Name: _____

This is an open book/library/notes/web take-home exam, but you are not to collaborate. Your instructor is the only human source you are allowed to consult. Be sure to cite all outside sources you use.

Please submit your solution to each problem on a **separate page**.

This exam is due by **email** (cberkesc@umn.edu) at **10:00 a.m. on Thursday, May 9, 2018**. Your solutions do not need to be typed. You are permitted to send scans of handwritten work.

Problem	1	2	3	4	5	6	Total
Points	15	20	20	10	25	10	100
Score							

1. Let R be an integral domain with quotient field F, and let $p(x)$ be a monic polynomial in $R[x]$. Assume that $p(x) = a(x)b(x)$, and $a(x)$ and $b(x)$ are monic polynomials in $F[x]$ of degree smaller than $p(x)$. Prove that if $a(x) \notin R[x]$, then R is not a UFD. Deduce that $\mathbb{Z}[2\sqrt{2}]$ is not a UFD.

2. Let $c(n)$, $r(n)$, $q(n)$, respectively, be the number of irreducible factors of $x^n - 1$ when considered as elements of $\mathbb{C}[x]$, $\mathbb{R}[x]$, $\mathbb{Q}[x]$, respectively. Let A be any matrix in $\mathbb{Q}^{n\times n}$ having $\det(xI - A) = x^n - 1$. (For example, one can take A to be the permutation matrix representing an n-cycle in the symmetric group S_n.)
   (a) Write down $c(n)$, $r(n)$, $q(n)$ as functions of n in the simplest forms that you can.
   (b) Regarding $V = \mathbb{R}^n$ as an $\mathbb{R}[x]$-module with x acting on V as multiplication by the matrix A, how many $\mathbb{R}[x]$-submodules $W \subset V$ will there be, including both $\{0\}$ and V itself among them?
   (c) Answer the same question as in (b), replacing $\mathbb{R}$ with $\mathbb{Q}$, so $V = \mathbb{Q}^n$ is a $\mathbb{Q}[x]$-module in which x acts as multiplication by A.

3. (a) (10 points) Prove that $x^4 + x^3 + x^2 + x + 1$ is irreducible in $\mathbb{F}_{13}[x]$, where $\mathbb{F}_{13}$ is the finite field with 13 elements.
   (b) (15 points) Consider the factorization of $f(x) = x^{17^2} - x$ into irreducible polynomials in $\mathbb{F}_{17}[x]$. For each possible degree $d = 1, 2, 3, \ldots$, how many irreducible factors will there be of degree d?

4. How many intermediate fields lie strictly between $\mathbb{Q}$ and $\mathbb{Q}(\zeta_{19})$, where ζ_{19} is a primitive 19th root of unity? You need not describe them all explicitly, but you must explain your answer.

5. Let $K = \mathbb{Q}(\sqrt[n]{a})$, where $a \in \mathbb{Q}$ and $a > 0$, and suppose that $[K : \mathbb{Q}] = n$ (so $x^n - a$ is irreducible).
   (a) Let E be any subfield of K and let $[E : \mathbb{Q}] = d$. Prove that $E = \mathbb{Q}(\sqrt[d]{a})$.
   [Hint: Consider $N_{K/E}(\sqrt[n]{a}) \in E$.]
   (b) Prove that if n is odd, then K has no nontrivial subfields that are Galois over $\mathbb{Q}$, and if n is even, then the only nontrivial subfield of K that is Galois over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{a})$.
   (c) Let L be the Galois closure of K. Prove that $[L : \mathbb{Q}] = n\varphi(n)$ or $\frac{1}{2}n\varphi(n)$.
   [Hint: Note that $\mathbb{Q}(\zeta_n) \cap K$ is a Galois extension of $\mathbb{Q}$.]

6. Using the lexicographic ordering defined by $x > y$ in $F[x, y]$, for some field F, show that $\{x - y^3, y^5 - y^6\}$ is the reduced Gröbner basis for the ideal $I = \langle x - y^3, -x^2 + xy^2\rangle$.