MATH 3022 ALGEBRA II
ASSIGNMENT 2

JOE TRAN

Question 2. (a) *Let R be a commutative ring with unity ($1_R \neq 0_R$). Show that if $\{0_R\}$ and R and the only ideals of R, then R is a field.*
(b) *Let F be a field. Use (a) to show that $F[x]$ is not a field.*

Solution. (a) Suppose that R is not a field. Then there exists some $x \neq 0 \in R$ such that x has no inverse, so $\langle x \rangle = \{rx : r \in R\} \neq \langle 0 \rangle$ and we cannot obtain 1_R (as this would mean that there exists an $r \in R$ such that $rx = 1$, and since R is commutative, then we also have that $rx = xr = 1$ which implies that $x^{-1} = r$), and it cannot be R also. By contrapositive, we have shown that R is not a field.

(b) Let $p(x) \in F[x]$. Then $xp(x) \in F[x]$ and suppose that $xp(x) = 1$. Then when $x = 0 \in F$, we obtain that $0 = 1 \in F$, which is absurd.

Question 3. *Show that the principal ideal $\langle x - 1 \rangle$ in $\mathbb{Z}[x]$ is prime but not maximal.*

Solution. Note that because we have $\mathbb{Z}[x]/\langle x-1 \rangle \simeq \mathbb{Z}$, and because $\mathbb{Z}$ is an integral domain, then so is $\mathbb{Z}[x]/\langle x-1 \rangle$, and so $\langle x-1 \rangle$ is a prime ideal. However, $\mathbb{Z}[x]/\langle x-1 \rangle \simeq \mathbb{Z}$ and $\mathbb{Z}$ is not a field, so $\mathbb{Z}[x]/\langle x-1 \rangle$ cannot be a field, so $\langle x-1 \rangle$ cannot be maximal.

Question 5. *Let R be an integral domain. Assume that the division algorithm always holds in $R[x]$. Prove that R is a field.*

Solution. To see that R is a field, we need to show that every element in R has a multiplicative inverse. Indeed, let $r \neq 0 \in R$, and let $r_1(x) \in R[x]$ be such that $r_1(x) = r$ and $\deg(r_1(x)) = 0$. Let $p(x) \in R[x]$ be an irreducible polynomial with $\deg(p(x)) \geq 1$. Then by assumption, we use the division algorithm so that

$$r_1(x) = p(x)q(x) + r(x)$$

where either $r(x) = 0$ or $\deg(r(x)) < \deg(p(x))$. Now we consider the following cases:

- Case 1: If $r(x) = 0$, then $r_1(x) = p(x)q(x)$, but r_1 would be a multiple of $p(x)$, which is absurd, because $r \neq 0 \in R$ and $\deg(r_1(x)) = 0$, while $\deg(p(x)) > 0$.
- Case 2: If $0 = \deg(r(x)) < \deg(p(x))$ and since $\deg(r(x))$ cannot be smaller than 0, so this case does not hold.

Therefore, there is no such polynomials of degree greater than 0 in $R[x]$.

Now consider the polynomial given by

$$p(x) = xr + 1$$

Since there are no irreducible polynomials of degree 0, then $p(x)$ is reducible. Then by the division algorithm, there exists polynomials $a(x)$ and $b(x)$ such that

$$p(x) = a(x)b(x) = xr + 1$$

which implies that xr is a multiple of an element of R and so, there exists an element r^{-1} such that $rr^{-1} = 1$. Therefore, as $r \neq 0 \in R$ was arbitrary, every nonzero element in R has a multiplicative inverse, so R is a field.

Date: February 23, 2024.

Question 8. *Let p be prime.*

(a) *Show that there are $\frac{p(p+1)}{2}$ reducible polynomials over $\mathbb{Z}_p$ of the form x^2+ax+b.*
(b) *Determine the number of irreducible polynomials over $\mathbb{Z}_p$ of the form x^2+ax+b.*
(c) *Show that there exists a field of order p^2 for every prime p.*
(d) *Construct a finite field with four elements. Give the addition table and the multiplication table of your field.*

Solution. (a) Assume that x^2+ax+b is a reducible polynomial over $\mathbb{Z}_p$. Then there exists $x-\alpha$ and $x-\beta \in \mathbb{Z}_p[x]$ such that

$$x^2+ax+b = \begin{cases} (x-\alpha)(x-\beta) & \text{if } \alpha \neq \beta \\ (x-\alpha)^2 & \text{if } \alpha = \beta \end{cases}$$

Then since over $\mathbb{Z}_p$, we have $|\mathbb{Z}_p| = p$, then the number of quadratic monic polynomials is p^2. Since there are $\binom{p}{2}$ ways of choosing α and β in the first case (without repetition), and p ways for the second case. Therefore,

$$\begin{aligned} \binom{p}{2} + p &= \frac{p!}{2!(p-2)!} + p \\ &= \frac{p(p-1)(p-2)!}{2(p-2)!} + p \\ &= \frac{p(p-1)}{2} + p \\ &= \frac{p(p-1)+2p}{2} \\ &= \frac{p(p-1+2)}{2} \\ &= \frac{p(p+1)}{2} \end{aligned}$$

Therefore, there are $\frac{p(p+1)}{2}$ reducible polynomials over $\mathbb{Z}_p$ of the form x^2+ax+b.

(b) Because the number of quadratic monic polynomials is p^2 and the number of reducible quadratic monic polynomials is $\frac{p(p+1)}{2}$ from (a), then the number of irreducible monic quadratic polynomials are

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

(c) Since there is a polynomial of the form x^2+ax+b that is irreducible over $\mathbb{Z}_p$, then the quotient $\mathbb{Z}_p[x]/\langle x^2+ax+b\rangle$ is a field with p^2 elements, since as mentioned from (a), the number of quadratic monic polynomials is p^2.

(d) First let us consider $\mathbb{Z}_2$. We seek an irreducible polynomial $p(x)$ of degree 1 over $\mathbb{Z}_2$. Note that the following polynomials of degree 1 are possible in $\mathbb{Z}_2$:

$$p(x) = x \quad p(x) = x+1$$

However, note that $p(x) = x+1$ is irreducible since $f(0) = 1 \neq 0$, $f(1) = 2 \neq 0$, and therefore, $\mathbb{Z}_2[x]/\langle x+1\rangle$ is a finite field of order 4. Note that if $I = \langle x+1\rangle$, then the quotient ring is given as

$$\mathbb{Z}_2[x]/\langle x+1\rangle = \{0+\langle x+1\rangle, 1+\langle x+1\rangle, x+\langle x+1\rangle, x+1+\langle x+1\rangle\}$$

Then our addition table is given as

$+$	$0+I$	$1+I$	$x+I$	$(x+1)+I$
$0+I$	$0+I$	$1+I$	$x+I$	$(x+1)+I$
$1+I$	$1+I$	$0+I$	$(x+1)+I$	$x+I$
$x+I$	$x+I$	$(x+1)+I$	$0+I$	$1+I$
$(x+1)+I$	$(x+1)+I$	$x+I$	$1+I$	$0+I$

and the multiplication table is given as

$\cdot$	$0+I$	$1+I$	$x+I$	$(x+1)+I$
$0+I$	$0+I$	$0+I$	$0+I$	$0+I$
$1+I$	$0+I$	$1+I$	$x+I$	$(x+1)+I$
$x+I$	$0+I$	$x+I$	$(x+1)+I$	$1+I$
$(x+1)+I$	$0+I$	$(x+1)+I$	$1+I$	$x+I$

Question 10. *Either prove that $f(x) = 3x^5 - 4x^4 + 7x^3 + 16x^2 - 2$ is irreducible over $\mathbb{Q}$, or factor it into a product of irreducible factors in $\mathbb{Q}[x]$.*

Solution. We claim that $f(x)$ is irreducible over $\mathbb{Q}$. Indeed, say we take $x = -1 \in \mathbb{Q}$. Then observe that

$$f(-1) = 3(-1)^5 - 4(-1)^4 + 7(-1)^3 + 16(-1)^2 - 2 = 0$$

so $x + 1 \in \mathbb{Q}[x]$ is a factor of $f(x)$. Then by performing long division,

$$
\begin{array}{r|l}
 & 3x^4 - 7x^3 + 14x^2 + 2x - 2 \\
\hline
x+1 & 3x^5 - 4x^4 + 7x^3 + 16x^2 \qquad - 2 \\
 & -3x^5 - 3x^4 \\
\cline{2-2}
 & -7x^4 + 7x^3 \\
 & 7x^4 + 7x^3 \\
\cline{2-2}
 & 14x^3 + 16x^2 \\
 & -14x^3 - 14x^2 \\
\cline{2-2}
 & 2x^2 \\
 & -2x^2 - 2x \\
\cline{2-2}
 & -2x - 2 \\
 & 2x + 2 \\
\cline{2-2}
 & 0
\end{array}
$$

Now by the division algorithm, we can write

$$3x^5 - 4x^4 + 7x^3 + 16x^2 - 2 = (x+1)(3x^4 - 7x^3 + 14x^2 + 2x - 2)$$

Let $g(x) = 3x^4 - 7x^3 + 14x^2 + 2x - 2$. Say we take $x = \frac{1}{3} \in \mathbb{Q}$. Then observe that

$$g\left(\frac{1}{3}\right) = 3\left(\frac{1}{3}\right)^4 - 7\left(\frac{1}{3}\right)^3 + 14\left(\frac{1}{3}\right)^2 + 2\left(\frac{1}{3}\right) - 2 = 0$$

so $x - \frac{1}{3} \in \mathbb{Q}[x]$ is a factor of $g(x)$. Then by performing long division,

$$\begin{array}{r|l} & 3x^3 - 6x^2 + 12x + 6 \\ \hline x - \frac{1}{3} & 3x^4 - 7x^3 + 14x^2 + 2x - 2 \\ & -3x^4 + x^3 \\ \hline & -6x^3 + 14x^2 \\ & 6x^3 - 2x^2 \\ \hline & 12x^2 + 2x \\ & -12x^2 + 4x \\ \hline & 6x - 2 \\ & -6x + 2 \\ \hline & 0 \end{array}$$

Now by the division algorithm,

$$\begin{aligned} 3x^4 - 7x^3 + 14x^2 + 2x - 2 &= \left(x - \frac{1}{3}\right)(3x^3 - 6x^2 + 12x + 6) \\ &= (3x - 1)(x^3 - 2x^2 + 4x + 2) \end{aligned}$$

Let $h(x) = x^3 - 2x^2 + 4x + 2$. We claim that $h(x)$ is irreducible over $\mathbb{Q}$. Indeed, because the leading coefficient of $h(x)$ is 1 and the constant term of $h(x)$ is 2, then we have the test factors of 2, being 1 and 2. Checking each,

$$\begin{aligned} h(1) &= (1)^3 - 2(1)^2 + 4(1) + 2 = 5 \neq 0 \\ h(2) &= (2)^3 - 2(2)^2 + 4(2) + 2 = 10 \neq 0 \end{aligned}$$

Since none of the above test factors are such that $h(x) = 0$, then $h(x)$ is not irreducible.

Therefore,

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

Bonus. *Complete the questions specified on Page 5 of your Test 1:*

(2) (a) *Let R be a ring with identity. Show that if $a \in R$ is a zero divisor, then it is not a unit.*
(b) *Is the converse true? Justify your answer.*

Solution. (a) Assume that $a \in R$ is a zero divisor, and assume for a contradiction that $a \in R$ is a unit. Since a is a zero divisor, then there exists a $b \neq 0 \in R$ such that

$$ab = 0 \tag{1}$$

and since a is a unit, then there exists a unique $a^{-1} \in R$ such that

$$aa^{-1} = [a^{-1}a = 1] \tag{2}$$

Then right multiplying both sides of (2) in the bracket by b so that

$$\begin{aligned} (a^{-1}a)b &= 1b \\ a^{-1}(ab) &= b \\ a^{-1} \cdot 0 &= b \\ b &= 0 \end{aligned}$$

which is absurd because it contradicts the assumption that $b \neq 0 \in R$ and thus contradicts the assumption that a is a zero divisor. Therefore, it must be the case that a cannot be a unit.

(b) The converse of (a) is if a is not a unit, then a is a zero divisor. We claim that the statement is true. Assume that a is not a unit. Then for every $a^{-1} \in R$, we have that

$$a \cdot a^{-1} = [a^{-1} \cdot a \neq 1] \tag{1}$$

And now assume for a contradiction, that a is not a zero divisor. Then for every $b \neq 0 \in R$, we have that $ab \neq 0$, so let $c \neq 0$ be such that

$$ab = c \tag{2}$$

Then right multiplying both sides of (1) by b so that

$$\begin{aligned}(a^{-1} \cdot a) \cdot b &\neq 1 \cdot b \\ a^{-1} \cdot (a \cdot b) &\neq b \\ a^{-1} \cdot c &\neq b \\ a \cdot (a^{-1} \cdot c) &\neq a \cdot b \\ c &\neq ab\end{aligned}$$

which is a contradiction. Therefore, if a is not a unit, then a must be a zero divisor.