ALGEBRA COMPREHENSIVE EXAMINATION

Spring 2004

Brookfield
Bishop*
Cates.

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 finite group and S a nonempty sub*set* of G with the property that $SS = S$. Prove that S is a sub*group* of G.

2. Classify the group of units of the ring $\mathbf{Z}_{20}$ according to the Classification Theorem of Finite (or Finitely Generated) Abelian Groups.

3. Let G be a group of order 275 ($= 5^2 \cdot 11$). Show that $G'' = \{e\}$, where G' is the derived group of G, the subgroup generated by the commutators of G.

RINGS

1. Prove that a Euclidean domain satisfies the ascending chain condition on its ideals; i.e., if $I_1 \subseteq I_2 \subseteq \mathrm{I}_3 \subseteq \ldots$ is a chain of ideals in a ring R, then there exists an integer n such that thereafter, $I_n = I_{n+1} = \ldots$

2. Let R be the ring of functions from $\mathbf{R}$ to $\mathbf{R}$, the real numbers. Reminder: For $f, g \in R$, $f + g$ and fg are defined by $(f + g)(x) = f(x) + g(x)$ and $(fg)(x) = f(x)g(x)$ for all $x \in \mathrm{R}$.

   (a) Show that
   $$I = \{f \in R \mid f(0) = 0\}$$
   is an ideal of R which is maximal,

   (b) If $\mathbf{Z}[x]$ is the ring of polynomials over the integers $\mathbf{Z}$, show that
   $$J = \{f \in \mathbf{Z}[x] \mid f(0) = 0\}$$
   is an ideal of $\mathbf{Z}[x]$ which is *not* maximal.

3. Ler $R[[x]]$ denote the ring of formal power series of ring R.
   (a) Find $(1+ x)^{-1}$ in $\mathbf{Q}[[x]]$ where $\mathbf{Q}$ is the field of rational numbers.
   (b) Verify that $\mathbf{Q}[[x]]$ is not a field.

FIELDS

1. Let $\mathbf{Q}$ be the field of rationals and $\mathbf{C}$ be the complex numbers and let $\alpha \in \mathbf{C}$ be a zero of the irreducible polynomial $p(x) = x^4 - 2x^2 + 9$.
   (a) Confirm that $p(x)$ is irreducible over $\mathbf{Q}$
   (b) (i) Express α^{-1} as a $\mathbf{Q}$-linear combination of $\{1, \alpha, \alpha^2, \alpha^3\}$.
   (ii) Find $(1+\alpha)^{-1}$ as a $\mathbf{Q}$-linear combination of $\{1, \alpha, \alpha^2, \alpha^3\}$.

2. Let $\mathrm{GF}(p^n)$ denote the Galois field with p^n elements.
   (a) Prove that $\mathrm{GF}(p^a) \subseteq \mathrm{GF}(p^b)$ iff a divides b.
   (b) Prove that $\mathrm{GF}(p^a) \cap \mathrm{GF}(p^b) = \mathrm{GF}(p^d)$, where $d = \gcd(a, b)$.

3. Recall that an extension field E of a field F is called <u>simple</u> if it can be generated by a single element, say $E = F(\alpha)$ (= $F[\alpha]$ if α is algebraic over F), for some $\alpha \in E$. For $F = \mathbf{Q}$, the field of rational numbers, $\mathbf{Q}[\sqrt{3}]$ and $\mathbf{Q}[\sqrt[3]{2}]$ are simple algebraic extensions of $\mathbf{Q}$. Produce (and verify) a real number α such that $\mathbf{Q}[\sqrt{3}, \sqrt[3]{2}] = \mathbf{Q}[\alpha]$.