Algebra Qualifying Exam **Name:**
January 7th, 2015

Instructions:

- Provide justification for each of your answers and make your arguments clear, but try to avoid excessive detail.
- The exam has **8** questions; you need to answer all to get full credit.

1. Let G be a finite group with distinct primes p, q, r dividing the order of G. Let S_p, S_q denote a Sylow p and a Sylow q-subgroup of G respectively. Let n_p denote the number of Sylow p-subgroups of G (and similarly for n_q, n_r).

(a) If $n_p = 1$ and $n_q = 1$, then show every element of S_p commutes with every element of S_q. (*Hint*: if $x \in S_p$ and $y \in S_q$, then where does the commutator $[x, y]$ lie?)

(b) Now suppose $|G| = pqr$ and suppose $n_p = n_q = n_r = 1$. Show that G is isomorphic to the cyclic group $\mathbf{Z}/pqr \cong \mathbf{Z}/p \times \mathbf{Z}/q \times \mathbf{Z}/r$.

(c) Show that there is only one group of order $255 = 3 \cdot 5 \cdot 17$ up to isomorphism, namely the cyclic group $\mathbf{Z}/255$.

2. Indicate whether the following statements are TRUE or FALSE. If you believe a given statement is True, then provide a short proof; if False, then construct a counterexample.

(a) If the ring R is a PID, then in R every prime ideal is a maximal ideal.

(b) If a (non-simple) group G has the property that every proper subgroup is normal, then G must be abelian.

(c) There is only one group G of order 21 up to isomorphism i.e., $|G| = 21$ implies $G \cong \mathbf{Z}/21 \cong \mathbf{Z}/3 \times \mathbf{Z}/7$.

3. A commutative ring R (with 1) is called a *local ring* if it has a unique maximal ideal. Show that a commutative ring R is a local ring if and only if for any elements $u, v \in R$ such that $u + v = 1$, then either u or v is a unit in R.

4. Let R be an integral domain (with 1) such that the polynomial ring $R[x]$ is a PID (principal ideal domain). Show that R must in fact be a field. (*Hint*: Let $a \in R$ be any non-zero element. By considering the ideal $(a, x) \subseteq R[x]$ show that a is a unit.)

5. Let G be a finite group of order $|G| = 2m$, where m is an odd integer. Show that G has a subgroup of index 2. (*Hint*: Construct a homomorphism $G \to \mathrm{S}_{2m} \to \{\pm 1\}$, where the second map is the usual sign map and show that the composite map is surjective. And so, the kernel is the required subgroup.)

6. Let $\alpha = \sqrt{i + 2}$, where i is a square root of -1. Find the minimal polynomial of α over $\mathbf{Q}$. Be sure to show that the polynomial you find is irreducible.

7. Let $p(x) = x^5 - 4x + 2 \in \mathbf{Q}[x]$. Let $E/\mathbf{Q}$ be the splitting field of $p(x)$ over $\mathbf{Q}$.

(a) Show that $p(x)$ is irreducible over $\mathbf{Q}$. Show further (using Calculus as needed) that $p(x)$ has three real roots and two complex roots.

(b) Show that the Galois group $\mathrm{Gal}(E/\mathbf{Q})$ contains an element of order 5 and a transposition (*Hint*: what is the effect of complex conjugation?)

(c) Since $\mathrm{Gal}(E/\mathbf{Q}) \subseteq \mathrm{S}_5$, the symmetric group, argue that the element of order 5 must be a 5-cycle. Conclude that $\mathrm{Gal}(E/\mathbf{Q})$ is in fact the full symmetric group S_5.

8. Let $\mathbf{F}_p$ denote the finite field of size p, where p is an integer prime. In this problem, assume further that $p > 2$. Suppose $f(x) = x^m + 1$ is an irreducible polynomial in $\mathbf{F}_p[x]$ and let E be its splitting field over $\mathbf{F}_p$.

(a) Show that for any root α of $f(x)$ in E, we have that $\alpha^{2m} = 1$ and $\alpha^k \neq 1$ for any $1 \leqslant k < 2m$.

(b) Prove that $2m$ divides $p^m - 1$ but that $2m$ does not divide $p^n - 1$ for any $1 \leqslant n < m$.

(*Hint*: Consider the size and nature of the multiplicative group of $\mathbf{F}_{p^m}$ and use Lagrange's theorem.)