MATH 113: HW 12: Ideals, Polynomial rings

Due in class on Thursday, November 30.

1. (10 pts) Section 22, Exercises 4 and 16.

   SOLUTIONS:

   (4)

$$\begin{aligned} f(x) + g(x) &= (2x^3 + 4x^2 + 3x + 2) + 3x^4 + 2x + 4 \\ &= 3x^4 + 2x^3 + (3+2)x + 6 \\ &= 3x^4 + 2x^3 + 1 \end{aligned}$$

   (16)

$$\begin{aligned} \phi_3(x^{231} + 3x^{117} - 2x^{53} + 1) &= 3^{231} + 3^{118} - 2 * 3^5 3 + 1 \\ &= 3^{57*4+3} + 3^{4*29+2} - 2 * 3^{13*4+1} + 1 \\ &\equiv 3^3 + 3^2 - 2 * 3 + 1 \mod 5 \quad \text{(Fermat)} \\ &\equiv 27 + 9 - 6 + 1 \mod 5 \\ &\equiv 31 \mod 5 \\ &\equiv 1 \mod 5 \end{aligned}$$

2. (8 pts) Prove that D is an integral domain implies that $D[x]$ is an integral domain.

   SOLUTION:

   Theorem 22.2 implies that since D is a commutative ring with unity, $D[x]$ is a commutative ring with unity. We must therefore prove that $D[x]$ does not contain any zero divisors. Consider

$$f(x) = \sum_{i=0}^{n} a_i x^i, \qquad g(x) = \sum_{i=0}^{m} b_i x^i, \qquad f(x)g(x) = 0.$$

   Then each coefficient of $f(x)g(x)$ must equal 0.

   <u>Short solution</u>

   Consider the largest positive integer m such that $a_m \neq 0$ and the largest positive integer n such that $b_n \neq 0$. Then the coefficient of x^{m+n} is $a_m b_n$. But D is an integral domain, so $a_m b_n \neq 0$. So $f(x)g(x) \neq 0$.

Long solution

$$f(x)g(x) = \sum_{k=0}^{m+n} x^k \sum_{j=0}^{k} a_j b_{k-j}.$$

We'll prove that either $f(x)$ or $g(x)$ is zero, by induction on the first k coefficients of either $f(x)$ or $g(x)$.

Base case: So $a_0 b_0 = 0$, which means either $a_0 = -$ or $b_0 = 0$.

Inductive step: Assume that $a_i = 0$ for $i \leq k$. Then $\sum_{j=0}^{k+1} a_j b_{k+1-j} = 0 \Rightarrow a_{k+1} b_0 = 0$. Therefore either $a_{k+1} = 0$ or $b_0 = 0$ since D is an integral domain. If $a_{k+1} = 0$, we are done. So assume that $b_0 = 0$. Then $\sum_{j=0}^{k+2} a_j b_{k+2-j} = 0 \Rightarrow a_{k+1} b_1 = 0$. Continuing this process, assuming that $a_{k+1} \neq 0$, we see that $b_i = 0$ for i from 0 to $m + n - (k+1)$. But the degree of $f(x)$ is greater than or equal to $k+1$. So $b_i = 0$ for all i.

3. (8 pts) Let p be a positive prime integer. Prove that $\sqrt{p} \notin \mathbb{Q}$.

   SOLUTION:

   Assume that $\sqrt{p} \in \mathbb{Q}$. Then $\sqrt{p} = \frac{a}{b}$, where $\frac{a}{b}$ is in lowest terms. Then $p = \frac{a^2}{b^2} \Rightarrow b^2 p = a^2$. So p divides a^2. Since p is prime, this means that p divides a. Therefore $a = pk$ for some k, which means that $p = \frac{p^2k^2}{b^2}$. Thus $b^2 p = p^2 k^2$. Divide both sides by p to get $b^2 = pk^2$. So p divides b. But this contradicts the assumption that $\frac{a}{b}$ was in lowest terms.

4. (12 pts) Section 23, Exercises 2 and 6.

   SOLUTION:

   (2) $f(x) = [5x^4 + 5x^2 + 6x]g(x) + (x+2)$ Solve using long division.

   (4) The generators are 3 and 5.

5. (4 pts) Determine whether or not the polynomial $f(x) = 3x^9 - 16x^3 + 32x^2 - 18$ is irreducible over $\mathbb{Q}$?

   SOLUTION:

Eisenstein's Criterion for $p = 2$ applies, since 2 divides all coefficients except the first and $2^2 = 4$ does not divide the last coefficient. Therefore the polynomial is irreducible over $\mathbb{Q}$.

6. (8 pts) Section 26, Exercise 14.

   SOLUTION:

   Let $R = \mathbb{Z}_6$. The elements 2 and 3 are zero divisors in this ring. The ideal generated by 2 is the ideal $\langle 2 \rangle = \{0, 2, 4\}$. The factor ring $R/\langle 2 \rangle$ consists of two cosets and is isomorphic to $\mathbb{Z}_2$, which is an integral domain.

7. (10 pts) Let R be a ring and $\phi : R \to R'$ a non-trivial ring homomorphism. For the following two statements, provide either a proof or a counterexample.

   (a) If a is a unit in R, then $\phi(a)$ is a unit in R'.

   SOLUTION: (many possibilities)

   Let $R = \mathbb{Z}$ and let $R' = R \times R$. Let $\phi(z) = (z, 0)$. The multiplicative identity in $R \times R$ is $(1, 1)$. The element -1 is a unit in R but $\phi(-1) = (-1, 0)$ is not a unit in $R \times R$ since $(-1, 0)(a, b) = (-a, 0) \neq (1, 1)$ for any choice (a, b).

   (b) If a is a zero divisor in R, then $\phi(a)$ is a zero divisor in R'.

   SOLUTION: Let $R = \mathbb{Z}_6$. Then 3 is a zero divisor in R. Let

   $$\phi : R \to \mathbb{Z}_6/\langle 2 \rangle$$

   be defined by $\phi(a) = a + \langle 2 \rangle$. So $\phi(3)$ is the multiplicative identity in R'. So $\phi(3)$ is not a zero divisor in R'.

GROUP PROBLEM (Presented in class on Tuesday, November 28)

Section 26, Exercise 20.

$\underline{\phi_p(ab) = \phi_p(a)\phi_p(b)}$
$\phi_p(ab) = (ab)^p = a^p b^p = \phi_p(a)\phi_p(b)$, since R is commutative.

$\underline{\phi_p(a+b)\phi_p(a) + \phi_p(b)}$
We need the binomial theorem: For $a, b \in R$,

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}.$$

proof:
BASE CASE:

$$\begin{aligned}(a+b)^1 &= b + a \\ &= a^0 b^1 + a^1 b^0 \\ &= \sum_{i=0}^{1} \binom{1}{i} a^i b^{1-i}\end{aligned}$$

Assume the theorem is true for all positive integers less than or equal to k. Then consider $k+1$.

$$\begin{aligned}(a+b)^{k+1} &= (a+b)^k (a+b) \\ &= (\sum_{i=0}^{k} \binom{k}{i} a^i b^{k-i})(a+b) \\ &= \sum_{i=0}^{k} \binom{k}{i} a^{i+1} b^{k-i} + \sum_{i=0}^{k} \binom{k}{i} a^i b^{k-i+1} \\ &= \sum_{i=1}^{k+1} \binom{k}{i-1} a^i b^{k+1-i} + \sum_{i=0}^{k} \binom{k}{i} a^i b^{k+1-i} \\ &= \binom{k}{k} a^{k+1} b^0 + \sum_{i=1}^{k} \binom{k}{i-1} a^i b^{k+1-i} + \sum_{i=1}^{k} \binom{k}{i} a^i b^{k+1-i} + \binom{k}{0} a^0 b^{k+1} \\ &= a^{k+1} + b^{k+1} + \sum_{i=1}^{k} \binom{k+1}{i} a^i b^{k+1-i} \\ &= \sum_{i=0}^{k+1} \binom{k+1}{i} a^i b^{k+1-i}\end{aligned}$$

So

$$\begin{aligned}\phi_p(a+b) &= (a+b)^p \\ &= \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i} \\ &= a^p + b^p + \sum_{i=1}^{p-1} \binom{p}{i} a^i b^{p-i}\end{aligned}$$

But $\binom{p}{i}$ is divisible by p for i between 1 and $p-1$. Since the characteristic of R is p, each term in the sum becomes zero and we are left with $a^p + b^p$.