Mathematics 403A Final Exam Name: Answers

March 16, 2005

Instructions: This is a closed book exam, no notes or calculators allowed. Justify all of your answers. Unless a particular problem states otherwise, you may refer to and use any result from the book, but for full credit, do not use results from homework or practice problems – if you need one of those results, you should prove it.

As usual, $\mathbf{Z}$ is the ring of integers, $\mathbf{Q}$ is the rational numbers, and $\mathbf{C}$ is the complex numbers.

This is a timed exam, so you may use abbreviations and symbols (such as "$\forall$"): as long as I can make sense of what you write without struggling too much, it's okay.

1. Using only the definition of Euclidean domain, prove that $\mathbf{Z}[i]$ is a Euclidean domain.

Solution: First, we need to check that $\mathbf{Z}[i]$ is an integral domain. Since it's a subring of $\mathbf{C}$ and $\mathbf{C}$ is an integral domain (in fact a field), then $\mathbf{Z}[i]$ must be one as well.

Next, we define a size function $\sigma : \mathbf{Z}[i] \to \mathbf{Z}$ by $\sigma(a+bi) = |a+bi|^2 = a^2+b^2$. (In general, this size function doesn't have to be defined on the zero element, but it's okay if it is, as in this case.) Using this, we have to show that for all $\alpha, \beta \in \mathbf{Z}[i]$ with $\beta \neq 0$, there exist $q, r \in \mathbf{Z}[i]$ such that

$$\alpha = \beta q + r, \quad \text{and} \quad \sigma(r) < \sigma(\beta) \text{ (or } r = 0).$$

Let q be a point in $\mathbf{Z}[i]$ which is as close as possible to the quotient $\alpha/\beta \in \mathbf{C}$. Since every point in $\mathbf{C}$ is distance at most $1/\sqrt{2}$ from a point in $\mathbf{Z}[i]$ (by elementary geometry), then we know that $|\alpha/\beta - q| < 1/\sqrt{2} < 1$. Let $r = \alpha - \beta q$. Since the size function σ respects the multiplication, and since $\sigma(\alpha/\beta - q) < 1$, then $\sigma(\alpha - \beta q) < \sigma(\beta)$, as desired.

2. (a) Is $\mathbf{Z}[x,y]$ a UFD? Is it a PID? Is it a Euclidean domain? Prove that your answers are correct.

Solution: This ring is a UFD, but not a PID or a Euclidean domain. The main theorem in the section on Gauss's lemma says that if R is a UFD, then so is $R[x]$. Apply that twice here: $\mathbf{Z}$ is a UFD, hence so is $\mathbf{Z}[x]$, hence so is $\mathbf{Z}[x][y] \cong \mathbf{Z}[x,y]$.

Also, the ideal (x,y) is not principal. The elements x and y are each irreducible, so their only common divisors are ± 1, so these are the only candidates for a single generator for this ideal. But $(1) \neq (x,y)$ because, for example, $1 \notin (x,y)$. So the ideal is not principal, and the ring is not a PID.

Since every Euclidean domain is a PID, this ring can't be a Euclidean domain.

(b) Is $\mathbf{Z}[\sqrt{-5}]$ a UFD? Is it a PID? Is it a Euclidean domain? Prove that your answers are correct.

Solution: This ring is not a UFD, a PID, or a Euclidean domain. Since every Euclidean domain is a PID and every PID is a UFD, it suffices to explain why it is not a UFD.

Let $\delta = \sqrt{-5}$. The element 6 factors in two ways: $6 = 2 \cdot 3 = (1+\delta)(1-\delta)$. This is *not* enough to show that 6 is not a UFD; after all, the integer 12 factors in two ways as $12 = 3 \cdot 4 = 2 \cdot 6$, but this doesn't mean that $\mathbf{Z}$ is not a UFD. No, we also have to show that all of the factors above are irreducible, and the factors in one are not associates of the factors in the other, so that there are two different factorizations into irreducible elements. To do this, consider the norm map N (called σ in the previous problem): $N(a+b\delta) = a^2 + 5b^2$. This is "multiplicative," meaning that $N(\alpha\beta) = N(\alpha)N(\beta)$ for any α, β. Also, an element α is a unit if and only if $N(\alpha) = 1$.

$N(2) = 4$, so any proper factors of 2 have norm 2. There are no elements of norm 2: there are no integers a and b so that $a^2 + 5b^2 = 2$.

$N(3) = 9$, so any proper factors of 3 have norm 3, and there are no such elements in $\mathbf{Z}[\delta]$.

$N(1 \pm \delta) = 6$, so any proper factors have norm 2 or 3, and there are no such elements.

Thus all of these factors are irreducible, and since their norms are all different, they are not associates of each other. Therefore $\mathbf{Z}[\delta]$ fails to be a UFD.

3. For each of these polynomials in $\mathbf{Q}[x]$, either factor them or explain why they're irreducible.

(a) x^3+3x+5

Solution: Irreducible. Reduce mod 2 to get x^3+x+1. Since this is degree 3, if it factored nontrivially, then one factor would have degree 1, which would mean that the polynomial has a root. But it has no roots: just plug in 0 and 1. So x^3+x+1 doesn't factor in $\mathbf{F}_2[x]$, and therefore x^3+3x+5 doesn't factor in $\mathbf{Q}[x]$.

(b) $x^7-10x^6+5x^2-25x+20$

Solution: Irreducible. Apply Eisenstein's criterion with $p=5$: 5 does not divide the leading coefficient, it does divide all of the other coefficients, and its square 25 does not divide the constant term. The hypotheses of Eisenstein's criterion are satisfied, and thus the polynomial doesn't factor.

(c) x^4+x^2+1

Solution: This factors as $x^4+x^2+1=(x^2+x+1)(x^2-x+1)$. (It has no roots mod 2, so it has no linear factors in $\mathbf{Q}[x]$ either. Then if you try to factor it as $(x^2+ax+b)(x^2+cx+d)$, you can pretty easily solve for a, b, c, and d.)

4. Which integers n can be written as a sum of two squares: that is, for which integers n is there an integer solution to $x^2+y^2=n$?

Solution: All integers n so that in their prime factorization, every prime congruent to 3 mod 4 appears with an even power. (The other primes can appear to any power.)

See Artin, section 12?, for a discussion.

You got partial credit if you pointed out that in the case when n is prime, the answer is: all primes congruent to 1 mod 4, and also 2, because of the main theorem about factorization in the Gaussian integers.

5. Identify the kernel of the homomorphism $\varphi : \mathbf{C}[x,y] \to \mathbf{C}[t]$ defined by $\varphi(x) = t^2$, $\varphi(y) = t^3$.

Solution: The kernel is the ideal $I = (y^2 - x^3)$.

It is clear that $y^2 - x^3$ is in the kernel, and hence the kernel contains the ideal I.

Let $f(x,y)$ be an element of $\mathbf{C}[x,y]$. View this ring as $\mathbf{C}[x][y]$ – polynomials in y with coefficients in $\mathbf{C}[x]$. The polynomial $y^2 - x^3$ is monic of degree 2 from this viewpoint, so divide by it to get

$$f(x,y) = (y^2 - x^3)g(x,y) + r(x,y),$$

where $r(x,y) = 0$ or the degree of r, with respect to y, is at most 1. That is, $r(x,y) = a(x)y + b(x)$ for some polynomials $a(x)$ and $b(x)$, so

$$f(x,y) = (y^2 - x^3)g(x,y) + a(x)y + b(x). \qquad (*)$$

If $f(x,y) \in \ker\varphi$, then $\varphi(f(x,y)) = 0$. On the other hand, the description (*) gives

$$\begin{aligned} \varphi(f(x,y)) &= \varphi(a(x)y) + \varphi(b(x)) \\ &= a(t^2)t^3 + b(t^2). \end{aligned}$$

The polynomial $b(t^2)$ has only even powers of t. So does the polynomial $a(t^2)$, and so $a(t^2)t^3$ has only odd powers of t. These two polynomials can't cancel each other off, so they each must be zero, so $a(x)$ and $b(x)$ must be zero. That is, $f(x,y)$ is a multiple of $y^2 - x^3$, which is what we wanted to show.

6. Prove that in the ring $\mathbf{Z}[\sqrt{-7}]$, 2 is irreducible but 2 is not prime. (Hint: factor 8.)

Solution: 2 is irreducible by a norm argument, as in problem 2(b): the norm of 2 is 4, so any proper factors have norm 2, but there are no integers a and b so that $a^2+7b^2=2$.

Let $\delta=\sqrt{-7}$ and factor 8: $8=(1+\delta)(1-\delta)$. In the ring $\mathbf{Z}[\delta]$, 2 does not divide $1+\delta$ or $1-\delta$. Since 2 divides a product (8) but doesn't divide any of its factors, 2 cannot be prime.

The fact that 2 doesn't divide $1\pm\delta$ can be proved in at least two ways:

- By a norm argument: the norm of 2 is 4, and the norm of $1\pm\delta$ is 8, so if there were an element α so that $2\alpha=1+\delta$, say, then $N(\alpha)$ would have to be 2. But as pointed out in the first paragraph, there are no elements in this ring of norm 2.
- By an elementary divisibility argument: for any element $a+b\delta$ in this ring, $2(a+b\delta)=2a+2b\delta$. Thus an element $x+y\delta$ is a multiple of 2 if and only if x and y are both even. This fails for $1\pm\delta$, so these elements are not divisible by 2.

(Note, by the way, that $\mathbf{Z}[\sqrt{-7}]$ is not the ring of integers in a quadratic number field, so many of the theorems from the book don't apply.)