exists an element $g \in G$ of order p. Thus $\phi(g) \in S_n$ has order p. But, since $n < p$ this is impossible, as the order of an element of S_n is the least common multiple of the lengths of the cycles in its decomposition into disjoint cycles. Since p is prime, this means that its decomposition into disjoint cycles has at least one cycle of length p. But a cycle of S_n cannot have length greater than n. $\square$

3. Let R be a PID. Show that every ideal I of R, with $I \neq 0, R$, is a product of finitely many maximal ideals, and that this decomposition is unique up to reordering.

Proof. Since R is a PID, we have that $I = (a)$. Since $I \neq 0$, we have that $a \neq 0$. Since $I \neq R$, we have that $a \notin R^\times$.

Since R is a UFD [as PID implies UFD], we have that $a = p_1 \cdots p_k$, with p_i's irreducibles. Since R is a UFD, this implies that the p_i's are primes, and hence (p_i) is a prime ideal. Since R is a PID, we have that (p_i) is maximal. Thus,

$$I = (a) = (p_1) \cdots (p_k).$$

Now, suppose that $I = M_1 \cdots M_l$, with M_i's maximal. Then, since R is a PID, there exists $m_i \in R$ such that $M_i = (m_i)$. Since M_i is prime, so is m_i, and hence irreducible. Therefore, since $I = (a)$, there exists a unit u such that $a = u \cdot m_1 \cdots m_l$, and this is another factorization of a. By uniqueness of factorization, we have that $k = l$, and after a possible reordering, we can assume that p_i and m_i are associates. But then $(p_i) = (m_i) = M_i$.

□

4. Let R be a noetherian commutative ring with 1 [and $1 \neq 0$] and D be a multiplicative closed subset of R with $1 \in R$ and $0 \notin R$. Let $R_D \stackrel{\text{def}}{=} D^{-1}R$ be the localization of R at D. Show that R_D is also noetherian.

Proof. Let $J_1 \subseteq J_2 \subseteq J_3 \subseteq \cdots$ be an infinite chain of ideal from R_D. Let $I_i \stackrel{\text{def}}{=} {}^{\text{c}}J_i$ be the contraction of the ideal J_i, i.e., if $\pi : R \to R_D$ is the homomorphism defined by $\pi(r) = r/1$, then $I_i \stackrel{\text{def}}{=} \pi^{-1}(J_i)$. Then, we have $I_1 \subseteq I_2 \subseteq \cdots$. Since R is a noetherian [and I_i's are ideals of R], we have that there exists N such that $I_n = I_N$ for all $n \geq N$. Then, we must have $J_n = {}^{\text{e}}I_n = {}^{\text{e}}I_N = J_N$. [**Note:** We've seen in class that if J is an ideal of R_D, then ${}^{\text{e}}({}^{\text{c}}J) = J$, but if I and ideal of R that is not prime, then maybe ${}^{\text{c}}({}^{\text{e}}I) \neq I$.] Thus, R_D satisfies the ACC of ideals, and hence it is noetherian.

Here is an alternative proof: Let $\pi : R \to R_D$ be the homomorphism defined by $\pi(r) = r/1$, I be an ideal of R_D and $I' \stackrel{\text{def}}{=} \pi^{-1}(I)$ be the contraction of I to R [which we know is an ideal]. Then, since R is noetherian, we have that $I' = (a_1, \ldots, a_n)$ for some $a_i \in R$.

We claim that $I = (a_1/1, \ldots, a_n/1)$. Since $a_i \in I'$, we have that $\pi(a_i) = a_i/1 \in I$ [by definition of I]. So, clearly $(a_1/1, \ldots, a_n/1) \subseteq I$.

Now, let $r/d \in I$. Then, $d/1 \cdot r/d = r/1 \in I$. Therefore, $r \in I'$. Thus, $r = r_1a_1 + \cdots + r_na_n$, for some $r_i \in R$. Thus $r/1 = (r_1a_1 + \cdots + r_na_n)/1 = r_1/1 \cdot a_1/1 + \cdots + r_n/1 \cdot a_n/1$, and so $r/d = r_1/d \cdot a_1/1 + \cdots + r_n/d \cdot a_n/1$. Therefore, $r/d \in (a_1/1, \ldots, a_n/1)$ and $I \subseteq (a_1/1, \ldots, a_n/1)$.

$\square$