Math 662 **Spring 2014**
Final Exam **Drew Armstrong**

---

1. (Galois Connections) Let R be **any ring**. Given any set of points $S \subseteq K^n$ we define a set of polynomials $\mathcal{I}(S) := \{f \in R[x_1, \ldots, x_n] : f(\alpha) = 0 \text{ for all } \alpha \in S\}$, and given any set of polynomials $T \subseteq R[x_1, \ldots, x_n]$ we define a set of points $\mathcal{V}(T) := \{\alpha \in R^n : f(\alpha) = 0 \text{ for all } f \in T\}$.

(a) Given $S \subseteq R^n$, prove that $\mathcal{I}(S)$ is an ideal of $R[x_1, \ldots, x_n]$.

Proof. Given $f, g \in I(S)$ and $h \in R[x_1, \ldots, x_n]$ we have $(f - gh)(\alpha) = f(\alpha) - h(\alpha)g(\alpha) = 0 - h(\alpha) \cdot 0 = 0$. Hence $f - hg \in I(S)$. □

(b) Given $T \subseteq T' \subseteq R[x_1, \ldots, x_n]$, prove that $\mathcal{V}(T') \subseteq \mathcal{V}(T)$.

Proof. Let $\alpha \in \mathcal{V}(T')$ so that $f(\alpha) = 0$ for all $f \in T'$. Since $T \subseteq T'$ we also have $f(\alpha) = 0$ for all $f \in T$, hence $\alpha \in \mathcal{V}(T)$. □

(c) Given $T \subseteq R[x_1, \ldots, x_n]$, prove that $T \subseteq \mathcal{I}(\mathcal{V}(T))$.

Proof. Fix $f \in T$. We want to show that $f \in \mathcal{I}(\mathcal{V}(T))$, in other words that $f(\alpha) = 0$ for all $\alpha \in \mathcal{V}(T)$. But given any fixed $\alpha \in \mathcal{V}(T)$ we have $g(\alpha) = 0$ for all $g \in T$. In particular we have $f(\alpha) = 0$. Since this is true for all $\alpha \in \mathcal{V}(T)$ we conclude that $f \in \mathcal{I}(\mathcal{V}(T))$. □

(d) Given $T \subseteq R[x_1, \ldots, x_n]$, prove that $\mathcal{V}(\mathcal{I}(\mathcal{V}(T))) = \mathcal{V}(T)$. [Hint: Use (b) and (c). You can also assume that $S \subseteq \mathcal{V}(\mathcal{I}(S))$ for all $S \subseteq R^n$, the proof of which is similar to (c).]

Proof. By part (c) we have $T \subseteq \mathcal{I}(\mathcal{V}(T))$. Then applying $\mathcal{V}$ to both sides and using (b) gives $\mathcal{V}(\mathcal{I}(\mathcal{V}(T))) \subseteq \mathcal{V}(T)$. On the other hand we know that $S \subseteq \mathcal{V}(\mathcal{I}(S))$ for all sets $S \subseteq R^n$. Taking $S = \mathcal{V}(T)$ gives $\mathcal{V}(T) \subseteq \mathcal{V}(\mathcal{I}(\mathcal{V}(T)))$. □

(e) Consider $S \subseteq R^n$. If $S = \mathcal{V}(T)$ for some **set** $T \subseteq R[x_1, \ldots, x_n]$ prove that $S = \mathcal{V}(I)$ for some **ideal** $I \leq R[x_1, \ldots, x_n]$ containing T.

Proof. Let $I := \mathcal{I}(\mathcal{V}(T))$. Parts (a) and (c) say that I is an ideal containing T and part (d) says that $\mathcal{V}(T) = \mathcal{V}(\mathcal{I}(\mathcal{V}(T))) = \mathcal{V}(I)$. □

[Remark: We say that $V \in R^n$ is a variety if $V = \mathcal{V}(T)$ for some set of functions $T \subseteq R[x_1, \ldots, x_n]$. This problems says that we lose nothing by assuming T to be an ideal.]

2. (Systems of Equations) Let R be a **Noetherian ring**.

(a) State the definition of Noetherian ring.

Proof. We say that a ring is Noetherian if it satisfies either of the following two equivalent conditions:

- There is no infinite increasing chain of ideals.
- Every ideal is finitely generated.

□

(b) State the Hilbert Basis Theorem.

Proof. Let R be a ring. The Hilbert Basis Theorem says

$$R \text{ is Noetherian} \Longrightarrow R[x] \text{ is Noetherian.}$$

By induction we conclude that if R is Noetherian then so is $R[x_1, \ldots, x_n]$. $\square$

(c) Given polynomials $f_1, \ldots, f_k \in R[x_1, \ldots, x_n]$ we define the set

$$\mathcal{V}(f_1, \ldots, f_k) := \{\alpha \in R^n : f_i(\alpha) = 0 \text{ for all } 1 \leq i \leq k\}.$$

Prove that $\mathcal{V}(f_1, \ldots, f_k) = \mathcal{V}((f_1, \ldots, f_k))$ where $(f_1, \ldots, f_k) \leq R[x_1, \ldots, x_n]$ is the ideal generated by $f_1, \ldots, f_k$.

Proof. Since $\{f_1, \ldots, f_k\} \subseteq (f_1, \ldots, f_k)$, Problem 1(b) implies that $\mathcal{V}((f_1, \ldots, f_k)) \subseteq \mathcal{V}(f_1, \ldots, f_k)$. Conversely, suppose that $\alpha \in V(f_1, \ldots, f_k)$ so that $f_i(\alpha) = 0$ for all $1 \leq i \leq k$. Then consider any $f \in (f_1, \ldots, f_k)$ so that we have $f = g_1 f_1 + \cdots + g_k f_k$ for some $g_1, \ldots, g_k \in R[x_1, \ldots, x_n]$. It follows that $f(\alpha) = g_1(\alpha) f_1(\alpha) + \cdots + g_k(\alpha) f_k(\alpha) = g_1(\alpha) \cdot 0 + \cdots + g_k(\alpha) \cdot 0 = 0$, hence $f \in V((f_1, \ldots, f_k))$. $\square$

(d) Given any set $T \subseteq R[x_1, \ldots, x_n]$ prove that we have $\mathcal{V}(T) = \mathcal{V}(f_1, \ldots, f_k)$ for some **finite** set of polynomials $f_1, \ldots, f_k \in R[x_1, \ldots, x_n]$. [Hint: Problem 1.]

Proof. By Problem 1(e) we know that $\mathcal{V}(T) = \mathcal{V}(I)$ for some ideal $I \leq R[x_1, \ldots, x_n]$ and by the Hilbert Basis Theorem we know that $I = (f_1, \ldots, f_k)$ for some finite set of generators $f_1, \ldots, f_k \in R[x_1, \ldots, x_n]$. Then by part (c) we have

$$\mathcal{V}(T) = \mathcal{V}(I) = \mathcal{V}((f_1, \ldots, f_k)) = \mathcal{V}(f_1, \ldots, f_k).$$

$\square$

[Remark: When working over a Noetherian ring, Problems 1 and 2 say that a variety is the same thing as the solution set of a finite system of polynomial equations.]

3. (The Radical of an Ideal) Let R be **any ring**. Given an ideal $I \leq R[x_1, \ldots, x_n]$ we define its radical $\sqrt{I} := \{f \in R[x_1, \ldots, x_n] : f^n \in I \text{ for some } n\}$. We say that $I \leq R[x_1, \ldots, x_n]$ is a"radical ideal" if $I = \sqrt{I}$.

(a) Given an ideal $I \leq R[x_1, \ldots, x_n]$, prove that the set $\sqrt{I}$ is an ideal. [Hint: Given $f, g \in \sqrt{I}$ and $r \in R[x_1, \ldots, x_n]$ prove that $(f - rg)^N \in I$ for some N. Which N?]

Proof. Consider $f, g \in \sqrt{I}$ and $r \in R[x_1, \ldots, x_n]$. Since $f, g \in \sqrt{I}$ there exist m, n such that $f^m \in I$ and $g^n \in I$. Then we have

$$(f - rg)^{m+n} = \sum_{i+j=m+n} \binom{i+j}{i} f^i (-r)^j g^j.$$

Note that $i + j = m + n$ implies that $i \geq m$ (hence $f^i \in I$) or $j \geq n$ (hence $g^j \in I$). Thus every term in the above equation is in I, hence $(f - rg)^{m+n} \in I$. We conclude that $f - rg \in \sqrt{I}$. $\square$

(b) Given an ideal $I \leq R[x_1, \ldots, x_n]$, prove that $I \leq \sqrt{I}$ and hence $\mathcal{V}(\sqrt{I}) \subseteq \mathcal{V}(I)$.

Proof. Let $f \in I$. Then since $f^1 \in I$ we have $f \in \sqrt{I}$. We conclude that $I \leq \sqrt{I}$ and then Problem 1(b) implies that $\mathcal{V}(\sqrt{I}) \subseteq \mathcal{V}(I)$. $\square$

(c) If R is **reduced** (i.e. contains no nilpotent elements), prove that $\mathcal{V}(I) \subseteq \mathcal{V}(\sqrt{I})$.

Proof. Now suppose R is reduced and fix $\alpha \in \mathcal{V}(I)$ so that $f(\alpha) = 0$ for all $f \in I$. We want to show that $f(\alpha) = 0$ for all $f \in \sqrt{I}$. But if $f \in \sqrt{I}$ then we have $f^m \in I$ for some m and then $f(\alpha)^m = 0$. Since R is reduced this implies that $f(\alpha) = 0$. $\square$

(d) Following part (c), conclude that $\sqrt{I} \subseteq \mathcal{I}(\mathcal{V}(I))$. [Hint: Problem 1(c).]

Proof. By parts (b) and (c) we know that $\mathcal{V}(\sqrt{I}) = \mathcal{V}(I)$. Then Problem 1(c) implies that $\sqrt{I} \subseteq \mathcal{I}(\mathcal{V}(\sqrt{I})) = \mathcal{I}(\mathcal{V}(I))$. $\square$

[Remark: When working over a reduced ring, Problem 3 says that a variety is the same as the set of zeroes of a radical ideal. This is stronger than the conclusion of Problem 1(e).]

4. (Weak Nullstellensatz) Let K be **any field**. Given any point $\alpha \in K^n$ we consider the ideal of functions that vanish at α:

$$\mathfrak{m}_\alpha := \mathcal{I}(\{\alpha\}) = \{f \in K[x_1, \ldots, x_n] : f(\alpha) = 0\}.$$

(a) Given $\alpha \in K^n$, prove that $\mathfrak{m}_\alpha$ is a **maximal** ideal. [Hint: It's the kernel of something.]

Proof. Consider the evaluation homomorphism $\mathsf{ev}_\alpha : K[x_1, \ldots, x_n] \to K$. This map is surjective because given any $\beta \in K$ we can apply ev_α to the constant function $\beta \in K[x_1, \ldots, x_n]$ to get $\mathsf{ev}_\alpha(\beta) = \beta$. Note that the kernel is $\mathfrak{m}_\alpha = \ker(\mathsf{ev}_\alpha)$. By the First Isomorphism Theorem we know that $K[x_1, \ldots, x_n]/\mathfrak{m}_\alpha \approx K$. Since K is a field this implies that $\mathfrak{m}_\alpha < K[x_1, \ldots, x_n]$ is a maximal ideal. $\square$

(b) If $\alpha = (\alpha_1, \ldots, \alpha_n) \in K^n$, prove that $m_\alpha = (x_1 - \alpha_1, \ldots, x_n - \alpha_n)$. [Hint: Consider $f(x_1, \ldots, x_n)$ such that $f(\alpha) = 0$. First divide f by $(x_1 - \alpha_1)$, then divide the remainder by $(x_2 - \alpha_2)$, then ...]

Proof. Consider $f \in K[x_1, \ldots, x_n]$. Divide f by $(x_1 - \alpha_1)$ in the ring $K[x_1, \ldots, x_n]$ to get $f = q_1(x_1 - \alpha_1) + r_1$ where r_1 is in the subring $K[x_2, \ldots, x_n]$. Then divide r_1 by $(x_2 - \alpha_2)$ in the subring $K[x_2, \ldots, x_n]$ to get $f = q_1(x_1 - \alpha_1) + q_2(x_2 - \alpha_2) + r_2$ where r_2 is in the subring $r_2 \in K[x_3, \ldots, x_n]$. Continuing in this way we get

$$f = q_1(x_1 - \alpha_1) + \cdots + q_n(x_n - \alpha_n) + r$$

where $r \in K$ is a constant. Finally, evaluating at α gives

$$0 = f(\alpha) = q_1(\alpha) \cdot + \cdots + q_n(\alpha) \cdot + r = r.$$

and we conclude that $f \in (x_1 - \alpha_1, \ldots, x_n - \alpha_n)$. Conversely, every f in this ideal satisfies $f(\alpha) = 0$, hence $f \in \mathfrak{m}_\alpha$. $\square$

(c) If **every** maximal ideal of $K[x_1, \ldots, x_n]$ has the form $\mathfrak{m}_\alpha$ for some $\alpha \in K^n$, prove that for all ideals I we have $I \neq K[x_1, \ldots, x_n] \implies \mathcal{V}(I) \neq \emptyset$. [Hint: If $I \neq K[x_1, \ldots, x_n]$ then you can assume (Zorn) that I is contained in a maximal ideal.]

Proof. Suppose that every maximal ideal of $K[x_1, \ldots, x_n]$ has the form $\mathfrak{m}_\alpha$ for some $\alpha \in K^n$ and assume that $I \neq K[x_1, \ldots, x_n]$. By Zorn's Lemma, I is contained in a maximal ideal $\mathfrak{m}_\alpha = I(\{\alpha\})$. Then by Problem 1 we have $\{\alpha\} \subseteq \mathcal{V}(\mathcal{I}(\{\alpha\})) \subseteq \mathcal{V}(I)$, hence $\mathcal{V}(I) \neq \emptyset$. $\square$

[Remark: In (c) we **assumed** that every maximal ideal of $K[x_1, \ldots, x_n]$ has the form $\mathfrak{m}_\alpha$. If K is algebraically closed then this assumption is true, but (as you know) it is not easy to prove.]

5. (Strong Nullstellensatz) Let K be an **algebraically closed field**. In this case Hilbert proved that $\sqrt{I} = \mathcal{I}(\mathcal{V}(I))$ (compare Problem 3(d)). Please don't prove this!! You will apply Hilbert's result to prove something called "Study's Lemma".

(a) Use a small number of words to tell me why $K[x_1, \ldots, x_n]$ is a UFD.

Proof. Here is an acceptable solution: say "Gauss' Lemma". You can of course go into more detail at your own risk. $\square$

(b) Prove that every irreducible element in a UFD is prime. [Hint: If $a|bc$ then we have $ak = bc$. Factor both sides into irreducibles and compare.]

Proof. Suppose that we have $ak = bc$ in a UFD and suppose that a irreducible. Factor k, b, and c into irreducibles and compare the irreducible factorization on both sides of the equation $ak = bc$. Since a is an irreducible factor on the left it must be associate to some irreducible factor on the right. That is, a must be associate to an irreducible factor of b or c. But this implies that $a|b$ or $a|c$. $\square$

(c) Given a polynomial $f \in K[x_1, \ldots, x_n]$ we define the "hypersurface"

$$\mathcal{V}(f) := \mathcal{V}((f)) = \{\alpha \in K^n : f(\alpha) = 0\}.$$

Consider $f, g \in K[x_1, \ldots, x_n]$ such that f divides g. Prove that $\mathcal{V}(f) \subseteq \mathcal{V}(g)$.

Proof. Suppose that $f|g$, say $g = fh$. Then for all $\alpha \in V(f)$ we have $g(\alpha) = f(\alpha)h(\alpha) = 0 \cdot h(\alpha) = 0$, hence $\alpha \in V(g)$. $\square$

(d) **(Study's Lemma)** Consider $f, g \in K[x_1, \ldots, x_n]$ such that f is **irreducible**. Prove that if $\mathcal{V}(f) \subseteq \mathcal{V}(g)$ then f divides g. [Hint: Show that $g \in \mathcal{I}(\mathcal{V}(f))$. If f divides g^n use (a) and (b) to show that f divides g.]

Proof. Consider $f, g \in K[x_1, \ldots, x_n]$ with f irreducible, and suppose that $V(f) \subseteq V(g)$. Then by Problem 1 we have $g \in (g) \subseteq \mathcal{I}(\mathcal{V}(g)) \subseteq \mathcal{I}(\mathcal{V}(f))$. By Hilbert's Nullstellensatz this implies that $g \in \sqrt{(f)}$ and hence $g^n \in (f)$ for some n. In other words, $f|g^n$. Since f an irreducible element of the UFD $K[x_1, \ldots, x_n]$ we know that f is prime by part (b). Hence $f|g^n \Rightarrow f|g$. $\square$

[Remark: Study's Lemma says the following. Let K be algebraically closed. Then any polynomial that vanishes on a hypersurface is divisible by the "minimal polynomial" of the hypersurface.]