ALGEBRA COMPREHENSIVE EXAMINATION

Spring 2006

Bishop*
Krebs
Shaheen.

Answer 5 questions only. You must answer *at least one* from each of groups, rings, and fields. Be sure to show enough work that your answers are adequately supported.

GROUPS

1. Let G be a group. Suppose that M is a normal subgroup of G such that
   - $M \neq G$, and
   - If S is a subgroup of G and $M \subseteq S$, then $M = S$ or $S = G$.

   Prove that G/M is a cyclic group of prime order.

2. Prove that $\mathbf{Z}_{mn} \cong \mathbf{Z}_m \times \mathbf{Z}_n$ if and only if $\gcd(m, n) = 1$.

3. a. Identify a group of order 60 that is not solvable (you do not need to prove this).
   b. Identify two groups of order 60 that are nonisomorphic, nonabelian, and solvable and verify that they do meet this criteria.

RINGS

1. Let R be a subring of a field F such that, for every $x \in F$, either $x \in R$ or $x^{-1} \in R$. Prove that the ideals of R are linearly ordered; i.e., if I and J are ideals of R, then either $I \subseteq J$ or $J \subseteq I$.

2. a. Let F be a field and let $F[x]$ be the ring of polynomials over F. Prove that every ideal in $F[x]$ is principal.
   b. Let $\mathbf{Q}$ be the field of rationals. Find (and verify) a principal generator for (f, g), the ideal generated $f = x^3 + 3x^2 + 2x$ and $g = x^2 - 1$.

3. Let $\mathbf{N}$ be the set of positive integers, and let $\mathbf{Z}$ be the set of integers. Let R be the set of functions from $\mathbf{N}$ to $\mathbf{Z}$. Define + and $\cdot$ on R in the obvious way: $(f + g)(n) = f(n) + g(n)$ and $(f \cdot g)(n) = f(n) \cdot g(n)$. Note (you do not have to prove this) that with this addition and multiplication, R is a ring. For any $S \subseteq \mathbf{N}$, let

   $$I(S) = \{f \in R \mid f(n) = 0 \text{ for all } n \in S\}.$$

   a. For any $S \subseteq \mathbf{N}$, prove that the set $I(S)$ is an ideal of R.
   b. If $S_1 \subseteq S_2 \subseteq \mathbf{N}$, prove that $I(S_2) \subseteq I(S_1)$.
   c. Find an infinite chain of proper ideals of R, $I_1 \subset I_2 \subset I_3 \subset \ldots$

FIELDS

1. Let G be a finite group. Prove that there exists a field K and a Galois extension field L such that $\mathrm{Gal}(L/K) \cong G$; i.e., the Galois group of the extension is isomorphic to G.

2. Let $\mathbf{Q}$ be the field of rational numbers and $E = \mathbf{Q}(\sqrt{3}, \sqrt{5})$ and $\alpha .= \sqrt{3} + \sqrt{5}$.
   a.. Prove that $[E : \mathbf{Q}] = 4$ and that $E = \mathbf{Q}(\alpha)$ and
   b. Describe the Galois group $G(E/\mathbf{Q})$.

3. Let F_q be a finite field of q elements with q odd. Show that $a \in F_q^* = F_q - \{0\}$ has a square root in F_q^* (that is, $x^2 = a$ has a solution in F_q^*) if and only if $a^{(q-1)/2} = 1$.