Math 103b Spring 2014 Exam 1

April 25, 2014

NAME: SOLUTIONS

Instructions: No books, notes, calculators, phones etc. are allowed to be used during the exam. You may quote the theorems that we proved in class, or that are proved in the textbook, in your proofs, unless the problem says otherwise. Generally, do not quote the result of a homework exercise in your proof—if you need such a result you should go through the proof again.

Problem 1 /10	
Problem 2 /15	
Problem 3 /15	
Total /40	

1. (10 pts)

(a) (5 pts) Define what it means for a ring R to be an integral domain. Define what it means for a ring R to be a field.

A ring R is an integral domain if it is a commutative ring with unity which has no zerodivisors; that is, if $ab = 0$ implies that $a = 0$ or $b = 0$.

A ring R is a field if it is a commutative ring with unity such that every nonzero $a \in R$ is a unit; that is, for every $0 \neq a \in R$ there exists $b \in R$ with $ab = 1$.

(b) (5 pts) Give a brief proof that a field must be an integral domain (this is a theorem in the text and in class; I want you to reprove it).

Since a field is a commutative ring with unity, it suffices to prove that $ab = 0$ implies that $a = 0$ or $b = 0$. Suppose that $ab = 0$. If $a \neq 0$, then a is a unit by the definition of a field, so there is an element $a^{-1} \in R$ such that $a^{-1}a = 1$. Then $b = a^{-1}ab = a^{-1}0 = 0$.

2. (15 pts) Let $R = \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} | a, b \in \mathbb{Z}\}$.
(a) (5 pts) Prove that R is a subring of the ring $\mathbb{R}$ of real numbers.

By the subring test, we need to show that R is nonempty, closed under subtraction, and closed under multiplication. It is obvious that R is nonempty; for example, $0 = 0 + 0\sqrt{2} \in R$.

If $a+b\sqrt{2}, c+d\sqrt{2} \in R$, where $a, b, c, d \in \mathbb{Z}$, then $(a+b\sqrt{2})-(c+d\sqrt{2}) = (a-c) + (b-d)\sqrt{2} \in R$, since $a-b, c-d \in \mathbb{Z}$ also.

We also have $(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (bd + ac)\sqrt{2} \in R$, since $(ac + 2bd)$ and $(bd + ac)$ are also in $\mathbb{Z}$. Thus R is a subring of $\mathbb{R}$.

(b) (10 pts) Let $I = \langle 2 + \sqrt{2} \rangle$ be the principal ideal of R generated by $2 + \sqrt{2}$. Prove that the factor ring R/I has exactly 2 elements. (Hint: use a similar method as we used for studying factor rings of $\mathbb{Z}[i]$).

By definition, $I = \{(2+\sqrt{2})(c+d\sqrt{2}) | c, d \in \mathbb{Z}\}$. Take an arbitrary element $a + b\sqrt{2} \in R$, where $a, b \in \mathbb{Z}$. We have $(2 + \sqrt{2})(b) = 2b + b\sqrt{2} \in I$. Thus $(a+b\sqrt{2})-(2b+b\sqrt{2}) = (a-2b)$. This means that $(a+b\sqrt{2})+I = (a-2b)+I$ in the factor ring R/I. In other words, every element of R/I is equal to $c+I$ for some integer $c \in \mathbb{Z}$.

Next, we have $(2 + \sqrt{2})(2 - \sqrt{2}) = 4 - 2 = 2 \in I$. Now $c = 2q + r$ for some $q \in \mathbb{Z}$ and $r \in \{0, 1\}$, by the division theorem for integers. Since $2 \in I$, we have $2q \in I$, and thus $c + I = r + I$. It follows that

$$R/I = \{0 + I, 1 + I\}.$$

It remains to show that the cosets $0 + I$ and $1 + I$ are nonequal. If they are equal, then $1 \in I$, so $1 = (2 + \sqrt{2})(c + d\sqrt{2}) = (2c + 2d) + (c + 2d)\sqrt{2}$ for some $c, d \in \mathbb{Z}$. If $c + 2d \neq 0$, then this equation can be solved for $\sqrt{2}$ yielding $\sqrt{2} \in \mathbb{Q}$; but it is well known that $\sqrt{2}$ is irrational. Thus $c + 2d = 0$ and consequently $1 = 2c + 2d$. This implies that 1 is an even integer, a contradiction.

Thus R/I consists of exactly two distinct cosets, $0 + I$ and $1 + I$.

3. (15 pts) Let $R = \mathbb{Z} \oplus \mathbb{Z}$, the direct sum of two copies of the ring $\mathbb{Z}$. Recall that this consists of all ordered pairs $\{(a, b) | a, b \in \mathbb{Z}\}$, with addition and multiplication defined coordinatewise.

(a) (5 pts) Let $I = \{(2a, 3b) | a, b \in \mathbb{Z}\}$. Prove that I is an ideal of R.

By the test for ideals, since R is a commutative ring, we need only show that I is nonempty, closed under subtraction, and that given $r \in R$ and $x \in I$ we have $rx \in I$.

I is obviously nonempty ($(0, 0) \in I$ for example). Given arbitrary elements $(2a, 3b) \in I$, $(2c, 3d) \in I$, where $a, b, c, d \in \mathbb{Z}$, we have $(2a, 3b) - (2c, 3d) = (2(a - c), 3(b - d)) \in I$.

Similarly, given $(2a, 3b) \in I$, $(c, d) \in R$, we have $(c, d)(2a, 3b) = (2ac, 3bd) \in I$. Thus I is an ideal of R.

(b) (5 pts) Find the characteristic of the factor ring R/I.

By a theorem we proved, since R/I is a ring with unity $(1, 1) + I$, the characteristic of R/I is the smallest positive integer n, if any, such that $n \cdot [(1, 1) + I] = (0, 0) + I$. But $n \cdot [(1, 1) + I] = (n, n) + I$, and this is equal to $(0, 0) + I$ if and only if $(n, n) \in I$.

Now if $(n, n) \in I$, then $(n, n) = (2a, 3b)$ for some $a, b \in \mathbb{Z}$, so n is a multiple of 2 and 3; thus n is a multiple of $\text{lcm}(2, 3) = 6$. On the other hand, certainly $(6, 6) \in I$. Thus 6 is the smallest positive integer n such that $(n, n) \in I$. This implies that the characteristic of R/I is 6.

(c) (5 pts) Is I a prime ideal of R? Is I a maximal ideal of R? Justify your answers.

I is not prime, and I is not maximal. There are several ways to do the parts of this problem, and so we indicate the alternatives.

One can prove that I is not prime directly from the definition of prime ideal: note that $(1, 3) \notin I$, since 1 is not a multiple of 2. Similarly, $(2, 1) \notin I$. But $(1, 3)(2, 1) = (2, 3) \in I$. Since I contains a product of elements which are not in I, the ideal I is not prime.

Alternatively, one can see that I is not prime by quoting a theorem we proved: The characteristic of an integral domain must be prime. Since R/I has characteristic 6, the factor ring R/I is not an integral domain. We also proved (since the ring R is commutative) that I is a prime ideal if and only if R/I is an integral domain. Thus I is not a prime ideal.

To see that I is not maximal, one can also use the result we proved that a maximal ideal of a commutative ring with unity is also a prime ideal. Then since I is not prime, it is not maximal.

Alternatively, one can prove that I is not maximal directly from the definition. Consider $J = \{(a, 3b) | a, b \in \mathbb{Z}\}$. Then J is an ideal of R, by a completely similar proof as the proof of part (a). But it is easy to see that $I \subsetneq J \subsetneq R$. Thus I is not a maximal ideal by definition.