MATH 315 Assignment 5

Instructor: Dr. Thomas Bitoun
Name: Yifeng Pan
UCID: 30063828

Winter 2020

Instructions

1. Any source MUST be cited. If you use somebody else's solution, you must demonstrate to the grader that you understand the proof you are using.
2. For each problem, you MUST indicate, along with your solution, the people you have been discussing the problem with. This includes the instructor and the TA. If you haven't discussed the problem with anyone, write so along with your solution, for each problem.
3. Write your solutions in your own words, and legibly. Please don't overcrowd your answers with unnecessary arguments.
4. Please submit your solutions as a portrait-oriented pdf and put your name in the filename.

With the exception of Problem (1.3), I completed every problem independently without discussion with anyone.

Sources are cited inline.

1

1.1 What is the polynomial in $\mathbb{R}[x]$ which is monic of degree 4, with roots $\{1, 2, 3\}$ such that the root 1 has multiplicity 2?

[1] We need root $\{1, 2, 3\}$. So $(x-1)^a(x-2)^b(x-3)^c$.

Since degree is 4, $a + b + c = 4$.

Root 1 has multiplicity 2, so $a = 2$.

Therefore we have $(x-1)^2(x-2)(x-3)$.

1.2 Determine the monic divisors of $2x^3 - 4x^2 + 2x - 4$ in $\mathbb{Q}[x]$. Justify your answer.

[2] $\mathbb{Q}[x]$ is a UFD, so we have to find it's irreducible factors.

By inspection 2 is a root, so $(x-2)$ is a factor, and $2x^3 - 4x^2 + 2x - 4 = (x-2)(2x^2+2)$.

So $x^3 - 4x^2 + 2x - 4 = 2(x-2)(x^2+1)$.

The monic divisors are $\{(x-2), (x^2+1), (x-2)(x^2+1)\}$.

1.3 Determine the monic irreducible polynomials of degree 3 over $\mathbb{Z}/3\mathbb{Z}[x]$. Justify your answer.

We need to find all (a, b, c), such that $x^3 + ax^2 + bx + c$ is irreducible in $\mathbb{Z}/3\mathbb{Z}$.

There are only $3^3 = 27$ polynomials to check.

$c \neq 0$, otherwise x is a factor.

Since $\mathbb{Z}/3\mathbb{Z}$ is a field, and therefore a UFD, $x^3 + ax^2 + bx + c$ has one of the following irreducible factor forms:

1. $(x-i)(x-j)(x-k)$.
2. $(x^2 + ix + j)(x-k)$.
3. $x^3 + ix^2 + jx + k$.

Therefore, if $x^3 + ax^2 + bx + c$ is reducible, then it has a constant factor. [3]

Evaluating each (a, b, c) at $x \in \mathbb{Z}/3\mathbb{Z}$ requires $3 * 3 * 2 * 3 = 54$ computations, which can easily be done with lazy for-loops:

```
int p = 3;
for(int i = 0; i < p; ++i)
    for(int j = 0; j < p; ++j)
        for(int k = 0; k < p; ++k){
            bool irr = true;
            for(int x = 0; x < p; ++x)
                if ((x*x*x + i*x*x + j*x + k) % p == 0)
                    irr = false;
            if(irr)
                std::cout << "(" << i << ", " << j << ", " << k << "), \n";
        }
```

We get $x^3 + ax^2 + bx + c$ for $(a, b, c) \in \{(0, 2, 1), (0, 2, 2), (1, 0, 2), (1, 1, 2), (1, 2, 1), (2, 0, 1), (2, 1, 1), (2, 2, 2)\}$

[1] Reference: `https://en.wikipedia.org/wiki/Multiplicity_(mathematics)#Multiplicity_of_a_root_of_a_polynomial`

[2] Reference: `https://en.wikipedia.org/wiki/Principal_ideal_domain#Examples`

[3] Devin Kwok (UCID: 10016484) pointed this out to me. Before, I was calculating the image of $\{(i, j, k)\}$ and subtracting that from $\{(a, b, c)\}$ to get the irreducible solutions.

2

2.1 Using the division algorithm, find the greatest common divisor of $x^4 + x + 1$ and $x^3 + 2$ in $\mathbb{Q}[x]$ and express it as a linear combination of these polynomials. Explain your computation.

i	r	s	t	$q = r_{i-1}/r_i$
0	$x^4 + x + 1$	1	0	$-$
1	$x^3 + 2$	0	1	x
2	$(x^4 + x + 1) - x(x^3 + 2) = -x + 1$	1	$-x$	$-x^2$
3	$(x^3 + 2) - (-x^2)(-x + 1) = x^2 + 2$	x^2	$1 - x^3$	0
4	$(-x + 1) - 0(x^2 + 2) = -x + 1$	1	$-x$	$-x$
5	$(x^2 + 2) - (-x)(-x + 1) = x + 2$	$x^2 + x$	$1 - x^3 - x^2$	-1
6	$(-x + 1) - (-1)(x + 2) = 3$	$1 + x^2 + x$	$1 - x^3 - x^2 - x$	$(x + 2)/3$
7	$(x + 2) - ((x + 2)/3)(3) = 0$	$s_5 - s_6q_6$	$t_5 - t_6q_6$	$-$

[4] where $s_5 - s_6q_6 = (x^2 + x) - \frac{x+2}{3}(1 + x^2 + x) = \frac{-x^3-2}{3}$, [5]
and $t_5 - t_6q_6 = (1 - x^3 - x^2) - \frac{x+2}{3}(1 - x^3 - x^2 - x) = \frac{x^4+x+1}{3}$.

$r_6 = 3 = r_0s_6 + r_1t_6 = (x^4 + x + 1)(1 + x^2 + x) + (x^3 + 2)(1 - x^3 - x^2 - x)$.

$\gcd(x^4 + x + 1, x^3 + 2) = 1$ (Multiply the above by $1/3$).

2.2 Let $P, Q \in \mathbb{Z}[x]$. Prove that P and Q are relatively prime in $\mathbb{Q}[x]$ if and only if the ideal (P, Q) of $\mathbb{Z}[x]$ generated by P and Q contains a non-zero integer (i.e. $\mathbb{Z} \cap (P, Q) \neq \{0\}$). Here (P, Q) is the smallest ideal of $\mathbb{Z}[x]$ containing P and Q, $(P, Q) = \{\alpha P + \beta Q | \alpha, \beta \in \mathbb{Z}[x]\}$

Suppose P and Q are relatively prime in $\mathbb{Q}[x]$.

By definition of relatively prime, $\exists p(x), q(x) \in \mathbb{Q}[x]$ (henceforth refered to as p, q) such that $pP + qQ = 1$.

But $p = a/b$ for some $a \in \mathbb{Z}[x], b \in \mathbb{N}$ [6] , and $q = c/d$ for some $c \in \mathbb{Z}[x], d \in \mathbb{N}$.

So $pP + qQ = adP + cbQ = bd$, where $ad, cb \in \mathbb{Z}[x], bd \in \mathbb{N}$. Therefore $bd \in (P, Q)$.

Now, Suppose (P, Q) contains a non-zero integer $n \in \mathbb{Z} \setminus \{0\}$.

So $\exists a, b \in \mathbb{Z}[x]$ such that $aP + bQ = n$.

So for $a/n, b/n \in \mathbb{Q}[x]$, $a/nP + b/nQ = 1$.

Therefore P and Q are relatively prime in $\mathbb{Q}[x]$. □

2.3 For which primes p and which integers $n \geq 1$ is the polynomial $x^n - p$ irreducible in $\mathbb{Q}[x]$? Justify your answer.

Let p be a prime. Let $n \geq 1$.

By the Eisenstein Criterion: [7]
Since p divides $-p$, p^2 does not divide $-p$, and p does not divide 1, $(1)x^n + (-p) = x^n - p$ in irreducible in $\mathbb{Q}[x]$. □

[4] Reference: https://en.wikipedia.org/wiki/Polynomial_greatest_common_divisor#B%C3%A9zout's_identity_and_extended_GCD_algorithm

[5] Calculator: https://www.symbolab.com/.

[6] Let b be the lowest common multiple of the denominators of the coefficients of p in their irreducible fraction forms.

[7] Artin's Algebra, Proposition 12.4.6, Eisenstein Criterion.

3

3.1 Let α be the class of x in the quotient ring $\mathbb{Q}[x]/(f)$, where $f = x^4 + x^3 + x^2 + x + 1$. Find $a_0, a_1, a_2, a_3 \in \mathbb{Q}$ such that $(\alpha^3 + \alpha^2 + \alpha)(\alpha^5 + 1) = a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3$ in $\mathbb{Q}[x]/(f)$.

Let $I = (x^4 + x^3 + x^2 + x + 1)$, where $a \in R$.

Let $\alpha = [x] = x + I$.

Let $n \geq 1$. We have $[x]^n = (x + I)^n = x^n + I = [x^n]$.

Now, [8]

$$\begin{aligned}
(\alpha^3 + \alpha^2 + \alpha)(\alpha^5 + 1) &= \alpha^8 + \alpha^7 + \alpha^6 + \alpha^3 + \alpha^2 + \alpha \\
&= x^8 + x^7 + x^6 + x^3 + x^2 + x + I \\
&= x^8 + x^7 + x^6 + x^3 + x^2 + x + q(x^4 + x^3 + x^2 + x + 1), \text{ for any } q \in \mathbb{Q}[x] \\
&= x^8 + x^7 + x^6 + x^3 + x^2 + x + qx^4 + qx^3 + qx^2 + qx + q \\
&= (q + x^4)x^4 + (q + x^4 + 1)x^3 + (q + x^4 + 1)x^2 + (q + 1)x + q \\
&= (q + x^4 - 1)x^4 + (q + x^4 + 1)x^3 + (q + x^4 + 1)x^2 + (q + 1)x + (q + x^4) \\
&= (q + x^4 - x - 1)x^4 + (q + x^4 + 1)x^3 + (q + x^4 + 1)x^2 + (q + x^4 + 1)x + (q + x^4) \\
&= (q + x^4 - x)x^4 + (q + x^4 - x + 1)x^3 + (q + x^4 + 1)x^2 + (q + x^4 + 1)x + (q + x^4) \\
&= (q + x^4 - x)x^4 + (q + x^4 - x + 2)x^3 + (q + x^4 - x + 1)x^2 + (q + x^4 + 1)x + (q + x^4) \\
&= (q + x^4 - x)x^4 + (q + x^4 - x + 2)x^3 + (q + x^4 - x + 2)x^2 + (q + x^4 - x + 1)x + (q + x^4) \\
&= (q + x^4 - x)x^4 + (q + x^4 - x + 2)x^3 + (q + x^4 - x + 2)x^2 + (q + x^4 - x + 2)x + (q + x^4 - x) \\
&= px^4 + (p + a_3)x^3 + (p + a_2)x^2 + (p + a_1)x + (p + a_0) \\
&\quad \text{where } p = q + x^4 - x, \boxed{\boldsymbol{a_3 = 2, a_2 = 2, a_1 = 2, a_0 = 0}} \\
&= a_0 + a_1x + a_2x^2 + a_3x^3 + px^4 + px^3 + px^2 + px + p \\
&= a_0 + a_1x + a_2x^2 + a_3x^3 + p(x^4 + x^3 + x^2 + x + 1) \\
&= a_0 + a_1x + a_2x^2 + a_3x^3 + I \\
&= a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3
\end{aligned}$$

To verify, Suppose $q \in (\alpha^3 + \alpha^2 + \alpha)(\alpha^5 + 1)$.

So $q = x^8 + x^7 + x^6 + x^3 + x^2 + x + q(x^4 + x^3 + x^2 + x + 1)$, for some $q \in \mathbb{Q}[x]$

Then $q = 2x^3 + 2x^2 + 2x + p(x^4 + x^3 + x^2 + x + 1)$, where $p = q + x^4 - x \in \mathbb{Q}[x]$. [9] □

[8] There is a more concise way to do this, but I was tired of dividing polynomials after problem (2.2).

[9] The two equations are equal; Calculator: `https://www.symbolab.com/`.

3.2 Let $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Prove that $F = \mathbb{F}_2[x]/(x^3 + x + 1)$ is a field, but $\mathbb{F}_3[x]/(x^3 + x + 1)$ is not a field.

[10] $x^3 + x + 1$ is irreducible in $\mathbb{F}_2[x]$, but reducible in $\mathbb{F}_3[x]$.

Lemma 1. $\mathbb{F}_p[x]/(f(x))$ is a field $\iff$ $f(x)$ is irreducible in $\mathbb{F}_p[x]$.

[11] Proof: Suppose $f(x) \in \mathbb{F}_p[x]$ is irreducible (henceforth refered to as f).

Let $[g] \in \mathbb{F}_p[x]/(f)$, where $g \in \mathbb{F}_p[x] \setminus \{0\}$. We find the inverse of $[g]$.

Since f is irreducible, $\gcd(f, g) = c$ for some constant $c \in \mathbb{F}_p$. Otherwise, c would be a non-constant factor of f.

By Bézout's Identity used in (2.1):
$\exists a, b \in \mathbb{F}_p[x]$, such that $af + bg = 1$. Now,

$$\begin{aligned}
[af + bg] &= [1] \\
[a][f] + [b][g] &= [1] \\
[a][0] + [b][g] &= [1] \\
[b][g] &= [1]
\end{aligned}$$

Therefore $[b]$ is the multiplicative inverse of $[g]$ in $\mathbb{F}_p[x]/(f)$, where $[1]$ is the multiplicative identity.

Since $\mathbb{F}_p[x]/(f)$ is a quotient ring, and since every element has an inverse, $\mathbb{F}_p[x]/(f)$ is a field.

Now for the logical inverse: Suppose f is reducible. So $\exists$ non-constants $a, b \in F_p[x]$ such that $ab = f$.

We have $[ab] = [f] \to [a][b] = [0]$.

Suppose $[a] = [0]$. So $\exists r \in \mathbb{F}_p[x]$, such that $rf = a$. Now, $ab = f \to rfb = f$, and since we know $\mathbb{F}_p[x]$ is an integral domain, $rb = 0$. But $r \neq 0$, $b \neq 0$ from construction, so $\mathbb{F}_p[x]$ has non-zero zero divisors. Contradiction.

Therefore $[a] \neq [0]$. Similarly, $[b] \neq [0]$.

Since $[a] \neq [0]$ and $[b] \neq [0]$, $\mathbb{F}_p[x]/(f)$ has non-zero zero divisors, and therefore is not an integral domain, and therefore not a field. □

3.3 What is the order $|F|$ of F? Justify your answer.

$|F| = p^3 = 2^3 = 8$:

Since $x^3 + x + 1$ is irreducible in $\mathbb{F}_2[x]$, $\mathbb{F}_2[x]/(x^3 + x + 1)$ kills all polynomials above degree 3.

So you have $ax^2 + bx + c$ for $a, b, c \in \mathbb{Z}/2\mathbb{Z}$. □

Additional Citations

"Algebra" by Michael Artin (ISBN 13: 9780132413770).

Wikipedia.

Proofread by Devin Kwok (UCID: 10016484).

[10] Input "$IrreduciblePolynomialQ[x^3 + x + 1, Modulus- > 2]$" in `https://www.wolframalpha.com/`

[11] Reference: `http://sites.millersville.edu/bikenaga/abstract-algebra-1/quotient-rings-of-polynomial-rings/quotient-rings-of-polynomial-rings.html`