Mathematics 100B Exam 1 Practice Problems

Instructions: Exam 1 is Friday January 27. 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 1. Anything discussed up to and including the material in lecture on Friday January 20 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 1 will consist of 5 problems, of a range of difficulty, that mirrors the difficulty of problems on this worksheet.

1. How many units are there in $\mathbf{Z}/15\mathbf{Z}$?

   Proof. The units are residue classes $\overline{n}$ where n is relatively prime to 15. One counts and finds that there are 8 such classes (namely, the residue classes of $1, 2, 4, 7, 8, 11, 13, 14$.) □

2. Let $R = \mathbf{Z}/15\mathbf{Z}$.

   (a) Give an example of two nonzero polynomials f, g in $R[x]$ of positive degree such that the product $f(x)g(x) = 0$ in $R[x]$.

   (b) Suppose $f(x) \in R[x]$ has leading coefficient a unit in R, i.e., $f(x) = a_0 + a_1x + \cdots + a_nx^n$ with $a_n \in R^\times$. Prove that if $g(x) \in R[x]$ and $f(x)g(x) = 0$, then $g(x) = 0$.

   Proof. For the first part, take, for example $f(x) = \overline{3}x$ and $g(x) = \overline{5}x$. For the second part, we prove the contrapositive. Thus suppose $g(x) = b_0 + b_1x + \cdots + b_mx^m$ with $b_m \neq 0$ in R. Then the leading term of the product is $a_nb_mx^{n+m}$. Because a_n is a unit, $a_nb_m \neq 0$ in R, so $f(x)g(x) \neq 0$ in $R[x]$. □

3. Let $R = \mathbf{Z}[\sqrt{2}]$.

   (a) Prove that the ring R has infinitely many units. **Hint**: First prove that $3 - 2\sqrt{2}$ is a unit.

   (b) Prove that every element of R is an algebraic number.

   Proof. Note that if $a, b \in \mathbf{Z}$ so that $a + b\sqrt{2} \in R$, then $a - b\sqrt{2} \in R$ and their product is $a^2 - 2b^2$. Taking $a = 3$ and $b = 2$ we see that $u := 3 - 2\sqrt{2}$ is in $R^\times$.

   Note that $\sqrt{2} \approx 1.4$ so $u \approx .2$. Thus the elements u^k, $k = 0, 1, 2, 3, \ldots$ are distinct elements of R. Because u is a unit, each u^k is a unit, so $R^\times$ is infinite.

   For the second part, simply observe that $a+b\sqrt{2}$ is a root of the polynomial $(x-(a+b\sqrt{2}))(x-(a-b\sqrt{2})) = x^2 - 2ax + a^2 - 2b^2$. □

4. Let $R = \mathbf{Z}[\sqrt{2}]$ and let S be the subset of $M_2(\mathbf{Z})$ the (2×2 matrices with integer entries) consisting of matrices of the form $\begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$. That is,

$$S = \left\{ \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} : a, b \in \mathbf{Z} \right\}.$$

Prove that S is a ring with the usual matrix addition and multiplication, and that R is isomorphic to S.

Proof. It is clear that S is closed under addition, and is an abelian group under matrix addition. Moreover, S contains the identity matrix (with $a = 1$,$b = 0$), and one checks by explicit computation that S is closed under matrix multiplication, which is commutative. In fact:

$$\begin{pmatrix} a_1 & b_1 \\ 2b_1 & a_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 2b_2 & a_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 + 2b_1b_2 & a_1b_2 + a_2b_1 \\ 2(a_1b_2 + a_2b_1) & a_1a_2 + 2b_1b_2 \end{pmatrix}.$$

Because usual matrix multiplication is associative and distributes over addition, the same holds in S, so S is a ring.

To see that R and S are isomorphic, first observe that, because $\sqrt{2}^2 = 2$, every element of R can be expressed in the form $a + b\sqrt{2}$. Moreover, this expression is unique because $\sqrt{2}$ is irrational. Define $\varphi : R \to S$ as $\varphi(a + b\sqrt{2}) = \begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$. It is clear that φ takes 1 to 1, and respects addition. That it respects multiplication follows from expanding $(a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2})$ and comparing with the above matrix product. □

5. Recall that an element x of a ring R is said to be *nilpotent* if there exists a positive integer N so that $x^N = 0$ in R. Let R be a ring, and I the subset of nilpotent elements of R. Prove that I is an ideal of R.

Proof. The set I is nonempty because $0 \in I$. It is closed under multiplication by R as if $x^M = 0$, then $(rx)^M = r^M x^M = 0$. To see that I is closed under addition, suppose $x^M = 0$ and $y^N = 0$. We claim that $(x + y)^{N+M} = 0$. To see this, expand out to obtain $(x + y)^{N+M} = \sum_k \binom{N+M}{k} x^k y^{N+M-k}$. But now note that either $k \geq N$ or $N + M - k \geq M$ (because their sum is $N + M$) so one of these terms is 0. □

6. Find generators for the kernel of the map $\varphi : \mathbf{Z}[x] \to \mathbf{R}$ defined as $\varphi(f(x)) = f(\sqrt{3})$. (For this problem, you may use, without proving, that $\sqrt{3}$ is irrational.)

Proof. The kernel is the principal ideal $(x^2 - 3)$. To see this, first observe that $x^2 - 3$ is in the kernel. Now, suppose $g(x) \in \ker(\varphi)$. Then because $x^2 - 3$ is monic, we can divide it into $g(x)$ to obtain $g(x) = q(x)(x^2 - 3) + ax + b$ for some integers a, b. Evaluating at $x = \sqrt{3}$ we obtain $a\sqrt{3} + b = 0$. Thus $a = b = 0$ because $\sqrt{3}$ is irrational. This proves the claim, that $x^2 - 3$ divides $g(x)$. □

7. Suppose $x \in \mathbf{C}$ is an algebraic number. Prove that $2x$ is also an algebraic number.

Proof. Because x is algebraic, there are integers $a_n, a_{n-1}, \ldots, a_0$ so that $a_0 + a_1x + \cdots + a_nx^n = 0$. Thus $2^n a_0 + (2^{n-1}a_1)(2x) + \cdots a_n(2x)^n = 0$, so $2x$ is also algebraic. □

8. Suppose that S is a ring with 35 elements. Either:

   (a) Give an example of such an S with characteristic 3, OR

(b) prove that S cannot have characteristic 3.

Proof. The ring S cannot have characteristic 3. Indeed, suppose $n = char(S)$. Then n is the order of 1 in the additive group $(S, +)$, so n divides 35 by Lagrange's theorem. Consequently $n = 5, 7, 35$ are possible ($n = 1$ is excluded because S is not the 0 ring). In particular, S cannot have characteristic 3. □

9. Let $R = \mathbf{Z}/5\mathbf{Z}$.

   (a) Give an example a ring homomorphism $\varphi : R[x, y] \to R[x, y]$ that is injective but not surjective.

   (b) Give an example of a ring homomorphism $\psi : R[x, y] \to R[x, y]$ that is surjective but not the identity.

   Proof. For the first part, one can take, for example $x \mapsto x^2$, $y \mapsto y$, so that $\varphi(f(x, y)) = f(x^2, y)$. This is not surjective, because the image consists of polynomials whose terms in x all have even degrees. It is also clear, directly from the definition, that φ is injective.

   For the second part, one can define $\psi(f(x, y)) = f(x + 1, y)$. This is not the identity, and is clearly surjective, because it has as inverse $f(x, y) \mapsto f(x - 1, y)$. □

10. Prove that there does not exists a ring homomorphism from $\mathbf{Z}[\sqrt{2}]$ to $\mathbf{Z}[\sqrt{3}]$. (For this problem, you may use, without proving, that $\sqrt{3}$ is irrational.)

    Proof. Suppose $\varphi : \mathbf{Z}[\sqrt{2}] \to \mathbf{Z}[\sqrt{3}]$ is a ring homomorphism. We will derive a contradiction. To do so, let $\varphi(\sqrt{2}) = a + b\sqrt{3}$. Then on the one hand, $(a + b\sqrt{3})^2 = \varphi(\sqrt{2})^2 = \varphi(2) = 2$. On the other hand, expanding, $(a + b\sqrt{3})^2 = a^2 + 3b^2 + 2ab\sqrt{3}$. Because $\sqrt{3}$ is irrational, we must have $a^2 + 3b^2 = 2$ and $2ab = 0$. These equations do not have any solution, a contradiction. □