Math 103b Spring 2014 Midterm 2

May 23, 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 Generally, do not quote the result of a homework exercise in your proof—if you need such a result you should go through the proof again.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 /10	
Problem 3 /15	
Total /35	

1 (10 pts)

(a)(5 pts) Define what it means for an element x in an integral domain R to be irreducible. Define what it means for an element x in an integral domain R to be prime.

An element $x \in R$ is irreducible if x is nonzero and not a unit, and whenever $x = yz$ for elements $y, z \in R$, either y or z is a unit. An element $x \in R$ is prime if x is nonzero and not a unit, and if whenever $x|yz$ for elements $y, z \in R$, then either $x|y$ or $x|z$.

(b) (5 pts). Prove that in any integral domain R, a prime element must be irreducible. (This is a theorem in class and in the text. I want you to reprove it).

Let $x \in R$ be prime. Then by definition x is not zero and not a unit. Suppose that $x = yz$ for elements $y, z \in R$. Then $x|yz$ (recall that $a|b$ means $b = ac$ for some c). By the definition of prime, either $x|y$ or $x|z$. In the first case, we have $y = cx$ for some $c \in R$. Then $x = yz = cxz$. Since R is an integral domain, $x = xcz$ implies $1 = cz$ since cancellation of nonzero elements holds. This equation shows that z is a unit. Similarly, if $x|z$ a symmetric argument shows that y is a unit. So either y or z must be a unit, so x is irreducible by definition.

2 (10 pts)

(a) (5 pts). Is the polynomial $f(x) = x^5 + 25x^2 + 15x - 35 \in \mathbb{Q}[x]$ irreducible? Justify your answer.

This polynomial is irreducible over $\mathbb{Q}$ by the Eisenstein criterion with $p = 5$. Namely, f has integer coefficients, p does not divide the leading coefficient 1; p divides every other coefficient; and $p^2 = 25$ does not divide the constant term -35.

(b) (5 pts). Is the ring $R = \mathbb{Z}_5[x]/\langle x^3 + \overline{2}x + \overline{3}\rangle$ a field? Justify your answer.

By theorems we studied in class and in the textbook, R is a field if an only if the principal ideal $\langle x^3 + \overline{2}x + \overline{3}\rangle$ is a maximal ideal in $\mathbb{Z}_5[x]$, if and only if $x^3 + \overline{2}x + \overline{3}$ is an irreducible polynomial in $\mathbb{Z}_5[x]$. Now since this polynomial has degree 3, it is irreducible in $\mathbb{Z}_5[x]$ if and only if it has a root in $\mathbb{Z}_5$, by another theorem we proved. By checking all possible elements in $\mathbb{Z}_5$, one quickly finds that $\overline{2}$ is a root, since $\overline{8 + 4 + 3} = \overline{15} = \overline{0}$ in $\mathbb{Z}_5$. So the polynomial is not irreducible over $\mathbb{Z}_5[x]$, and hence R is not a field.

3 (15 pts). Consider the ring $R = \mathbb{Z}[\sqrt{-10}] = \{a + b\sqrt{-10} | a, b \in \mathbb{Z}\}$, as a subring of $\mathbb{C}$. Recall that R has a norm function $N(a + b\sqrt{-10}) = |a^2 + 10b^2| = a^2 + 10b^2$ with the following properties (which you can assume without proof):

(i) $N(x) = 0$ if and only if $x = 0$;
(ii) $N(x)N(y) = N(xy)$ for all $x, y \in R$;
(iii) x is a unit in R if and only if $N(x) = 1$; and
(iv) if $N(x)$ is a prime number in $\mathbb{Z}$, then x is irreducible in R.

(a) (5 pts). Show that if $x \in R$ is an element with $N(x) = pq$, where p, q are prime integers such that no element in R has norm p or norm q, then x is irreducible.

Note that x is not 0 and x is not a unit, since $N(x) \neq 0, 1$. Suppose that $x = yz$ with $y, z \in R$. Then $pq = N(x) = N(y)N(z)$. If neither y nor z is a unit, then we must have $N(y) \neq 1$, $N(z) \neq 1$. But since $N(y)N(z) = pq$, by unique factorization of integers this forces either $N(y) = p$ and $N(z) = q$ or $N(y) = q$ and $N(z) = p$. By assumption, no elements in the ring have norm p or norm q. This gives a contradiction and shows that either y or z has to be a unit. Then x is irreducible by definition.

(Note that this proof shows that the hypothesis is too strong; the same proof would work if we assume that no element in R has norm p; we don't need to know in addition that no element in R has norm q.)

(b) (5 pts). Show that no element of R has norm 2 or norm 5. Then prove that $2, 5$, and $\sqrt{-10}$ are irreducible elements of R.

If $x \in R$ has $N(x) = 2$, then $x = a + b\sqrt{-10}$ with $a^2 + 10b^2 = 2$. If $b \neq 0$, then $10b^2 \geq 10$ and so $a^2 + 10b^2 \geq 10 > 2$, a contradiction. So $b = 0$ and $a^2 = 2$. But no integer has square 2 since $\sqrt{2}$ is irrational. Thus again we reach a contradiction and no such x exists.

Similarly, if $x \in R$ has $N(x) = 5$ where $x = a + b\sqrt{-10}$, then we get $a^2 + 10b^2 = 5$ and similarly reach a contradiction since $\sqrt{5}$ is also irrational.

Now $N(2) = 4 = (2)(2)$, $N(5) = 25 = (5)(5)$, and $N(\sqrt{-10}) = 10 = (2)(5)$. Using part (a) and the result that no elements of norm 2 or 5 exist in this ring, we see that $2, 5$, and $\sqrt{-10}$ are all irreducible in this ring.

(c) (5 pts). Is R a Euclidean domain (ED)? Is R a principal ideal domain (PID)? Is R a unique factorization domain (UFD)? Justify your answers.

(Hint: consider the equation $(2)(5) = (\sqrt{-10})(\sqrt{-10})$).

We have the equation $(2)(5) = (\sqrt{-10})(\sqrt{-10})$, in which the elements $2, 5$, and $\sqrt{-10}$ are all irreducible using part (b). if R is a UFD, then by definition factorization into irreducibles is unique up to order and associates. Thus $\sqrt{-10}$ must be an associate of 2 (and also an associate of 5). So $\sqrt{-10} = (2)u$ for some unit $u \in R$. Applying the norm and recalling that $N(u) = 1$ since u is a unit, $10 = N(\sqrt{-10}) = N(2)N(u) = 4$, a contradiction. Thus R is not a UFD.

(As an alternative for showing that $\sqrt{-10}$ and 2 are not associates, you could first prove that ± 1 are the only units in R, since $N(a + b\sqrt{-10}) = a^2 + 10b^2 = 1$ has only the solutions $a = \pm 1$, $b = 0$. But clearly $\sqrt{-10} \neq \pm 2$.)

We proved that a ED is a PID, and that a PID is a UFD. Once we know that R is not a UFD, it can't possibly be a ED or a PID.