# Final (In Class Part)

M551 – Abstract Algebra

December 13th, 2007

**1.** Let $p$ be a prime and $G$ be a *non-abelian* group of order $p^3$. Prove that $Z(G)$ [the center of $G$] has order $p$ and that it is equal to the commutator subgroup $G'$ [also denoted by $[G, G]$].

*Proof.* Since $G$ is a $p$-group, we have that $Z(G) \neq 1$, and since $G$ is not abelian, we have that $Z(G) \neq G$. So, we must have $|Z(G)| = p$ or $p^2$. If $|Z(G)| = p^2$, we would have that $|G/Z(G)| = p$, and hence cyclic. [Note that $Z(G)$ is always normal in $G$.] But a previous result, we have that $G$ would the be abelian, which is a contradiction. Therefore, $|Z(G)| = p$.

Now, $|G/Z(G)| = p^2$, and hence [by another previous result], $G$ must be abelian. So, $G' \leq Z(G)$ [by yet another result]. Hence, $|G'| = 1$ or $G' = Z(G)$. But $G' = 1$ if, and only if, $G$ is abelian, and hence $G' = Z(G)$.

□

**2.** Let $p, q, r$ be three primes such that $p < q < r$ and $G$ be a group with $|G| = pqr$. Prove that $G$ is solvable. [You can use neither Feit-Thompson's nor Burnside's Theorems, which we did not prove in class.]

*Proof.* We prove two claims first.

**Claim:** If $|G| = pq$ with $p$ and $q$ primes and $p < q$, then $G$ is solvable. [These $p$, and $q$ are any primes, not necessarily the ones from the statement.]

*Proof.* We prove that $G$ has a normal subgroup of order $q$. By Sylow's Theorem, $G$ has a subgroup of order $q$, and since its index is the least prime divisor of $|G|$, it is normal.

[Alternatively, one can also use Sylow's Theorem again: if $n_q \stackrel{\text{def}}{=} n_q(G) \in \{1, p\}$, but $n_q \equiv 1 \pmod{q}$. Since $q > p$, we must have $n_q = 1$. So, if $\{Q\} = \text{Syl}_q(G)$, we have that $Q \triangleleft G$ and $|Q| = q$.]

So, we have that $G/Q$ has order $p$, and hence it is abelian. Since $Q$ also has prime order, $Q$ is also abelian. Thus,

$$1 \triangleleft Q \triangleleft G,$$

is a solvable series.

□

**Claim:** The group $G$ [from the statement] has a normal subgroup of prime order.

*Proof.* By Sylow's Theorem, we have that $n_r \stackrel{\text{def}}{=} n_r(G) \in \{1, p, q, pq\}$. Since $r > p, q$, we have that $n_r$ is either 1 or $pq$. If the former, we are done. So suppose $n_r = pq$. Then, we have $pq(r-1)$ elements of order $r$.

If $G$ does not have a normal subgroup of order $q$, then we have: $n_q \in \{1, p, r, pr\}$ and $n_q \equiv 1 \pmod{q}$. So, we must have $n_q \geq r$ [since $n_q \neq 1$ and $p < q$]. Thus, we would have at least $r(q-1)$ elements of order $q$.

But then, since we have at least $p-1$ elements of order $p$ and one element of order 1, then $G$ would have at least $pq(r-1)+r(q-1)+(p-1)+1 = pqr+(r-p)(q-1) > pqr = |G|$ elements, a contradiction.

Hence, either we have a normal subgroup of order $r$ or a normal subgroup of order $q$.

□

So, let $N$ be the normal subgroup of prime order of $G$ and $G/N$ be its quotient. Since $N$ is abelian, it's solvable. Since $|G/N|$ is a product of two distinct primes, $G/N$ is also solvable by the first claim. Thus, $G$ is solvable. [Using correspondence, if $H/N$ is the normal subgroup of prime order in $G/N$, we have that:

$$1 \triangleleft N \triangleleft H \triangleleft G$$

is a solvable series, since each quotient has prime order.]

□

**3.** Let $R$ be a DVR with field of fractions $F$. [You can use any theorem proved in class, but state it clearly.]

(a) Is $\mathbb{Q}[x, y]$ a DVR?

*Proof.* Suffice to show that $\mathbb{Q}[x, y]$ is not a PID. But $(y)$ is a prime ideal, since $\mathbb{Q}[x, y]/(y) = \mathbb{Q}[x]$, a domain, but not a field. Hence, $(y)$ is prime but not maximal, and thus $\mathbb{Q}[x, y]$ is not a PID.

□

(b) Show that if $a \in F$ and $f \in R[x]$ is *monic* polynomial such that $f(a) = 0$, then $a \in R$. [This says that $R$ is *integrally closed*.]

*Proof.* Let $\nu : F \to \mathbb{Z} \cup \{\infty\}$ be the valuation of $F$. Suppose that $\nu(a) = -k < 0$. If $f(x) = x^k + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0 \in R[x]$ [and so $\nu(b_i) \geq 0$] and $f(a) = 0$, then

$$a^n = -b_{n-1}a^{n-1} - \cdots - b_1 a - b_0,$$

and thus,

$$\begin{aligned} -kn &= \nu(a^n) \\ &= \nu(-b_{n-1}a^{n-1} - \cdots - b_1 a - b_0) \\ &\geq \min\{-ik + \nu(b_i) \ : \ i \in \{0, \ldots, (n-1)\}\} \\ &\geq \min\{-ik \ : \ i \in \{0, \ldots, (n-1)\}\} \\ &\geq -(n-1)k \\ &> -kn, \end{aligned}$$

which is a contradiction. Thus, $\nu(a) \geq 0$, i.e., $a \in R$.
[Alternatively, one can prove a more general result. A DVR is a UFD, and every UFD is integrally closed: if $a \in F$ is a root, then $f(x) = (x - a)g(x)$ in $F[x]$. Then, by [a consequence of] Gauss's Lemma, there are $\alpha, \beta \in F$ such that $f(x) = \alpha(x - a) \cdot \beta g(x)$, with $\alpha(x - a), \beta g(x) \in R[x]$. [This is Proposition 9.3.5.] Since $f$ is monic, so is $g$, and thus $\alpha\beta = 1$. Since $\alpha(x - a) \in R[x]$, we must have $\alpha \in R$, and since $\beta g(x) \in R[x]$ and $g$ is monic, $\beta \in R$. So, $\beta\alpha(x - a) = (x - a) \in R[x]$ and thus $a \in R$.]

□

(c) Show that $F$ is not *algebraically closed*, i.e., that there exists a non-constant polynomial $g \in F[x] - F$ that has no roots in $F$.

*Proof.* Let $t$ be a uniformizer, i.e., an element of $R$ such that $\nu(t) = 1$. [So, we have that the unique maximal ideal of $R$ [which is local] is [principal] generated by $t$.]
Let $x^2 - t \in R[x]$. [By (b), if this polynomial has a root, it must be in $R$.] Let $\alpha$ be such a root. Then $\alpha^2 = t$, and hence $\nu(\alpha) = \nu(t)/2 = 1/2$. But the range of $\nu$ is $\mathbb{Z} \cup \{\infty\}$, and so this is a contradiction.

□

**4.** Let $R$ be a UFD.

(a) Prove that $R[x_1, x_2, \ldots]$ is also a UFD. [So, this ring is a non-Noetherian UFD.]

*Proof.* We have seen in class [as an application of Gauss's Lemma] that $S_n \stackrel{\text{def}}{=} R[x_1, \ldots, x_n]$ is an UFD for all $n$. Let's also denote $S \stackrel{\text{def}}{=} R[x_1, x_2, \ldots]$. Now let $f \in S$. Then, there exists $n$ such that $f \in S_n$.

**Claim:** $f$ is irreducible in $S$ if, and only if, it is irreducible in $S_n$.

*Proof.* The "only if" part is trivial, *since the units of both rings are the same*, namely $R^\times$. [We have to be a bit careful here!]

Now, if $f = gh$, with $g, h \in S - R^\times$, then there exists $m \geq n$ such that $g, h \in S_m$, which can be taken to be minimal. If $m > n$, then we have that $0 = \deg_{x_m} f = \deg_{x_m} g + \deg_{x_m} h$ [since $R[x_1, \ldots, x_{m-1}]$ is a domain, since $R$ is a domain]. But then, $g, h \in S_{m-1}$, contradicting the minimality of $m$. Thus, $g, h \in S_n$, and hence $f$ is reducible in $S_n$.

□

We now show that if $f$ is irreducible in $S$, then it must be prime. [Remember that this guarantees uniqueness of factorization.] Suppose that $f \mid gh$ in $S$. Then, there exists $m \geq n$ such that $f, g, h \in S_m$ and $f \mid gh$ in $S_m$. But $S_m$ is a UFD, and by the claim, $f$ must be irreducible in $S_m$ and therefore prime in $S_m$. Thus, $f \mid g$ or $f \mid h$ in $S_m$ and therefore in $S$.

Finally, it just remains to show the *existence of factorization*. Take $f \in S$. Then, there exists $n$ such that $f \in S_n$. Since $S_n$ is a UFD, there are $f_1, \ldots, f_k \in S_n$ irreducibles, such that $f = f_1 \cdots f_k$. But, by the claim, these are irreducibles in $S$ also, and hence this is a factorization of $f$ in $S$.

[Another way to see this existence is using the chain of principal ideals. Suppose we have

$$(f) = (f_0) \subseteq (f_1) \subseteq (f_2) \subseteq \cdots .$$

Suppose that $f \in S_n$. Since $f_1 \mid f$, there exists $g_1 \in S_m$, for some $m \geq n$ such that $f = g_1 f_1$ in $S_m$ [and hence, $f_1 \in S_m$]. By taking degrees in $x_m$ again, we can show that $m \leq n$. So, $f_1 \in S_n$. Repeating the argument, we have that $f_i \in S_n$ for all $i$, and $f_i \mid f_{i-1}$ in $S_n$. Since $S_n$ is a UFD, this sequence is eventually stationary, and hence there exists factorization in $S$.]

□

(b) Prove that if for all $a, b \in R$, there is $c \in R$ such that $(a, b) = (c)$ [i.e., $R$ is a Bezout domain], then $R$ is a PID. [We are still assuming that $R$ is a UFD!]

*Proof.* Let $I$ be an ideal which is not finitely generated. The, there are $a_1, a_2, \ldots \in I$ such that

$$(a_1) \subsetneqq (a_1, a_2) \subsetneqq (a_1, a_2, a_3) \subsetneqq \cdots .$$

But then, since $R$ is Bezout, for each $i$, there exists $b_i$ such that $(a_1, \ldots, a_i) = (b_i)$. [There is a little induction here, but we've mentioned it in class.] So, we have

$$(a_1) \subsetneqq (b_2) \subsetneqq (b_3) \subsetneqq \cdots .$$

But, the existence of factorization in $R$ guarantees that this sequence eventually stops. [If you want to see it explicitly, just note that each $b_i$ is a divisor of $a_1$, and if $a_1$ has finitely many divisors, up to multiplication by units [which does not affect the ideals]. In particular, if $a_1 = p_1 \cdots p_k$, with $p_i$ irreducible, the longest sequence of of principal ideals, as above, would have $k + 1$ ideals in it:

$$(p_1 \cdots p_k) \subsetneqq (p_1 \cdots p_{k-1}) \subsetneqq (p_1 \cdots p_{k-2}) \subsetneqq (p_1) \subsetneqq (1).]$$

[Alternatively, one can let $a \in I$ with the least number of factors, if $I \neq (0), R$, and prove that $I = (a)$.]

□