# 412 Individual HW3

Jack Madden

February 2024

## Problem 1

Take polynomials $a_nx^n + \cdots + a_0,\ b_mx^m + \cdots + b_0,\ c_kx^k + \cdots + c_0, \in R[x]$ and without loss of generality let $m \geq k$. Then, we have:

$$(a_nx^n + \cdots + a_0) \cdot (b_mx^m + \cdots + b_0 + c_kx^k + \cdots + c_0)$$

$$(a_nx^n + \cdots + a_0) \cdot ((b_m + c_m)x^m + \cdots + (b_k + c_k)x^k + \cdots (b_0 + c_0))$$

$$(a_nx^n + \cdots + a_0) \cdot \left(\sum_{i=0}^{m} (b_i + c_i)x^i\right)$$

$$a_nx^n \cdot \left(\sum_{i=0}^{m} (b_i + c_i)x^i\right) + \cdots + a_0 \cdot \left(\sum_{i=0}^{m} (b_i + c_i)x^i\right)$$

$$\left(\sum_{i=0}^{m} a_n(b_i + c_i)x^{i+n}\right) + \cdots + \left(\sum_{i=0}^{m} a_0(b_i + c_i)x^i\right)$$

By the distributivity of $R$ we have:

$$\left(\sum_{i=0}^{m} a_nb_ix^{i+n} + a_nc_ix^{i+n}\right) + \cdots + \left(\sum_{i=0}^{m} a_0b_ix^i + a_ic_ix^i\right)$$

Splitting and rearranging the sums:

$$\left(\sum_{i=0}^{m} a_nb_ix^{i+n} + \cdots + \sum_{i=0}^{m} a_0b_ix^i\right) + \left(\sum_{i=0}^{k} a_nc_ix^{i+n} + \cdots + \sum_{i=0}^{k} a_0c_ix^i\right)$$

$$\left(a_nx^n \sum_{i=0}^{m} b_ix^i + \cdots + a_0 \sum_{i=0}^{m} b_ix^i\right) + \left(a_nx^n \sum_{i=0}^{k} c_ix^i + \cdots + a_0 \sum_{i=0}^{k} c_ix^i\right)$$

$$\left((a_nx^n + \cdots + a_0) \cdot \sum_{i=0}^{m} b_ix^i\right) + \left((a_nx^n + \cdots + a_0) \cdot \sum_{i=0}^{k} c_ix^i\right)$$

$$((a_nx^n + \cdots + a_0) \cdot (b_mx^m + \cdots + b_0)) + ((a_nx^n + \cdots + a_0) + (c_kx^k + \cdots + c_0))$$

## Problem 2

a) By the rational roots test, we know that the roots of this polynomial are either 1, or -1. Neither of these are roots so this polynomial has no roots in $\mathbb{Q}$.

b) We can solve this problem using the quadratic formula.

c) The zeroes of this equation will be all $x \in \mathbb{Z}_5$ such that $x^5 = 1$. By Fermat's little theorem, we have that $x^5 = x \ mod\ 5$ for all $x \in \mathbb{Z}$. Thus, we can see that the only zero is therefore 1.

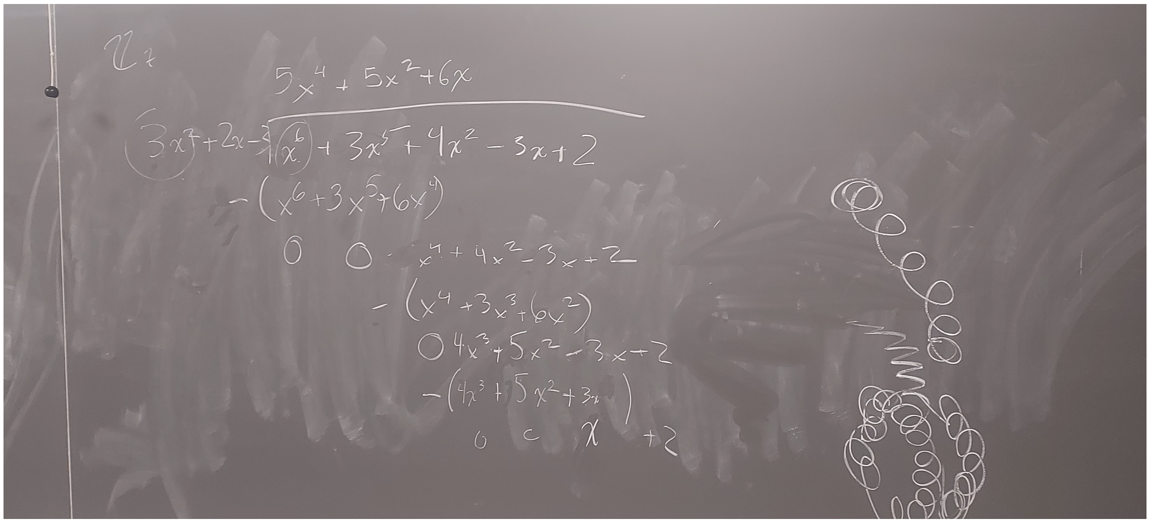
d) Using some facts about complex numbers that are outside of the content of this course we see that we are finding the fifth roots of unity of 1, which are $1, e^{i\frac{2\pi}{5}}, e^{-i\frac{2\pi}{5}}, e^{i\frac{4\pi}{5}}, e^{-i\frac{4\pi}{5}}$. Since there are at most 5 roots, and we have found 5 roots, we have found them all.

## Problem 3

a) Take two non-zero polynomials $a, b$ in $R[x]$ and let them have degrees $k$ and $m$. Then the leading term of $a \cdot b$ will be $(a_k \cdot b_m)x^{k+m}$. We know that $a_k, b_m \neq 0$ because we stated that the polynomials have degree $k$ and $m$. Thus, since $R$ is an integral domain their product will not be zero, and therefore the product of the two non-zero polynomials will have at least one non-zero term and therefore will not be zero. Thus, $R[x]$ is an integral domain.

b) Continuing from the previous argument, we see that the product of two non-zero polynomials in an integral domain $a, b$ will have degree $deg(a) + deg(b)$. Since the unity in $R[x]$ has degree 0, we can only multiply two polynomials of degree zero, i.e. constant polynomials to get the unit. Furthermore, these constant polynomials must have coefficients which are units in $R$.

## Problem 4


$\mathbb{Z}_7$
$5x^4 + 5x^2 + 6x$
$3x^2 + 2x - 3 \,|\, x^6 + 3x^5 + 4x^2 - 3x + 2$
$-(x^6 + 3x^5 + 6x^4)$
$0 \quad 0 \quad x^4 + 4x^2 - 3x + 2$
$-(x^4 + 3x^3 + 6x^2)$
$0 \quad 4x^3 + 5x^2 - 3x + 2$
$-(4x^3 + 5x^2 + 3x)$
$0 \quad 0 \quad x \quad +2$

$x^6 + 3x^5 + 4x^2 - 3x + 2 = (5x^4 + 5x^2 + 6x)(3x^2 + 2x - 3) + (x + 2).$

## Problem 5

After brute-forcing the numbers 1 through 10, we find that the polynomial has zeros at 3, 4, and 8. These will then be our linear factors. $(x - 3)(x - 4)(x - 8)$, but we must multiply by 2 as leading coefficient has 2 term. This yields $2(x - 3)(x - 4)(x - 8)/$

## Problem 6

a) We apply the rational root test and see that rational roots will be one of the following, 1, 2, 4, 8, -1, -2, -4, -8. We can plug them in and see that none work. Then, since the polynomial is of degree 3, having no roots implies that the polynomial is irreducible.

b) We can apply Eienstein's criterion, take $p = 3$.

c) Observe that this polynomial is same as $(x + 1)^5 + 3$. We perform a linear change of basis and see that this will have the same reducibility as $x^5 + 3$, which is irreducible under Eisenstein's criterion for $p = 3$.

## Problem 7

We have that there are $(p - 1)p^2$ total quadratic polynomials in $\mathbb{Z}_p[x]$, as for $ax^2 + bx + c \in \mathbb{Z}_p[x]$, there are $p - 1$ ways to choose $a$ (cannot be 0), and $p$ ways to choose $b$ and $c$. We see that all reducible polynomials can be written in the form $a(x - b)(x - c)$. We have that there are $(p - 1)$ ways to choose $a$, and $p^2 - \frac{p(p-1)}{2}$ ways to choose $c$ and $d$. The reason for the inclusion of the $\frac{p(p-1)}{2}$ term is to prevent the double counting when $c$ and $b$ are distinct but in different orders as this multiplication is commutative. Now that we have found the number of reducible polynomials we need only subtract that from the number of total polynomials to get the number of irreducible polynomials.

$$(p - 1)p^2 - (p - 1)\left(p^2 - \frac{p(p - 1)}{2}\right)$$

$$(p - 1)\left(p^2 - p^2 + \frac{p(p - 1)}{2}\right)$$

$$\frac{p(p - 1)^2}{2}$$

is the number of irreducible polynomials in $\mathbb{Z}_p[x]$.

# Problem 8

The ideals of $\mathbb{Z}_{12}$ are a subset of the additive subgroups of $\mathbb{Z}_{12}$, which we know to be $\langle 0\rangle, \langle 1\rangle, \langle 2\rangle, \langle 3\rangle, \langle 4\rangle, \langle 6\rangle$. Now, we show that for any factor $k$ of $n$, $k\ell$ will be a multiple of $k$ mod $n$ for any $\ell$. Let $k, m, n, q, r \in \mathbb{Z}$

$$n = km$$

$$\ell k = nq + r$$

$$\ell k = kmq + r$$

$$\ell k - kmq + r$$

$$k(\ell - mq) = r$$

so we see that is is a multiple of $k$ mod $n$. Thus, for any of the subgroups we listed, they are additive subgroups and also satisfy the multiplication requirement of the ideal and are all therefore ideals. We then have that $\mathbb{Z}_{12}/\langle 1\rangle \cong \mathbb{Z}_1$, $\mathbb{Z}_{12}/\langle 2\rangle \cong \mathbb{Z}_2$, $\mathbb{Z}_{12}/\langle 3\rangle \cong \mathbb{Z}_3$, $\mathbb{Z}_{12}/\langle 4\rangle \cong \mathbb{Z}_4$, $\mathbb{Z}_{12}/\langle 6\rangle \cong \mathbb{Z}_6, \mathbb{Z}_{12}/\langle 0\rangle \cong \mathbb{Z}_{12}$.

# Problem 9

Every ring homomorphism has a kernel, and that kernel is an ideal. Since a field has only the improper and trivial ideal, for a homomorphism $\phi : F \to R$, $ker(\phi) = F, ker(\phi) = \{0\}$. If $ker(\phi) = F$, then clearly $\phi$ maps everything to zero. Otherwise, let $ker(\phi) = \{0\}$. We will show that this implies that if $\phi(r) = \phi(s)$, $r = s$ and therefore $\phi$ is injective.

$$\phi(r) = \phi(s)$$

$$\phi(r) - \phi(s) = 0$$

$$\phi(r - s) = 0$$

By the fact that $ker(\phi) = \{0\}$, we have that $r - s = 0$ and therefore $r = s$, showing that $\phi$ is one to one.

# Problem 10

We have that

$$(x + y)^p = \sum_{i=0}^{p} \binom{p}{i} x^{p-i} y^i$$

due to the commutativity of the ring. If we can show that $p \mid \binom{p}{i}$ when $i \neq 0, p$, then every term other than $x^p$ and $y^p$ will become zero as in the statement we know that the ring has characteristic $p$. We have that:

$$\binom{p}{i} = \frac{p!}{i!(p-i)!}$$

We observe that if $i \neq 0, p$, then all the terms in the product in the denominator will be less than $p$. Since $\binom{p}{i}$ is an integer, and $p$ has no divisors but itself, we see that that product must be dividing other terms in the numerator and thus

$$\binom{p}{i} = p(k)$$

for some integer $k$ We may then rewrite the sum as:

$$(x+y)^p = x^p + pk_1 \cdot \left(x^{p-1}y\right) + \cdots + pk_{p-1} \cdot \left(xy^{p-1}\right) + y^p$$

Then, by definiton of the characeristic of the ring this sum becomes:

$$x^p + y^p = (x+y)^p$$

Showing that $(xy)^p = x^p y^p$ is much simpler:

$$(xy)^p = \overbrace{xy \cdots xy}^{ptimes} = x^p y^p$$

as this just follows from the commutativity of the ring.

# Problem 11

a) Let $r \in R$, and let $x$ be any element of $R$ such that $\phi(x) \in I$. Suppose that $\phi(rx) \notin I$, i.e $rx \notin \phi^{-1}(I)$. But $\phi(rx) = \phi(r)\phi(x)$, and since $\phi(x) \in I$, $\phi(r)\phi(x) = \phi(rx) \in I$. Contradiction. Also, we have from Math 411 that subgroups correspond to subgroups under group homomorhpism so $\phi^{-1}(I)$ is an additive subgroup.

b) Let $N$ be an ideal in $R$. Take arbitrary $\phi(a) \in \phi(R), a \in R$, and arbitrary $\phi(n), n \in N$. Then $\phi(a)\phi(n) = \phi(an)$. Since $an \in N, \phi(an) \in \phi(N)$ and $\phi(N)$ is an ideal in $\phi(R)$. $\phi(N)$ is also an additive subgroup as ring (group) homomorhpisms map subgroups to subgroups, and $N$ is a subgroup.

# Problem 12

Let us take $r \in \sqrt{I}$. We then have that $ra \in \sqrt{I}$ for all $a \in R$. We have $k$ such that $r^k \in I$. Then, $(ra)^k = r^k a^k$(commutativity). Since $r^k$ is in $I$, $r^k a^k = (ra)^k$ is also in $I$, and therefore $ra \in \sqrt{I}$ for arbitrary $a \in R$. We also must show that $\sqrt{I}$ is an additive subgroup. We have that $0^1 \in I$, and thus $0 \in \sqrt{I}$. Also, let $r \in \sqrt{I}$. Then we have $-r$ such that $r + -r = 0$. Take $(-r)^k$. We know that this is either $-(r^k)$ or $r^k$. Clearly $r^k \in I$. Also, since $I$ is a subgroup, $-(r^k)$ also in $I$. Thus it is closed under inverses. Lastly, we show closure. Suppose $x^k \in I$ and $y^{k'} \in I$. Then $x, y \in \sqrt{I}$. We must show that $(x+y)^n \in I$ for some $n$. Choose $n = k + k'$. Then

$$(x+y)^{k+k'} = x^k x^{k'} + x^k x^{k'-1} y + \cdots + x^k y^{k'} + \cdots xy^{k-1} y^{k'} + y^k yk'$$

We can see that every term in this sum will contain either the factor $x^k$ or $y^{k'}$. Thus all terms are in $I$ and therefore their sum is in $I$ as it is a subgroup. Thus, $x + y \in \sqrt{I}$.

# Problem 13

We will show that for two ideals $I$ and $J$ in a ring $R$, $I \cap J$ is also an ideal. Take $x \in I \cap J$. Then for any $a \in R$, $ax \in I$ and $ax \in J$ and therefore $ax \in I \cap J$ and thus we have satisfied this requirement. Also, we must show that it is the additive subgroup. Since every ideal contains zero, and therefore $I$ and $J$ both contain zero, then $I \cap J$ will contain zero. Also, take $x \in I \cap J$. Then $-x \in I$ and $-x \in J$ as $I$ and $J$ are addidive subgroups, and therefore $-x \in I \cap J$. Furthermore, take $x, y$ in $I \cap J$, and $a \in R$. We will show that $I \cap J$ is closed under addition, that is $x + y \in I \cap J$. $a(x + y)$ is $ax + ay$ by distributivity. $ax \in I$ and $ay \in I$ and therefore $ax + ay \in I$ as it is a subgroup. By the same argument, $ax + ay \in J$. Therefore, $ax + ay \in I \cap J$ for arbitrary $a$ and thus $I \cap J$ is closed and therefore a subgroup.

As a counterexample for union, take $\langle 2 \rangle \cup \langle 3 \rangle$. $2 \in \langle 2 \rangle, 3 \in \langle 3 \rangle$. But $2 + 3 = 5 \notin \langle 2 \rangle \cup \langle 3 \rangle$ so it is not closed under addition so not subgroup so not ideal.

# Problem 14

We can show that this is an ideal as follows. For any $f(x) \in \mathbb{R}[x]$, and any $g(x) = (x^2+1)g'(x) \in I$, $f(x)g(x) = (x^2 + 1)f(x)g'(x) \in I$. It is also an additive subgroup, as $0 = (x^2 + 1) \cdot 0$, and if $f(x) = (x^2 + 1)f'(x) \in I$, $-f(x) = -(x^2 + 1)f'(x) \in I$, and if $f(x) = (x^2 + 1)f'(x), g(x) = (x^2 + 1)g'(x) \in I, (x^2 + 1)f'(x) + (x^2 + 1)g'(x) = (x^2 + 1)(f'(x) + g'(x))$ by distributivity.