Mathematics 100B Exam 2 Practice Problems

Instructions: Exam 2 is Friday February 24. It will be an in class exam, 50 minutes long. No notes or calculators are allowed. This practice worksheet is to help you study for Exam 2. Anything discussed up to and including the material in lecture on Friday February 17 is fair game for the exam. 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. Exam 2 will consist of 5 problems, of a range of difficulty, that mirrors the difficulty of problems on this worksheet.

1. Let R, S be rings. Prove that a subset U of $R \times S$ is an ideal if and only if $U = I \times J = \{(x, y) : x \in I, y \in J\}$, where I is an ideal of R and J is an ideal of S.

   Proof. It is clear that if I and J are ideals of R and S, respectively, then $I \times J$ is an ideal of $R \times S$. For the converse, suppose $U \subseteq R \times S$ is given. Let $I = \{r \in R : (r, 0) \in U\}$ and similarly define $J = \{s \in S : (0, s) \in U\}$. Then one sees immediately that I, J are ideals, and $I \times J \subseteq U$. Moreover, if $u \in U$, say $u = (r, s)$, then $(r, 0) = (1, 0)u \in U$ and $(0, s) = (0, 1)u \in U$, so $r \in I$ and $s \in J$, proving $U = I \times J$. □

2. Suppose p is a prime number. Give an example of a ring with exactly one maximal ideal, and p^3 elements.

   Proof. For example, $S = \mathbf{F}_p[x]/(x^3)$ is such a ring. In general, if R is a finite ring of size m and $f(x) \in R[x]$ is monic of degree d, then $R[x]/(f(x))$ has size m^d. Thus, S has size p^3. Its maximal ideals are in bijection with the maximal ideals of $\mathbf{F}_p[x]$ that contain (x^3), so just the ideal (x). Thus it has one maximal ideal. □

3. Suppose F is a field. Prove that $F[x]$ contains infinitely many monic irreducible polynomials. (**Hint**: Suppose that there were only finitely many, $f_1(x), f_2(x), \ldots, f_m(x)$. Set $g(x) = f_1(x)f_2(x)\cdots f_m(x) + 1$. Consider the factorization of g.) Deduce that if p is a prime, there are infinitely many positive integers n so that there exists a field with p^n elements. (We will later prove that for every n, there is a field with p^n elements, and that this field is unique up to isomorphism.)

   Proof. If g is irreducible, we have a contradiction. If g reduces, then it must be divisible by an f_j, but then f_j divides 1, a contradiction. So there are infinitely many monic irreducibles. Consequently, for $F = \mathbf{F}_p$, there are infinitely n such that there is an irreducible monic polynomial $f(x)$ of degree n. But then $\mathbf{F}_p[x]/(f(x))$ is a field of size p^n. □

4. Let $f(x) = x^3 + x^2 + x + 1 \in \mathbf{R}[x]$. Factor f into irreducibles in $\mathbf{R}[x]$. **Hint**: Observe that $f(-1) = 0$.

   Proof. One factors out an $x+1$ to obtain $f(x) = (x+1)(x^2+1)$. The polynomials $x+1$ and x^2+1 are irreducible in $\mathbf{R}[x]$, so we are done. □

5. Suppose $f_1(x) = x^2 + b_1x + c_1 \in \mathbf{R}[x]$ and $f_2(x) = x^2 + b_2x + c_2 \in \mathbf{R}[x]$. Suppose moreover that $b_1^2 - 4c_1 < 0$ and $b_2^2 - 4c_2 < 0$. Prove that $\mathbf{R}[x]/(f_1(x))$ is isomorphic to $\mathbf{R}[x]/(f_2(x))$.

   Proof. Let $f(x) = x^2 + bx + c \in \mathbf{R}[x]$ with $b^2 - 4c < 0$. We prove $\mathbf{R}[x]/(f(x))$ is isomorphic to $\mathbf{C}$. To see this, set $\alpha = (-b + \sqrt{b^2 - 4})/2 \in \mathbf{C}$. Map $\mathbf{R}[x] \to \mathbf{C}$ by sending x to α. It is easy to see that this map is surjective. Its kernel is thus a maximal ideal of $\mathbf{R}[x]$ that contains $f(x)$. But f is irreducible so we are done. □

6. Suppose $f(x) \in \mathbf{Z}[x]$ is a monic polynomial, that is irreducible in $\mathbf{Q}[x]$. Set $R = \mathbf{Z}[x]/(f(x))$ and $F = \mathbf{Q}[x]/(f(x))$. Prove that R is an integral domain, and that F can be identified with the fraction field of R.

   Proof. We know from class that $f(x)$ is irreducible, because it is primitive and irreducible in $\mathbf{Q}[x]$. Thus R is an integral domain. In fact, the map from R to F induced by the inclusion $\mathbf{Z}[x] \to \mathbf{Q}[x]$ is an injection, because every integral polynomial divisible by $f(x)$ in $\mathbf{Q}[x]$ is divisible by $f(x)$ in $\mathbf{Z}[x]$. Moreover, because $f(x)$ is irreducible in $\mathbf{Q}[x]$, F is a field.

   Let F' denote the field of fractions of F. By the mapping property of F', we obtain an injection $F' \to F$ induced by the inclusion $R \to F$. But every element of F can be written as (the image of) $g(x)/N$ where $g(x) \in \mathbf{Z}[x]$ and $N \in \mathbf{Z}$. Thus $F' \to F$ is surjective as well, proving that they are isomorphic. □

7. Suppose F is a field, $f(x) \in F[x]$ and $f(x) = p_1(x)^{e_1} \cdots p_m(x)^{e_m}$ is the factorization of f into irreducibles. That is, each p_j is irreducible, and p_j is not an associate of p_k if $j \neq k$. Set $R_j = F[x]/(p_j(x)^{e_j})$. Prove that $F[x]/(f(x))$ is isomorphic to $R_1 \times \cdots \times R_m$.

   Proof. We apply the CRT. To see that it applies, we must only check that $(p_j^{e_j}) + (p_k^{e_k}) = F[x]$. But this follows from the fact p_j and p_k have no common divisor. □

8. Prove that the ring $\mathbf{Z}[x]/(7, x^3 + x^2 + x + 1)$ is isomorphic to $\mathbf{F}_7 \times E$ where E is a field with 49 elements.

   Proof. We have $x^3 + x^2 + x + 1 = (x + 1)(x^2 + 1)$, and $x^2 + 1$ is irreducible in $\mathbf{F}_7[x]$ because it does not have a root modulo 7. The claim follows. □

9. Prove that $\mathbf{Z}[\sqrt{-3}]$ is not a UFD. **Hint**: Consider the equality $2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$.

   Proof. Because 2 does not divide $1 \pm sqrt{-3}$ in $R = \mathbf{Z}[\sqrt{-3}]$, it suffices to check that 2 is irreducible in R. But if $2 = xy$, then $4 = |x|^2|y|^2$. But $2 = a^2 + 3b^2$ has no solutions, so $|x|^2 = 1$ or $|y|^2 = 1$, so 2 indeed is irreducible. □

10. Suppose $F \subseteq E$ are fields, and $\gamma \in E$ is such that there exists a nonzero polynomial $f(x) \in F[x]$ so that $f(\gamma) = 0$. Let $R = F[\gamma] \subseteq E$. Prove that R is a field.

    Proof. Let K be the kernel of the map $F[x] \to E$ that sends x to γ. Then $R \simeq F[x]/K$. By assumption, K is nonzero. Because E is a field, R is an integral domain, so K is prime. But every nonzero prime ideal of $F[x]$ is maximal, so R is a field. □