Name: Solutions

Mathematics 403 Exam

February 2, 2005

Instructions: This is a closed book exam, no notes or calculators allowed. Justify all of your answers. 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.

Z denotes the ring of integers. $\mathbf{F}_p$ denotes the field with p elements: $\mathbf{F}_p = \mathbf{Z}/(p)$. All rings mentioned in this exam are assumed to be commutative.

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. (10 points) Let F be a field. What are all of the ideals in $F[x]/(x^2-1)$? (Your answer may depend on the characteristic of F.)

   Answer. According to the "correspondence theorem," the ideals of $F[x]/(x^2-1)$ are in bijection with the ideals of $F[x]$ which contain (x^2-1). The ideals of $F[x]$ are all principal and so are of the form $(f(x))$ for some polynomial $f(x)$. Furthermore, $(f(x))$ contains (x^2-1) if and only if $f(x)$ divides x^2-1. The polynomial x^2-1 factors as $x^2-1=(x-1)(x+1)$, so its divisors are (up to unit multiple)

   $$1, x-1, x+1, x^2-1.$$

   When the characteristic of F is 2, the middle two terms are equal; otherwise, they are all distinct. Therefore when the characteristic of F is 2, there are three ideals in $F[x]/(x^2-1)$:

   $$(1),\ (\overline{x}+1),\ (\overline{x}^2+1) = (0).$$

   When the characteristic of F is not 2, there are four ideals in $F[x]/(x^2-1)$:

   $$(1),\ (\overline{x}-1),\ (\overline{x}+1),\ (\overline{x}^2-1) = (0).$$

   (I'm writing $\overline{x}$ for the residue of x in the quotient ring $F[x]/(x^2-1)$.)

2. (10 points) Let R be an integral domain. Given nonzero polynomials $f(x), g(x) \in R[x]$, prove that $\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x))$.

   Answer. Let $f(x) = \sum_{i=0}^{m} a_i x^i$ with $a_m \neq 0$, so that $\deg f(x) = m$. Let $g(x) = \sum_{j=0}^{n} b_j x^j$ with $b_n \neq 0$, so that $\deg g(x) = n$. In the product $f(x)g(x)$, the coefficient of x^k is $\sum_{i+j=k} a_i b_j$. This means that when $k > m+n$, this coefficient is zero, and when $k = m+n$, this coefficient equals $a_m b_n$. Since R is an integral domain and since a_m and b_n are nonzero, their product is also nonzero. Thus the leading term of $f(x)g(x)$ is $a_m b_n x^{m+n}$, so $\deg(f(x)g(x)) = m+n = \deg(f(x)) + \deg(g(x))$.

3. (5 points) For which prime numbers p is $\mathbf{F}_p[x]/(x^2+1)$ a field?

   This is a hard question in general, so I would like you to make an educated guess, and to provide justification and evidence for that guess.

   Answer. The answer is: all primes p which are congruent to 3 mod 4.

   To come up with this guess, $\mathbf{F}_p[x]/(x^2+1)$ is a field if and only if the ideal (x^2+1) is maximal, which is true if and only if the polynomial x^2+1 is irreducible. Because this is a degree 2 polynomial, this is true if and only if it has no roots: if and only if $x^2 \neq -1$ for all $x \in \mathbf{F}_p$. In summary: $\mathbf{F}_p[x]/(x^2+1)$ is a field if and only if $-1 = p-1$ is not a square in $\mathbf{F}_p$.

   Now try some primes to see what happens.

   - When $p = 2$, $1 = -1$ is a square, so we don't get a field.
   - When $p = 3$, $0^2 = 0$, $1^2 = 1$, and $2^2 = 1$, so $-1 = 2$ is not a square, so we get a field.
   - When $p = 5$, $2^2 = 4 = -1$, so we don't get a field.
   - When $p = 7$, the squares are 0, 1, 2, and 4, so $-1 = 6$ is not a square and we get a field.
   - When $p = 11$, the squares are 0, 1, 4, 5, and 9, so $-1 = 10$ is not a square and we get a field.
   - When $p = 13$, $5^2 = 25 = -1$, so we don't get a field.
   - When $p = 17$, $4^2 = 16 = -1$, so we don't get a field.

   So the good primes (so far) are 3, 7 and 11. These are all congruent to 3 mod 4. The bad primes (so far) are 2, 5, 13, 17. These are all congruent to 1 or 2 mod 4.

4. (5 points) The ring $\mathbf{Z}[x]/(9x^2+1)$ is isomorphic to a subring of the complex numbers. Which subring?

   Answer. View this ring as being $\mathbf{Z}$ with an element x adjoined which satisfies the relation $9x^2+1=0$, or $9x^2=-1$, or $x^2=-1/9$, so $x=\pm i/3$. So I would guess that the answer is $\mathbf{Z}[i/3]$; this is easy to verify with the first isomorphism theorem.

   (Note, by the way, that $\mathbf{Z}[i/3]$ is *not* equal to $\{a+\frac{bi}{3} : a,b,\in \mathbf{Z}\}$. Since $i/3$ and 3 are in our ring, so is their product i, and hence so is $(i)(i/3)=-1/3$. Note that $-1/3$ is not in $\{a+\frac{bi}{3} : a,b,\in \mathbf{Z}\}$.)

5. (5 points) Let a, b, and k be positive integers, and let $n=a^kb$. Show that the residue of ab is nilpotent in $\mathbf{Z}/(n)$. (Recall that an element of a ring is *nilpotent* if some power of it is zero.)

   Answer. $(ab)^k=a^kb^k=(a^kb)b^{k-1}=nb^{k-1}$, so when I reduce this mod n, I get zero.

6. (5 points) Let R and S be rings with identity elements 1_R and 1_S, respectively. Suppose that $\varphi : R \to S$ is a function with the properties $\varphi(a+b)=\varphi(a)+\varphi(b)$ and $\varphi(ab)=\varphi(a)\varphi(b)$ for all $a,b \in R$. Show that if $\varphi(1_R)$ is not equal to 1_S, then there is a nonzero element $b \in S$ so that $\varphi(1_R)b=0$.

   Answer. Let $a=\varphi(1_R)$. Since $1_R1_R=1_R$, then when I apply φ to this, I get $a^2=a$, so $a^2-a=0$. I can rewrite this as $(a-1)a=0$. If $\varphi(1_R)\neq 1$, then $a-1\neq 0$, so this is my element b.