MATH 210B

Name: Quin Darcy **Due Date:** 2/12/20
Instructor: Dr. Shannon **Assignment:** Homework 3

3. Assume that F is a field, $f(x) \in F[x]$, and that $a \in F$. Prove that a is a root of $f(x)$ iff $(x-a) \mid f(x)$.

   Proof. Assume that a is a root of $f(x)$. Then $f(a) = 0$. Since F is a field and $f(x), (x-a) \in F[x]$ where $(x-a) \neq 0$, then by the proof on pg.5 there exists unique polynomials $q(x), r(x) \in F[x]$ such that $f(x) = q(x)(x-2) + r(x)$ and $r(x) = 0$ or $\deg(r(x)) < \deg(x-a)$. Since $\deg((x-a)) = 1$, then $\deg(r(x)) = 0$. Thus, for some $t \in F$, $r(x) = t$. By assumption, $f(a) = 0$ and so $q(a)(a-a) + t = t = 0$. Thus, $f(x) = q(x)(x-a)$. Therefore, $(x-a) \mid f(x)$. Now assume that $(x-a) \mid f(x)$. Then for some $q(x) \in F[x]$, we have that $f(x) = q(x)(x-a)$. Thus, $f(a) = q(a)(a-a) = 0$. Therefore, a is a root of $f(x)$. $\square$

4. Assume that F is a field. Then $F[x]$ is a Euclidean domain, thus any two polynomials have a gcd and the gcd can be expressed as a linear combination of the two polynomials. Over $\mathbb{Z}_7[x]$, find the gcd of $f(x) = 3x^3 + 5x^2 + 6x$ and $g(x) = 4x^4 + 2x^3 + 6x^2 + 4x + 5$ and express the gcd as a linear combination of $f(x)$ and $g(x)$.

   Solution. We begin by finding the gcd of the two given polynomials and this requires repeated applications of the division algorithm. In doing this we obtain

$$\begin{aligned} g(x) &= (6x)f(x) + (5x^2 + 4x + 5) = q_1(x)f(x) + r_1(x) \\ f(x) &= (2x+5)r_1(x) + (4x+3). \end{aligned}$$

   Thus, the gcd of the two given polynomials is $4x + 3$. Using back substitution, we get that

$$(1 + q_2(x)q_1(x))f(x) - (q_2(x))g(x) = 4x + 3.$$

5. Find the elementary symmetric functions for $x^3 + bx^2 + cx + d = (x-r)(x-s)(x-t)$, and for $x^4 - 2x^2 - 3$.

   Solution. To begin, we compute the elementary symmetric functions for $x^3 + bx^2 + cx + d$ and obtain $\sigma_1 = r + s + t$, $\sigma_2 = rs + rt + st$, and $\sigma_3 = rst$. For $x^4 - 2x^2 - 3$ we get that

$$\begin{aligned} \sigma_1 &= i + (-i) + \sqrt{3} + (-\sqrt{3}) = 0 \\ \sigma_2 &= (i)(-i) + (i)(\sqrt{3}) + (i)(-\sqrt{3}) + (-i)(\sqrt{3}) + (-\sqrt{3})(\sqrt{3}) = -2 \\ \sigma_3 &= (i)(-i)(\sqrt{3}) + (i)(-i)(-\sqrt{3}) + (i)(\sqrt{3})(-\sqrt{3}) + (-i)(\sqrt{3})(-\sqrt{3}) = 0 \\ \sigma_4 &= (i)(-i)(\sqrt{3})(-\sqrt{3}) = -3. \end{aligned}$$

6. Assume that F is a field, that $p(x) \in F[x]$ is irreducible over $F[x]$, and that $\deg(p(x)) = n$. Let $I = (p(x))_i$.

   (a) Prove that every element of $F[x]/I$ can be written in the form $I+h(x)$ where $h(x) = 0$ or $\deg(h(x)) < n$, and that this representation is unique.

   Proof. Let $h(x) + I \in F[x]/I$. If $\deg(h(x)) < n$, then we are done. Otherwise, if $\deg(h(x)) \geq n$, then by the division algorithm, there exists $q(x), r(x) \in F[x]/I$ such that $h(x) = q(x)p(x) + r(x)$, where $r(x) = 0$ or $\deg(r(x)) < n$. If $r(x) = 0$, then $h(x) \in I$. If $r(x) \neq 0$, then since $q(x)p(x) \in I$, then $I + h(x) = I + r(x)$.

   Now suppose $I + h(x) = I + f_1(x) = I + f_2(x)$ where $\deg(f_1(x)) < n$ and $\deg(f_2(x)) < n$. Then $I + (f_1(x) - f_2(x)) = I$ and it follows that $p(x) \mid (f_1(x) - f_2(x))$. Thus, for some $q(x) \in F[x]$, we have $f_1(x) = q(x)p(x) + f_2(x)$. However, since $\deg(f_1(x)) < n$ and $\deg(q(x)p(x) + f_2(x)) \geq n$ for $q(x) \neq 0$, but this is impossible. Thus $q(x) = 0$ and $f_1(x) = f_2(x)$. $\square$

   (b) Prove that $\{I + 1, I + x, \dots, I + x^{n-1}\}$ is a basis for $F[x]/I$ over F.

   Proof. Suppose that for some $a_0, \dots, a_{n-1} \in F$

$$\sum_{i=0}^{n-1}(I + a_i x^i) = I + \sum_{i=0}^{n-1} a_i x^i = I.$$

   By the unique representation component of part (a), it follows that

$$\sum_{i=0}^{n-1} a_i x^i = 0.$$

   Moving the constant term over we see that $a_1 x + \cdots + a_{n-1}x^{n-1} = -a_0$.

   With indeterminates on the left and none on the right, this equality only holds for $a_i = 0$ for all i. Thus, the set is linearly independent. Since $F[x]/I$ is a field, then clearly $\langle\{I + 1, \dots, I + x^{n-1}\}\rangle \subseteq F[x]/I$ and so it suffices to show that the inclusion goes the other way. Let $I + h(x) \in F[x]/I$. By part (a), we can assume that $\deg(h(x)) < n$, say $\deg(h(x)) = j$. Then $h(x) = a_0 + a_1 x + \cdots + a_j x^j$ and so

$$I + h(x) = I + \sum_{i=0}^{j} a_i x^i \in \langle\{I + 1, \dots, I + x^{n-1}\}\rangle.$$

   Thus, $\langle\{I + 1, \dots, I + x^{n-1}\}\rangle \subseteq F[x]/I$ and so $\{I + 1, \dots, +I + x^{n-1}\}$ is a basis for $F[x]/I$. $\square$

   (c) Find a basis for $\mathbb{Q}[x]/(x^3 - 2)_i$ over $\mathbb{Q}$.

   Solution. Let $I = (x^3-2)_i$ and $S = \{I+1, I+x, I+x^2\}$. Assume for $a_0, a_1, a_2 \in \mathbb{Q}$ that

$$(I + a_0) + (I + a_1 x) + (I + a_2 x^2) = I + (a_0 + a_1 x + a_2 x^2) = I.$$

   By 6.a, this representation is unique and so $a_0 + a_1 x + a_2 x^2 = 0$ which only holds for $a_i = 0$ for all i. Thus, S is linearly independent. Now take $I + h(x) \in \mathbb{Q}[x]/I$.

Then by 6.a, we can assume that $\deg(h(x)) < 3$ and so let $h(x) = b_0 + b_1x + b_2x^2$, then

$$I + h(x) = I + (b_0 + b_1x + b_2x^2) = (I + b_0) + (I + b_1x) + (I + b_2x^2) \in S.$$

Thus, $\langle S \rangle = \mathbb{Q}/(x^3 - 2)_i$. Therefore, S is a basis.

7. Determine the number of elements of $\mathbb{Z}_5/(x^2-3)_i$, and determine whether or not $\mathbb{Z}_5[x]/(x^2-3)_i$ is a field.

Solution. By 6.a, we know every element of $\mathbb{Z}_5[x]/(x^2-3)_i$ can be written as $I + h(x)$ where $I = (x^2 - 3)_i$ and $h(x) = 0$ or $\deg(h(x)) < 2$. Thus, $h(x) = a_0 + a_1x$ for $a_0, a_1 \in \mathbb{Z}_5$. There are 5 elements in $\mathbb{Z}_5$ and so a_0 can take on any one of these 5 values, and the same for a_1. Thus, there are $5 \cdot 5 = 25$ elements in $\mathbb{Z}_5[x]/(x^2 - 3)_i$. Lastly, we will check to see if $x^2 - 3$ is irreducible over $\mathbb{Z}_5$. Supposing it is, we would have

$$x^2 - 3 = (ax + b)(cx + d)$$

which gives us the relations $ac = 1$, $ad + bc = 0$, $bd = -3$. Checking every element, we find that there are no solutions. Thus, $x^2 - 3$ is irreducible, which implies $(x^2 - 3)_i$ is maximal and so $\mathbb{Z}_5[x]/(x^2 - 3)_i$ is a field.

8.

(a) Assume that F is a field, $f(x), g(x), h(x) \in F[x]$, $f(x) = g(x) \cdot h(x)$, and for all $c \in F$, $g(c) \neq 0$ and $h(c) \neq 0$. Must $f(x)$ be irreducible over $F[x]$? Explain your answer.

Solution. No, as a counter example consider $f(x) \in \mathbb{Q}[x]$ where

$$f(x) = x^4 - x^2 - 2 = (x^2 - 2)(x^2 + 1)$$

In this case, f is reducible since neither $g(x)$ or $h(x)$ is a unit, and the roots of both factors are not elements of $\mathbb{Q}$.

(b) Assume that F is a field, $a \in F$, $m \mid n$, $m \neq 1$, and there exists $d \in F$, $d \neq \pm a$, such that $d^m = a$. Prove that $x^n - a$ is reducible over F. Determine if the converse is true.

Proof. We begin by noting that for any $m \in \mathbb{N}$,

$$x^m - t^m = (x - t)(x^{m-t} + x^{m-2}t + \cdots + t^{m-1})$$

Since $d^m = a$, then we may write $x^n - a = x^n - d^m$. Moreover, since $m \mid n$, then for some $k \in \mathbb{Z}$, we have $n = mk$. Thus,

$$\begin{aligned} x^n - a &= x^n - d^m \\ &= x^{mk} - d^m \\ &= (x^k)^m - d^m \\ &= (x^k - d)((x^k)^{m-1} + (x^k)^{m-2}d + \cdots + d^{m-1}) \end{aligned}$$

Since neither of the polynomials in the final product are a unit, then $x^n - a$ is irreducible. $\square$

9. Find (and explain) the multiplicative inverse of $(x^3+x+1)_i+x^2+2$ in $\mathbb{Z}_5[x]/(x^3+x+1)_i$.

Solution. We being by applying the division algorithm on x^3+x+1 and x^2+2 in order to find the gcd of the two polynomials. In doing so we get

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

Thus, 3 is the gcd of the two polynomials. Letting $f(x)=x^2+2$, $g(x)=x^3+x+1$, $q_1(x)=x$, and $q_2(x)=4x+4$, we can use back substitution to obtain the following linear combination of $f(x)$ and $g(x)$:

$$(1-q_2(x)q_1(x))f(x)-q_2(x)g(x)=3.$$

Multiplying both sides by 2 and expanding, we get

$$\begin{aligned}2\big[1-(4x+4)(x)\big]f(x)-2q_2(x)g(x) &= \big[2-8x^2-8x\big]f(x)-2q_2(x)g(x)\\ &= [2+2x^2+2x]f(x)-2q_2(x)g(x)\\ &= [2x^2+2x+2]f(x)-2q_2(x)g(x)\\ &= 1.\end{aligned}$$

For space economy, let $I=(g(x))_i$. Since $-2q_2(x)g(x)\in I$, then $I-2q_2(x)g(x)=I$, from which it follows

$$\begin{aligned}\big[I+f(x)\big]\big[I+(2x^2+2x+2)\big] &= I+(2x^2+2x+2)f(x)\\ &= \big[I+(2x^2+2x+2)f(x)\big]+I\\ &= \big[I+(2x^2+2x+2)f(x)\big]+\big[I-2q_2(x)g(x)\big]\\ &= I+\big[(2x^2+2x+2)f(x)-2q_2(x)g(x)\big]\\ &= I+1.\end{aligned}$$

Hence, the multiplicative inverse of $(x^3+x+2)_i+x^2+2$ is $(x^3+x+1)_i+2x^2+2x+2$.

10. Assume that F is a field, $p(x)\in F[x]$ is irreducible over F and $I=(p(x))_i$. Prove that $I+x$ is a root of $p(x)$ in $F[x]/I$.

Proof. Since $p(x)$ is irreducible, then I is maximal and so $F[x]/I$ is a field. Now consider a map $\psi\colon F\to F[x]/I$ defined by $\psi(a)=I+a$. If we let $a,b\in F$ such that $a=b$, then $\psi(a)=I+a=I+b=\psi(b)$ and so ψ is well defined. If $\psi(a)=\psi(b)$, then $I+a=I+b$ and so $I+(a-b)=I$. Thus, $a-b\in I$. Hence, $a-b$ is a multiple of $p(x)$ which has degree greater than or equal to 1. Since $a,b\in F$ then the only way in which $a-b$ is equal to a multiple of a polynomial of degree ≥ 1 is if $a-b=0$ and so $a=b$. Therefore, ψ is 1-1. Moreover, we have that

$$\psi(a+b)=I+a+b=(I+a)+(I+b)=\psi(a)+\psi(b)$$

and

$$\psi(ab)=I+ab=(I+a)(I+b)=\psi(a)\psi(b).$$

Thus, $\psi\colon F \to \psi(F)$ is an isomorphism and so we can identify each element $a \in F$ with a coset $I + a \in F[x]/I$. Moreover, since F is a field, $F[x]/I$ is a field, and ψ is an isomorphism onto the image of F, then $\psi(F)$ is a subfield of $F[x]/I$. Now consider the homomorphism from HW2, problem 7 with $\theta\colon F[x] \to F[x]/I$ defined by $\theta(f(x)) = f(I + x)$. Thus, if $p(x) = a_0 + a_1x + \cdots a_nx^n$ with $a_i \in F$, then

$$\begin{aligned}
\theta(p(x)) &= p(I + x) \\
&= a_0(I + x)^0 + a_1(I + x)^1 + a_2(I + x)^2 + \cdots + a_n(I + x)^n \\
&= (I + a_0) + (I + a_1x) + (I + a_2x^2) + \cdots + (I + a_nx^n) \\
&= I + (a_0 + a_1x + a_2x^2 + \cdots + a_nx^n) \\
&= I + p(x) \\
&= I.
\end{aligned}$$

Thus, $p(I + x) = I = \psi(0)$. So since $F \cong \psi(F) \subseteq F[x]/I$, then it follows that $F[x]/I$ can be thought of as an extension of F which contains a root of $p(x)$, namely $I + x$. $\square$