SWARTHMORE COLLEGE
Department of Mathematics and Statistics
Honors Examination

11 May 1996
8:30–11:30

Modern Algebra

DIRECTIONS: Please do at least one problem from each of the four sections; try to do at least six problems altogether. There are several essay questions scattered throughout the exam; do at most one of these, unless you just can't restrain yourself. By the way, if you choose one of the essay questions, don't just state the main results and sketch their proofs—tell me why the results are interesting as well.

I. GROUPS.

I.1. Let p be a prime number.

(a) Suppose that G is a group of order p^n. Show that G has a nontrivial center.

(b) Classify the groups of order p^2.

(c) Suppose that G is a group with p^n dividing the order of G. Must G have a subgroup of order p^n? Explain.

I.2. This is a rather open-ended problem; don't spend too long on it. (This one does not count as an essay question, by the way.) Fix an integer $n \geq 3$, and let D_n be the group of symmetries of a regular n-gon. What can you tell me about D_n? (For example, what is its order? Is it abelian? If not, what is its center? Is it simple? If not, what are its normal subgroups? Can you compute $\mathrm{Aut}(D_n)$ for any values of n?)

II. RINGS.

II.1. Let k be a field; for any integer $n > 0$, let C_n denote the cyclic group of order n. Let $k[C_n] = k[g]/(g^n - 1)$ (this is called $k[C_n]$ because it has a vector space basis $\{1, g, g^2, \ldots, g^{n-1}\}$, and the basis elements multiply according to the group multiplication in C_n). This is called the *group algebra* of C_n over k.

(a) Suppose that k has characteristic 2 (recall that this means that $1 + 1 = 0$ in k) and consider $k[C_2]$. Prove that

$$\begin{aligned} k[x] &\longrightarrow k[C_2] \\ x &\longmapsto 1 - g \end{aligned}$$

is a surjective ring homomorphism, and use this to get an alternate description of $k[C_2]$. (Even better, assume that k has characteristic p and do this for $k[C_p]$.)

(b) Classify the finitely generated $k[C_2]$-modules. Do you need the finite generation hypothesis?

(c) Recall that an *operation* of a group G on a set S is a function $G \times S \to S$ satisfying certain properties. Given a vector space V over k, does an operation of C_n on V make V into a $k[C_n]$-module? Why not?

II.2. Let R and S be rings, and $f\colon R \to S$ a ring homomorphism. Recall that an ideal I of R is *prime* if $xy \in I \Rightarrow$ either $x \in I$ or $y \in I$.

(a) Show that if P is a prime ideal of S, then

$$f^{-1}(P) = \{r \in R : f(r) \in P\}$$

is a prime ideal of R.

(b) Let N be the set of nilpotent elements of R:

$$N = \{r \in R : r^m = 0 \text{ for some } m \geq 1\}.$$

N is called the *nilradical* of R; it is an ideal (you don't have to prove that). Show that N is the intersection of all the prime ideals of R. (You may need to assume that R satisfies the ascending chain condition—there is no infinite strictly increasing chain

$$I_0 < I_1 < I_2 < I_3 < \dots$$

of ideals of R; alternatively, you may want to use Zorn's lemma. Also, see the warning below.)

(c) Part (a) lets us define a function

$$\begin{aligned} f^* : \{\text{prime ideals of } S\} &\longrightarrow \{\text{prime ideals of } R\}. \\ P &\longmapsto f^{-1}(P) \end{aligned}$$

Show that if $S = R/N$ and $f\colon R \to R/N$ is the quotient map, then f^* is a bijection.

Warning: part (b) may be too hard. If you struggle with it for a while and don't make much progress, you can do this instead:

(b′) Suppose that R is a principal ideal domain. Show that R satisfies the ascending chain condition. If you can, give an example of a ring that doesn't satisfy the ascending chain condition.

If, on the other hand, you thought that this whole problem was too easy, see what you can do with this:

(c′) Under what conditions on the rings R and S and the homomorphism f is the function f^* a bijection?

II.3. Prove the following two statements (You may use the fact that $Z[\sqrt{-2}]$ is a UFD.)

(a) A positive prime integer p (i.e. prime in Z) is of the form $a^2 + 2b^2$ for some integers a, b if and only if p splits in $Z[\sqrt{-2}]$. (that is, it is *not* prime in $Z[\sqrt{-2}]$.)

(b) A prime integer p splits in $Z[\sqrt{-2}]$ if and only if 2 is a square in the field Z/p.

III. Fields, Galois theory.

III.1. Let ζ be a primitive 5th root of unity. Consider the polynomial $f(x) = x^5 - 3$ over the fields

(a) $\mathbf{Q}(\zeta)$,

(b) $\mathbf{R}$,

(c) $\mathbf{C}$.

For each of the cases (a)–(c), find the splitting field and the Galois group of $f(x)$. What is the order of the Galois group of $f(x)$ over the field $\mathbf{Q}$?

III.2. Suppose that F is a field and K is a field extension of F. Prove: if K is algebraic over F, then for every subring R of K which contains F (i.e., for every ring R with $F \subseteq R \subseteq K$), R must be a field. Is the converse true? Prove or disprove.

III.3. Write an essay on one of these topics:

- construction with straightedge and compass,
- the classification of finite fields,
- the main theorem of Galois theory,
- solvability by radicals via Galois theory.

IV. Modules.

IV.1 Give an example of each of the following:
(a) A module which is not torsion free. (Recall that an R-module M is called torsion-free if $\forall m \in M$, $\nexists x \in R$, $x \neq 0$, such that $xm = 0$.)
(b) A module which is torsion-free but not free.
(c) A module which is free.
(d) A ring R such that every finitely generated torsion-free R-module is free.

IV.2. Write an essay on one of these topics:
- the classification of finitely generated modules over a Euclidean domain (or I suppose the classification of finitely generated abelian groups would be okay),
- Jordan canonical form,
- The similarities and dissimilarities between modules and vector spaces.

V. Algebraic Geometry.

V.1. Consider the algebraic plane curve C defined by the equation $y^2 - x^3 + x^2 = 0$.
(a) Construct a parameterization of the algebraic plane curve C by mapping each value of t to a point of intersection of the line $y = tx$ and the curve $y^2 + x^3 - x^2$.
(b) Use this to show that the kernel of the homomorphism

$$\mathbf{C}[x, y] \to \mathbf{C}[t]$$

which is the identity on $\mathbf{C}$ and sends $x \mapsto 1 - t^2$ and $y \mapsto t^3 - t$ is the principal ideal generated by $y^2 + x^3 - x^2$?
(c) Show that the ring

$$R = \mathbf{C}[x, y]/(y^2 + x^3 - x^2)$$

is a domain and has a field of fractions isomorphic to $\mathbf{C}[t]$.