Fundamental Concepts and Theorems for the Final exam

1. The ideal $I(S) \subset \mathbb{K}[x_1, \ldots, x_n]$ of a set $S \subset \mathbb{K}^n$.
2. The variety $V(I) \subset \mathbb{K}^n$ of an ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$.
3. Parametrization and implicitization
4. Zariski closure
5. Monomial orders
6. Multivariable division algorithm
7. Dickson's Lemma
8. Gröbner basis of an ideal
9. Hilbert Basis Theorem
10. Ascending chain condition and Descending chain condition
11. Buchberger's criterion and Buchberger's algorithm for Gröbner bases
12. Elimination ideals
13. Ideal product, sum, intersection, quotient, and saturation: know how to compute these
14. Hilbert's weak Nullstellensatz, Hilbert's Nullstellensatz, Hilbert's Strong Nullstellensatz
15. Radical of an ideal
16. Maximal, prime, primary, and irreducible ideals
17. Prime decomposition of radical ideals
18. Primary decomposition, associated primes, minimal primes, and embedded primes
19. Arithmetic of ideals and varieties
20. Coordinate ring of a variety and affine Hilbert function basics

Practice Problems for Final Exam

Use these problems to guide your study for the final exam.

1. Use the Euclidean algorithm to do the following.
   (a) Find $\gcd(112, 84)$ and find integers a, b so that $\gcd(112, 84) = a \cdot 84 + b \cdot 112$.
   (b) Find h so that $\langle x^3 + x + 1, x^2 + 2x + 3\rangle = \langle h\rangle$.
   (c) Find h so that $\langle x^3 - x, x^2 + 3x + 2\rangle = \langle h\rangle$.
   (d) Find h so that $\langle x^4 - x, x^5 - x, x^6 - x\rangle = \langle h\rangle$.

2. Find the row reduced echelon form of the matrix M below over $\mathbb{Q}(x)$ and over $\mathbb{F}_2[x]/\langle x^3+x+1\rangle$.

$$\begin{bmatrix} 1 & x & x^2 \\ 0 & 1+x & 1+x^2 \end{bmatrix}$$

3. Prove the following equalities of ideals in $\mathbb{Q}[x, y]$:

   (a) $\langle x+y, x-y\rangle = \langle x, y\rangle$

   (b) $\langle x+xy, y+xy, x^2, y^2\rangle = \langle x, y\rangle$

   (c) $\langle y^2-xz, xy-z, x^2-y\rangle = \langle y-x^2, z-x^3\rangle$

4. A *radical* ideal is an ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$ satisfying that if $f^k \in I$ for some integer k, then $f \in I$.

   (a) Prove that $I(V)$ is a radical ideal for any set $V \subset \mathbb{K}^n$.

   (b) Prove that $\langle x^2, y^2\rangle$ is not a radical ideal, so it is not the ideal of any set.

5. Suppose $p = (2, 3) \in \mathbb{R}^2$.

   (a) Prove that $I(p) = \langle x-2, y-3\rangle$, and that the polynomials $x-2, y-3$ are a Gröbner basis for $I(p)$ with respect to any term order.

   (b) Find the remainder under division of $F = x^2+y^2$ by $\{x-2, y-3\}$.

6. If $V \subset \mathbb{K}^3$ is the curve parametrized by $x = t, y = t^3, z = t^4$, prove that $I(V) = \langle y-x^3, z-x^4\rangle$.

7. For any ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$ and any fixed monomial order $\prec$ on $\mathbb{K}[x_1, \ldots, x_n]$, prove that the monomials of $\mathbb{K}[x_1, \ldots, x_n]$ which are not in the lead term ideal $\mathrm{LT}_\prec(I)$ form a basis for $\mathbb{K}[x_1, \ldots, x_n]/I$ as a $\mathbb{K}$-vector space. (See Section 5.3 of Cox-Little-O'Shea if you get stuck.)

8. If $X = \{p_1, \ldots, p_k\} \subset \mathbb{K}^2$ is a finite set of points and $S = \mathbb{K}[x, y]$ is the polynomial ring in two variables, show that $S/I(X)$ is a finite dimensional vector space.

9. Let $I = \langle x^2+2xy+3y^2, x^2+6y^2, x^2+xy+y^2\rangle$. We will consider the coefficients of I as coming from two different fields.

   (a) Show that $I \subset \mathbb{F}_{11}[x, y]$ is a monomial ideal.

   (b) Show that $I \subset \mathbb{F}_7[x, y]$ is not a monomial ideal.

10. (Singularities of some plane curves)

    (a) Let $f = y^2-x^3-x^2$. Show that the singular locus of $f = 0$ is the point $(0, 0)$ by explicitly showing that $\langle f, \frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}\rangle = \langle x, y\rangle$.

    (b) If $f = y^k - f(x)$, where $k \geq 2$ is an integer and $f(x)$ is a polynomial in x, prove that the curve $V(f)$ is smooth (non-singular) if and only if $f(x)$ does not have multiple roots. If $V(f)$ is singular, prove that the singular points all have the form $(r, 0)$ where r is a multiple root of $f(x)$.

11. If $I \subset \mathbb{K}[x_1, \ldots, x_n]$ is an ideal and $F \in \mathbb{K}[x_1, \ldots, x_n]$ is a polynomial, prove that $(I : F) \cdot F = I \cap \langle F\rangle$.

12. If $I = \langle f_1, \ldots, f_k \rangle \subset \mathbb{K}[x_1, \ldots, x_n]$ is an ideal and $F \in \mathbb{K}[x_1, \ldots, x_n]$ is a polynomial, prove that $\langle f_1, \ldots, f_k, 1 - yF \rangle \cap \mathbb{K}[x_1, \ldots, x_n] = I : F^\infty$.

13. If I, J are ideals in $\mathbb{K}[x_1, \ldots, x_n]$, prove that $I \cap J = (tI + (1-t)J) \cap \mathbb{K}[x_1, \ldots, x_n]$ (the proof of this can be found in Section 4.3 of Cox-Little-O'Shea).

14. Suppose $I = \langle m_1, m_2, \ldots, m_k \rangle$ is a monomial ideal generated by the monomials $m_1, \ldots, m_k \in \mathbb{K}[x_1, \ldots, x_n]$ and m is another monomial in $\mathbb{K}[x_1, \ldots, x_n]$.

    (a) Prove that

    $$\langle m_1, \ldots, m_k \rangle : m = \langle \mathrm{LCM}(m_1, m)/m, \ldots, \mathrm{LCM}(m_k, m)/m \rangle,$$

    where $\mathrm{LCM}(m_i, m)$ denotes the least common multiple of m_i and m.

    (b) Compute a *minimal* set of generators for $\langle x^2yz^2, xy^2z^3, y^3z^4 \rangle : xyz$.

15. (Primary ideal basics)

    (a) Show that the radical of a primary ideal is a prime ideal. If I is primary and $\sqrt{I} = \mathfrak{p}$, we say I is $\mathfrak{p}$-primary.

    (b) Show that if I and J are $\mathfrak{p}$-primary then $I \cap J$ is $\mathfrak{p}$-primary.

16. (Radical ideal basics)

    (a) Show that if I is a radical ideal and if J is any ideal then $I : J$ is a radical ideal.

    (b) Show that $\sqrt{I : J^\infty} = \sqrt{I} : J$

    (c) Show that $\sqrt{IJ} = \sqrt{I \cap J}$

    (d) A monomial is *squarefree* if it is not divisible by the square of any variable. Show that a monomial ideal is radical $\iff$ the minimal generators of I are squarefree.

    (e) Show that if $I \subseteq \sqrt{J}$ then there exists an m such that $I^m \subseteq J$

17. Find the Zariski closure of the following sets:

    (a) $\{(x, y) \in \mathbb{R}^2 : x \geq 0 \text{ and } y \geq 0\}$

    (b) The boundary of the first quadrant in $\mathbb{R}^2 = \{(x, 0) : x \geq 0\} \cup \{(0, y) : y \geq 0\}$.

    (c) $\mathbb{R} \setminus 0$

    (d) The set $\{(x, y) : x^2 + y^2 \leq 1\}$.

    (e) The set $\{(p, 0) : p \text{ is a prime number } \} \subset \mathbb{R}^2$.

18. (Weak Nullstellensatz and maximal ideals) Consider the following two statements in the polynomial ring $\mathbb{K}[x_1, \ldots, x_n]$ over an algebraically closed field $\mathbb{K}$.

    (a) (Weak Nullstellensatz) $V(I) \neq \emptyset \Leftrightarrow I = \mathbb{K}[x_1, \ldots, x_n]$.

    (b) Every maximal ideal $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ has the form $I = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$ for some $a_1, \ldots, a_n \in \mathbb{K}$.

In class we showed 18a⇒18b. Prove that 18b⇒18a. In other words, prove that the description of maximal ideals in 18b is equivalent to the weak Nullstellensatz.

19. (Exploring maximal ideals) Suppose $f_1(x), \ldots, f_n(x) \in \mathbb{K}[x]$. In the polynomial ring $\mathbb{K}[x_1, \ldots, x_n]$ (where $\mathbb{K}$ is any field), consider the ideal

$$I = \langle f_1(x_1), x_2 - f_2(x_1), \ldots, x_n - f_n(x_1) \rangle$$

    (a) Show that every $f \in \mathbb{K}[x_1, \ldots, x_n]$ can be written uniquely as $f = q + r$ where $q \in I$ and $r \in \mathbb{K}[x_1]$ with either $r = 0$ or $\deg(r) < \deg(f_1)$. Hint: use Lex order with x_1 the smallest variable (instead of the largest).

    (b) Use part (a) to prove that $\mathbb{K}[x_1, \ldots, x_n]/I \cong \mathbb{K}[x]/\langle f_1(x) \rangle$.

    (c) Prove that the following are equivalent:

        i. I is prime.

        ii. I is maximal.

        iii. $f_1(x)$ is irreducible.

    (d) Prove that I is radical if and only if $f_1(x)$ is squarefree.

20. (Squarefree lead term ideals) There is a general philosophy that good properties of an ideal I cannot be *gained* when passing to the lead term ideal $\langle \mathrm{LT}(I) \rangle$, only *lost*. In this problem you will prove one instance of this philosophy. Suppose $I \subset \mathbb{K}[x_1, \ldots, x_n]$ is an ideal and $G = \{g_1, \ldots, g_r\}$ is a Gröbner basis for I satisfying that $\mathrm{LT}(g_i)$ is squarefree for $i = 1, \ldots, r$.

    (a) If $f \in \sqrt{I}$, prove that $\mathrm{LT}(f)$ is divisible by $\mathrm{LT}(g_i)$ for some $g_i \in G$. Hint: $f^r \in I$ for some r.

    (b) Prove that I is radical. Hint: show that G is a Gröbner basis for $\sqrt{I}$.

    (c) From (a) and (b), conclude that if $\langle \mathrm{LT}(I) \rangle$ is radical, then I is radical.

    (d) Find an example to show that if I is radical, it is not necessarily true that $\langle \mathrm{LT}(I) \rangle$ is radical.

21. (Empty varieties) Find examples of ideals I, J in $\mathbb{R}[x, y]$ so that $V(I) = V(J) = \emptyset$.

22. (Prime ideal basics)

    (a) Show that an ideal P is prime if and only if for any two ideals I, J, $IJ \subseteq P \Rightarrow I \subseteq P$ or $J \subseteq P$.

    (b) Show that if $I_1, \ldots, I_k$ are ideals and P is prime, then $\cap_{i=1}^k I_i \subseteq P$ if and only if $I_j \subseteq P$ for some j.

    (c) (Prime avoidance) If $P_1, \ldots, P_k$ are prime ideals and $I \subseteq \cup_{i=1}^k P_i$ then $I \subseteq P_j$ for some j. Hint: use induction on k.

23. (Affine Hilbert Function) The ideal $I = \langle y^2 - y, x^3 - 3x^2 + 2x \rangle$ is the ideal of six points in $\mathbb{R}^2$, and its generators form a Gröbner basis for I with respect to graded reverse lexicographic order. Compute the affine Hilbert function of I and explain its geometric significance.