Mathematics 100B Final Exam Practice Problems

Instructions: The Final Exam is Wednesday March 22, 11:30am-2:30pm. It will be in Center 214, the room where lecture has been held all term. No notes or calculators are allowed. This practice worksheet is to help you study for the final. The final exam will cover the entire course. Note that inclusion of a topic on this sheet does not guarantee that a similar problem will appear on the exam, nor does exclusion of a topic from this sheet imply that that topic will not be on the exam.

1. True or False:

   (a) A ring R is an integral domain if and only if there exists a field F such that $R \subseteq F$.

   (b) There exists a ring of characteristic 3 and size 300.

   (c) Recall that an a complex number α is said to be *algebraic* (over $\mathbf{Q}$) if there exists a nonzero polynomial $f(x) \in \mathbf{Q}[x]$ such that $f(\alpha) = 0$. If $\alpha \in \mathbf{C}$ is algebraic over $\mathbf{Q}(\sqrt{2})$, then α is algebraic over $\mathbf{Q}$.

   (d) Suppose R is a UFD and $p \in R$ is nonzero and irreducible. Then $R/(p)$ is a field.

   (e) Suppose $\phi : F \to S$ is a nonzero map from a field to a ring. Then ϕ is injective.

   (f) For all prime numbers $p \in \mathbf{Z}$, $\mathbf{Z}[i]/(p)$ is a field.

   (g) Suppose F is a field, and $f(x), g(x) \in F[x]$ are nonzero polynomials with no common factor in $F[x]$. Then there exists a polynomial $p(x) \in F[x]$ such that $p(x)$ is divisible by $g(x)$ and $p(x)$ is 1 more than a multiple of $f(x)$.

   (h) There exists irreducible polynomials in $\mathbf{R}[x]$ of arbitrarily large degree.

   (i) There exists irreducible polynomials in $\mathbf{F}_5[x]$ of arbitrarily large degree.

   (j) There exists a subfield E of $\mathbf{C}$, so that $E \supseteq \mathbf{Q}(\sqrt{2})$ and $[E : \mathbf{Q}] = 7$.

   (k) A subset I of a ring R is an ideal if and only if there exists a ring S and a ring homomorphism $\phi : R \to S$ such that $I = \ker(\phi)$.

   (l) If R is a UFD and $P \subseteq R$ a prime ideal, then R/P is a UFD.

   (m) Let α be a real root of $x^5 - 7$. Then α is a constructible number.

   (n) If $\varphi : R \to S$ is a ring homomorphism, $Q \subseteq S$ is a prime ideal, and $P = \varphi^{-1}(Q) = \{r \in R : \varphi(r) \in Q\}$, then P is a prime ideal of R.

2. Suppose n is a positive integer. Let $\sigma(n)$ denote the number of positive integers d such that d divides n. Prove that $\mathbf{Z}/n\mathbf{Z}$ has $\sigma(n)$ ideals.

3. How many ideals does the ring $\mathbf{F}_3 \times \mathbf{Z}/49\mathbf{Z}$ have? Write down a ring S with $3 \times 49 = 147$ elements that has exactly 4 ideals.

4. Suppose F is a field, R is a ring, and $F \subseteq R$. Suppose moreover that R is finite-dimensional as an F vector space. If $\alpha \in R$, let $T_\alpha : R \to R$ be the F-linear map given by $T_\alpha(x) = \alpha x$. Let $N_{R/F}(\alpha)$ denote the determinant of T_α; it is called the norm of α. Prove that α is in $R^\times$ if and only if $N_{R/F}(\alpha) \in F^\times$.

5. Let $F = \mathbf{Q}$, $R = \mathbf{Q}[\sqrt{d}]$. If $x = a + b\sqrt{d} \in R$ with $a, b \in \mathbf{Q}$, what is $N_{R/F}(x)$?

6. Write down a polynomial in $\mathbf{Z}[x]$ of degree 100 that is irreducible in $\mathbf{Q}[x]$.

7. Denote by $\varphi : \mathbf{Z}[x] \to \mathbf{Z}[\sqrt{3}]$ the ring homomorphism that sends x to $1+\sqrt{3}$. Find a polynomial $f(x) \in \mathbf{Z}[x]$ such that $\ker(\varphi) = (f(x))$.

8. Suppose $d > 1$ is a positive integer. Let $R = \mathbf{Z}[\sqrt{-d}]$. Prove that $R^\times = \{\pm 1\}$.

9. Let $S = \mathbf{Z}[\sqrt{3}]$. Prove that the group of units $S^\times$ is infinite.

10. Give an example of a maximal ideal in the polynomial ring $\mathbf{Z}[x, y, z]$.

11. Prove that there does not exist a surjective ring homomorphism $\varphi : \mathbf{Z}[x_1, \ldots, x_n] \to \mathbf{Q}$.

12. Let $R = \mathbf{Z}[x]/(x^3)$. Does there exist integral domains $S_1, S_2, \ldots, S_n$ and an injective ring homomorphism $\varphi : R \to S_1 \times S_2 \times \cdots \times S_n$?

13. Suppose $n \in \mathbf{Z}$ is not a cube, i.e., there does not exist an integer m so that $n = m^3$. Prove that $x^3 - n$ is irreducible in $\mathbf{Q}[x]$.

14. Recall that an element x of a ring R is said to be *nilpotent* if there exists a positive integer N so that $x^N = 0$. A ring R is said to be *reduced* if the only nilpotent element of R is 0. Now, suppose F is a field, and $f(x) \in F[x]$ factors into irreducibles as $f(x) = p_1(x)^{e_1} \cdots p_m(x)^{e_m}$. Prove that $F[x]/(f(x))$ is reduced if and only if all $e_j = 1$.

15. Let $F \subseteq E$ be fields, and $f(x) \in F[x]$ a monic polynomial of degree n. Assume that in $E[x]$, $f(x) = (x-\alpha_1)\cdots(x-\alpha_n)$ with $\alpha_j \neq \alpha_k$ if $j \neq k$. Let $K = F(\alpha_1, \ldots, \alpha_n)$. Prove that the degree $[K : F] \leq n!$. **Hint**: Set $F_j = F(\alpha_1, \alpha_2, \ldots, \alpha_j)$ and let $f_{j+1}(x) = (x-\alpha_{j+1})(x-\alpha_{j+2})\cdots(x-\alpha_n)$. Prove that $f_{j+1} \in F_j[x]$ so $[F_{j+1} : F_j] \leq n-j$.

16. Let α be a root of the polynomial $x^3 + 2x^2 + x + 1$ in $\mathbf{C}$ and $\beta \in \mathbf{C}$ a root of the polynomial $x^4 + 7x^2 - 7$. What is the degree of $\mathbf{Q}(\alpha, \beta)$ over $\mathbf{Q}$?

17. Suppose V_1, V_2, V_3 are three vector spaces over a field F, $\dim(V_1) = \dim(V_3) = 4$ and $\dim(V_2) = 3$. Let $T_1 : V_1 \to V_2$ and $T_2 : V_2 \to V_3$ be linear maps. Can $T_2 \circ T_1 : V_1 \to V_3$ be surjective?

18. Suppose E is a finite extension of the complex numbers $\mathbf{C}$. Prove that $E = \mathbf{C}$.

19. Let n_1, n_2 be non-negative integers, and let $S = \mathbf{R} \times \cdots \times \mathbf{R} \times \mathbf{C} \times \cdots \times \mathbf{C}$, where there are n_1 copies of $\mathbf{R}$ and n_2 copies of $\mathbf{C}$. Embed $\mathbf{R}$ into S as $x \mapsto (x, x, \ldots, x)$. Prove that there exists an element $\gamma \in S$ so that $S = \mathbf{R}[\gamma]$.

20. Prove the following corollary of the Nullstellansatz (see below). Let M be a maximal ideal of $R := \mathbf{Z}[x_1, \ldots, x_n]$. Then R/M is a finite field. **Hint**: Set $R' = \mathbf{Q}[x_1, \ldots, x_n]$. Let $K = R/M$; denote by $\varphi : R \to K$ the quotient map. First, rule out the possibility that $char(K) = 0$ as follows. If $char(K) = 0$, then there is a surjection $\psi : R' \to K$ defined as $\psi(x_j) = \varphi(x_j)$, so K is a finite extension of $\mathbf{Q}$ (by the Nullstellansatz). Let $1 = w_0, w_1, \ldots, w_d$ be a basis of K over $\mathbf{Q}$. Mimic the argument of part 2 of the proof below to see that φ cannot be surjective. Thus $char(K) = p$ for some some prime number p. Consequently, $p \in M$, so $R/M \simeq \mathbf{F}_p[x_1, \ldots, x_n]/M'$ for a maximal ideal M' of $\mathbf{F}_p[x_1, \ldots, x_n]$. Again by the Nullstellansatz, conclude that K is a finite field.

The following statement is a famous theorem, called the **Nullstellansatz**.
Theorem: *Suppose k is a field, and M is a maximal ideal in $k[x_1, \ldots, x_n]$. Set $K = k[x_1, \ldots, x_n]/M$. Then K is a finite extension of k.*

We did not cover this theorem in class, so you are not responsible for it. However, you might be curious what sort of fields can you obtain by quotienting out maximal ideals in polynomial rings. Moreover, the proof of the Nullstenansatz is a good review of lots of the ideas we did discuss in class. In this problem, you work through a proof of this statement.

1. Recall that $k(t)$ denotes the fraction field of the polynomial ring $k[t]$. Prove that there is no surjective ring homomorphism $\varphi : k[x_1, \ldots, x_n] \to k(t)$. **Hint**: Write $\varphi(x_i) = f_i(t)/g_i(t)$ for polynomials $f_i, g_i \in k[t]$. There are an infinite number of irreducible polynomials of $k[t]$, so choose an irreducible polynomial $p(t)$ that does not divide any of the $g_i(t)$. Prove that $1/p(t)$ is not in the image of φ.

2. Generalize the previous part as follows: Suppose K is a field, which is a finite extension of $k(t)$. Prove that there is not a surjective ring homomorphism $\varphi : k[x_1, \ldots, x_n] \to K$. **Hint**: Let $1 = w_0, w_1, \ldots, w_d$ be a basis of K over $k(t)$. For every $j, k \in \{0, 1, \ldots, d\}$, we have $w_j w_k = \sum_r \frac{u^r_{jk}(t)}{v^r_{jk}(t)} w_r$ for some polynomials $u^r_{jk}(t), v^r_{jk}(t) \in k[t]$. Now suppose $\varphi(x_i) = \sum_r \frac{f^r_i(t)}{g^r_i(t)} w_r$ for polynomials $f^r_i(t), g^r_i(t) \in k[t]$. Then if $p(t)$ is irreducible and does not divide any $g^r_i(t)$ or any $v^r_{jk}(t)$, $\frac{1}{p(t)} w_0$ is not in the image of φ.

3. Suppose K is a field and $\varphi : k[x_1, \ldots, x_n] \to K$ is a surjective ring homomorphism. Suppose also (for the sake of contradiction) that K is not a finite extension of k. Set $K_0 = \varphi(k) \simeq k$, and let K_j be the fraction field of $\varphi(k[x_1, \ldots, x_j])$ inside K. Prove that there exists an index m so that

   - $K_{m+1} \simeq K_m(t)$ and
   - K is a finite extension of K_{m+1}.

   Hint: If $\varphi(x_{j+1})$ is algebraic over K_j, then K_{j+1} is finite over K_j. If this happens for every j, then K/k is finite. Thus there is some index j so that $K_{j+1} \simeq K_j(t)$. We let m be the biggest such index.

4. Let m be as in the previous part. Denote by $\psi : K_m[x_{m+1}, \ldots, x_n] \to K$ the map given by $\psi(x_j) = \varphi(x_j)$ and ψ is the identity on K_m. Observe that, on the one hand, ψ is surjective. On the other hand, observe that K is a finite extension of the field K_{m+1}, which is isomorphic to $K_m(t)$. Thus by part (2), with k changed to K_m, ψ cannot be a surjective. This is a contradiction and thus K/k is finite.