Math 404 Exam solutions

1. (a) Do problem 3 in the Miscellaneous exercises for Chapter 10.

   SOLUTION: Fix elements a and b of R; I want to show that $a+b=b+a$. Consider $(a+b)(1+1)$. Expanding one way, I get

   $$(a+b)(1+1) = a(1+1) + b(1+1) = a+a+b+b.$$

   Expanding the other way, I get

   $$(a+b)(1+1) = (a+b)1 + (a+b)1 = a+b+a+b.$$

   So $a+a+b+b = a+b+a+b$. Now add $-a$ to both sides, on the left, and add $-b$ to both sides, on the right, to get $a+b=b+a$, as desired.

   (b) Consider the ring $\mathbf{Z}$ of integers. Given $m, n \in \mathbf{Z}$, show that $(m) \subseteq (n)$ if and only if n divides m.

   SOLUTION. If $(m) \subseteq (n)$, then $m \in (n)$, so m is a multiple of n. In other words, n divides m. Conversely, if n divides m, say $m = nk$, then every multiple of m is also a multiple of n: $am = akn$. So every element of (m) is in (n); in other words, $(m) \subseteq (n)$.

2. Do either part (a) or part (b). Do not do both.

   (a) Do problem 2 in the Miscellaneous exercises for Chapter 10.

   SOLUTION. (a) To verify the product rule, let $f(x) = \sum a_m x^m$ and let $g(x) = \sum b_n x^n$. Now just compute $(fg)'$, fg', and $f'g$:

   $$(fg)' = (\sum_k \sum_{i+j=k} a_i b_j x^{i+j})' = \sum_k \sum_{i+j=k} (i+j) a_i b_j x^{i+j-1},$$
   $$fg' = (\sum_m a_m x^m)(\sum_n n b_n x^{n-1}) = \sum_k \sum_{i+j=k} a_i j b_j x^{i+j-1},$$
   $$f'g = (\sum_m m a_m x^{m-1})(\sum_n b_n x^n) = \sum_k \sum_{i+j=k} i a_i b_j x^{i+j-1},$$

   so

   $$fg' + f'g = \sum_k \sum_{i+j=k} (a_i j b_j + i a_i b_j) x^{i+j-1} = \sum_k \sum_{i+j=k} (i+j) a_i b_j x^{i+j-1}.$$

   This is equal to $(fg)'$.

   To verify the chain rule, it's probably a good idea to first notice that if $g(x)$ is any polynomial, then $(g(x)^m)' = mg(x)^{m-1}g'(x)$. This is easy to prove using the product rule and induction. Given this, with $f(x) = \sum a_m x^m$,

   $$f \circ g(x) = \sum a_m (g(x))^m,$$

   so

   $$(f \circ g)' = \sum a_m m g(x)^{m-1} g'(x).$$

   On the other hand, since $f'(x) = \sum m a_m x^{m-1}$,

   $$f' \circ g = \sum a_m m g(x)^{m-1},$$

   so $(f \circ g)' = (f' \circ g)g'$.

   (b) Suppose that α is a multiple root of $f(x)$; this means that $(x-\alpha)^2$ divides $f(x)$: $f(x) = g(x)(x-\alpha)^2$ for some polynomial $g(x)$. Then by the product rule, $f'(x) = g'(x)(x-\alpha)^2 + 2g(x)(x-\alpha)$: this is divisible by $x-\alpha$, so α is a root of $f'(x)$. Conversely, suppose that α is a root of $f(x)$ and of $f'(x)$. Then $f(x) = (x-\alpha)g(x)$ for some $g(x)$, and so $f'(x) = g(x) + (x-\alpha)g'(x)$. Plug in $x = \alpha$: $f'(\alpha) = g(\alpha) + 0$.

We are assuming that α is a root of $f'(x)$, so α must be a root of $g(x)$. Thus $g(x) = (x-\alpha)h(x)$ for some $h(x)$, so $f(x) = (x-\alpha)^2 h(x)$.

(c) $x^{15} - x$: the derivative of this is $15x^{14} - 1 = -1$ (we are working with coefficients in the field $\mathbf{F}_5$, so $5 = 0$, so $15 = 0$). -1 has no roots, so this polynomial has no roots in common with its derivative, so it has no multiple roots. $x^{15} - 2x^5 + 1$: the derivative is $15x^{14} - 10x^4 = 0$: every x is a root. So every root of the polynomial is also a root of its derivative. We just need to see if the polynomial has a root to finish the problem. Plug in $x = 1$: it's a root, hence a multiple root.

(b) Do problem 26 in Section 3 of Chapter 10.

SOLUTION. Here is a complete list of the ideals of $\mathbf{R}[[t]]$: (1), (t), (t^2), ..., (t^n), ..., (0). Certainly every one of these is an ideal; I have to show that these are the only ideals. A homework problem (10.2.6) tells us that if a power series $f(t) = a_0 + a_1 t + a_2 t^2 + \cdots$ has nonzero constant term a_0, then $f(t)$ is a unit, in which case $(f(t)) = (1)$. This suggests a way to proceed: given a nonzero ideal I, let n be the largest number so that t^n divides every element of I. (For example, if I contains a power series with a nonzero constant term, then n will be zero; if every power series in I has constant term zero, then n will be at least 1.)

Then all the elements I look like $f(t) = t^n g(t)$ for some power series $g(t)$. Thus $I \subseteq (t^n)$. By our choice of n, there is some power series $f_0(t)$ in I which is not divisible by t^{n+1}, in which case $f_0(t) = t^n g_0(t)$, where $g_0(t)$ has a nonzero constant term. But then $g_0(t)$ is a unit, and so has an inverse $h(t)$, in which case $t^n = f(t)h(t)$ is in I. Since $t^n \in I$, then $(t^n) \subseteq I$. Thus $(t^n) = I$.

3. Do either part (a) or part (b). Do not do both.

(a) Do problem 29 in Section 3 of Chapter 10.

SOLUTION. Consider the ring $R = \mathbf{Z}$ and the ideals (2) and (9). Their union contains 2 and 9, but not their sum $2 + 9 = 11$. Thus their union is not closed under addition, and so is not an ideal.

Now let R be any ring, and let I and J be ideals of R. I want to show that $I + J$ is an ideal. I have to show that it's a subgroup of R under addition. There are various ways to do this; one of them is to show that $I + J$ is nonempty, and to show that for all $x, y \in I + J$, $x - y$ is in $I + J$. Certainly $I + J$ is nonempty, since it contains $0 = 0 + 0$. Now let x and y be elements of $I + J$; this means that we can write x as a sum $x = a + b$ where $a \in I$ and $b \in J$; similarly, $y = c + d$ where $c \in I$ and $d \in J$. Then

$$x - y = (a + b) - (c + d) = (a - c) + (b - d).$$

Since I is an ideal, $a - c \in I$; since J is an ideal, $b - d \in J$. Thus the sum of these two is in $I + J$, as desired.

Also, I have to show that if $x = a + b$ is in $I + J$ (a and b as above) and if $r \in R$, then $rx \in I + J$. Well, $rx = ra + rb$, and $ra \in I$ because I is an ideal, and $rb \in J$ because J is an ideal.

(b) Describe the ring $\mathbf{R}[x]/(3x^2 + 7)$. (As usual, $\mathbf{R}$ denotes the real numbers.)

SOLUTION. This ring is isomorphic to $\mathbf{C}$. I'll use the first isomorphism theorem to prove it. Define a ring homomorphism $\varphi : \mathbf{R}[x] \to \mathbf{C}$ by $\varphi(f(x)) = f(i\sqrt{7/3})$. (In other words, φ is the substitution homomorphism $x \mapsto i\sqrt{7/3}$.) This is onto: any complex number $a + bi$ is equal to $a + bi\sqrt{7/3}\sqrt{3/7}$, and so is equal to $\varphi(a + b\sqrt{3/7}x)$. The kernel of φ consists of all real polynomials which have $i\sqrt{7/3}$ as a root. In particular, the kernel contains $3x^2 + 7$, so it contains the ideal $(3x^2 + 7)$. Also, if $f(x)$ is a real polynomial with $i\sqrt{7/3}$ as a root, then it also has $-i\sqrt{7/3}$ as a root, and so is divisible by

$$(x - i\sqrt{7/3})(x + i\sqrt{7/3}) = x^2 + 7/3.$$

So it's divisible by $3x^2 + 7$. Therefore the kernel is contained in the ideal $(3x^2 + 7)$. Now apply the first isomorphism theorem.

4. Let R be a ring and let I be an ideal. The *radical* of I is the set

$$\sqrt{I} = \{\, r \in R : \text{some power of } r \text{ is in } I \,\}.$$

(Do both parts.)

(a) Show that $\sqrt{I}$ is an ideal.

SOLUTION. First I'll show that $\sqrt{I}$ is a subgroup under addition. First of all, $\sqrt{I}$ contains 0: an element r of R is in $\sqrt{I}$ if and only some power of r is in I. Well, $0^1 = 0$ is in I, so $0 \in \sqrt{I}$. Next, suppose that $x \in \sqrt{I}$; this means that $x^n \in I$ for some n. $(-x)^n = (\pm 1)x^n$; since x^n is in I, so is $(\pm 1)x^n$. Thus $-x$ is in $\sqrt{I}$. Finally, suppose that x and y are two elements of $\sqrt{I}$. I have to show that $x + y \in \sqrt{I}$. Suppose that $x^m \in I$ and $y^n \in I$; then I claim that $(x + y)^{m+n-1}$ is in I (in which case $x + y$ is in $\sqrt{I}$). I know that

$$(x + y)^{m+n-1} = \sum_{i=0}^{m+n-1} c_i x^i y^{m+n-1-i}$$

where c_i is some binomial coefficient that I don't care about. I'll break this into two sums:

$$(x + y)^{m+n-1} = \sum_{i=0}^{m-1} c_i x^i y^{m+n-1-i} + \sum_{i=m}^{m+n-1} c_i x^i y^{m+n-1-i}.$$

In the first sum, every term is a multiple of y^n—an element of I. In the second sum, every term is a multiple of x^m—an element of I. Hence the whole sum is in I.

Second, I have to show that if $x \in \sqrt{I}$ and $r \in R$, then $rx \in \sqrt{I}$. If $x \in \sqrt{I}$, then $x^n \in I$ for some n. Then $r^n x^n \in I$, because I is an ideal. But $r^n x^n = (rx)^n$, so $rx \in \sqrt{I}$.

(b) Let $R = \mathbf{Z}$ and $I = (8)$. What is $\sqrt{(8)}$?

SOLUTION. $\sqrt{(8)} = (2)$. For every even number $2n$, $(2n)^3 = 8n^3 \in (8)$. Since some power of $2n$ is in (8), I can conclude that $2n \in \sqrt{(8)}$. Thus $(2) \subseteq \sqrt{(8)}$. To show the other inclusion, assume that $m \in \sqrt{(8)}$. Then some power of m is in (8): some power of m is divisible by 8. Then m can't be odd: m must be divisible by 2, so $m \in (2)$. Thus $\sqrt{(8)} \subseteq (2)$.

5. Let F be a field. A polynomial $f(x)$ in $F[x]$ is *irreducible* if $f(x)$ can't be factored in any nontrivial way: if $f(x) = g(x)h(x)$ with $g(x), h(x) \in F[x]$, then either $g(x)$ or $h(x)$ is a constant. For example, $x^2 + 1$ is irreducible in the ring $\mathbf{R}[x]$, but it's not irreducible in $\mathbf{C}[x]$.

(Do both parts.)

(a) Let p be a prime number and let $\mathbf{F}_p$ denote the field $\mathbf{Z}/p\mathbf{Z}$. If $f(x) \in \mathbf{F}_p[x]$ is an irreducible polynomial of degree n, show that $\mathbf{F}_p[x]/(f(x))$ is a field with p^n elements.

SOLUTION. To show that $\mathbf{F}_p[x]/(f(x))$ is a field, it suffices to show that $(f(x))$ is a maximal ideal of $\mathbf{F}_p[x]$. Suppose that $(f(x))$ is contained in an ideal I. Every ideal in $\mathbf{F}_p[x]$ is principal, so $I = (g(x))$ for some polynomial $g(x)$. Since $(f(x)) \subseteq (g(x))$, I can conclude that $f(x)$ is a multiple of $g(x)$: $f(x) = g(x)h(x)$. Since $f(x)$ is irreducible, either $g(x)$ is a constant, in which case $(g(x)) = (1)$, or $h(x)$ is a constant, in which case $h(x)$ is a unit so $(f(x)) = (g(x))$. Thus $(f(x))$ is a maximal ideal, and $\mathbf{F}_p[x]/(f(x))$ is a field.

Note that I can multiply $f(x)$ by a nonzero constant c to get a monic polynomial $m(x)$: $m(x) = cf(x)$. Then $(f(x)) = (m(x))$, so $\mathbf{F}_p[x]/(f(x)) = \mathbf{F}_p[x]/(m(x))$. By a result from class (and in the book), there is a bijection between $\mathbf{F}_p[x]/(m(x))$ and length n vectors $(a_0, \dots, a_{n-1})$ with entries in $\mathbf{F}_p$. Since $\mathbf{F}_p$ has p elements, there are p^n such vectors. Thus $\mathbf{F}_p[x]/(f(x))$ has p^n elements.

(b) Use the result from part (a) to construct a field with 9 elements.

SOLUTION. If I can find a degree 2 irreducible polynomial in $\mathbf{F}_3[x]$, I can apply part (a). I claim that $x^2 + 1$ is irreducible, so that $\mathbf{F}_3[x]/(x^2 + 1)$ is a field with 9 elements. To verify that $x^2 + 1$ is irreducible, I have to show that it can't be factored. Since it has degree 2, the only nontrivial way to factor it would be as a product of linear polynomials; hence it factors if and only if it has roots. It's easy to check that it doesn't have any roots: just plug in 0, 1, and 2—you never get 0.