Assignment 4

Mads Esben Hansen - s174434

Ex1

Question 1

Let $(\mathbb{R}, +, \cdot)$ denote the field of real numbers and $(\mathbb{R}[X], +, \cdot)$ the ring of polynomials with coefficients in $\mathbb{R}$.

a) Let $I := \langle X^2, X+1 \rangle$ be the ideal of $\mathbb{R}[X]$ generated by the polynomials X^2 and $X+1$. Determine whether or not $I = \mathbb{R}[X]$.

Per definition we have:

$I = \left\{ r_1 \cdot X^2 + r_2 \cdot (X+1) \,\middle|\, r_1, r_2 \in \mathbb{R}[X] \right\}$

According to Lemma 170, we have that:

$I = \langle X^2, X+1 \rangle = \langle gcd(X^2, X+1) \rangle$

Now we can use the Euclidian algorithm to compute the $gcd(X^2, X+1)$.

$$\begin{bmatrix} X^2 & 1 & 0 \\ X+1 & 0 & 1 \end{bmatrix} \rightarrow (R_1 - X \cdot R_1)$$

$$\begin{bmatrix} -X & 1 & -X \\ X+1 & 0 & 1 \end{bmatrix} \rightarrow (R_1 - 2\,R_1)$$

$$\begin{bmatrix} X & -1 & X \\ X+1 & 0 & 1 \end{bmatrix} \rightarrow (change\, R_1\, R_2)$$

$$\begin{bmatrix} X+1 & 0 & 1 \\ X & -1 & X \end{bmatrix} \rightarrow (R_1 - R_2)$$

$$\begin{bmatrix} 1 & 1 & 1-X \\ X & 1 & X \end{bmatrix} \rightarrow (R_1 - R_2)$$

We can now already see that we get:

$1 \cdot X^2 + (1 - X) \cdot (X+1) = gcd(X^2, X+1) = 1$

In turn we can write the ideal as:

$I = \langle 1 \rangle$

$I = \left\{ r \cdot 1 \,\middle|\, r \in \mathbb{R}[X] \right\} = \mathbb{R}[X]$

So we get that $I = \mathbb{R}[X]$

perfect! :)

b) Let $J \subseteq \mathbb{R}[X]$ be the set of polynomials $f(X) \in \mathbb{R}[X]$ such that either $f(X) = 0$ or $\deg(f(X)) \geq 2$. Is J an ideal of $\mathbb{R}[X]$? Motivate your answer.

We remember the definition of an ideal given as definition 158 in the book. We notice that for J to be an ideal, $(J, +)$ must be a subgroup of $(R[X], +)$ (notice addition here is addition of polynomials).

Firstly this means that addition must be associative in $(J, +)$. Accordition to the definition of polynomial addition given we:

$$P_1(X) + P_2(X) = \sum_{l=0}^{\max\{degree(P_i)\}} \left(p_{1_l} + p_{2_l}\right)X^l$$

We quickly see that:

$$\left(P_1(X) + P_2(X)\right) + P_3(X) = \sum_{l=0}^{\max\{degree(P_i)\}} \left(\left(p_{1l} + p_{2_l}\right) + p_{3_l}\right)X^l =$$

$$P_1(X) + \left(P_2(X) + P_3(X)\right) = \sum_{l=0}^{\max\{degree(P_i)\}} \left(p_{1l} + \left(p_{2_l} + p_{3_l}\right)\right)X^l$$

Meaning that it is associative.

Secondly it means that the identity element must be part of the ideal, which is quite obviously given by $f(X) = 0$. Which we know is part of the ideal.

Thirdly the sum of any two element in J must also be in J. Here we can pick $f, g \in J$ s.t. $f(X) = X^2 + 1$ and $g(X) = -X^2$. Both f and g are in J, since they are both polynomials with degree 2 and real coefficients. We can now take the sum of these polynomials:

$f(X) + g(X) = 1$

This means that the sum of f and g is unfortunately not in J. (J,+) is therefore not a subgroup of (R[X],+), and cannot be an ideal.

Perfect again. I do not think this solution can be improved in any way. Good job!

Ex2

Question 2

As usual, the finite field with 3 elements is denoted by $(\mathbb{F}_3,+,\cdot)$, while $(\mathbb{F}_3[X],+,\cdot)$ denotes the ring of polynomials with coefficients in $\mathbb{F}_3$.

a) Use the extended Euclidean algorithm to compute the multiplicative inverse of the element $X+\langle X^4+X^3+X+2\rangle$ in the quotient ring $(\mathbb{F}_3[X]/\langle X^4+X^3+X+2\rangle,+,\cdot)$.

For $X+\langle X^4+X^3+X+2\rangle$ to have an inverse, it must be a unit in $\left(F_3[X]\,/\,\langle X^4+X^3+X+2\rangle, 0, \cdot\right)$. It must therefore hold that $degree\left(gcd\left(X, \langle X^4+X^3+X+2\rangle\right)\right)=0$. We will now proceed with the extended Euclidian algorihm, and if it does have a multiplicative inverse, compute it.

$$\begin{bmatrix} X^4+X^3+X+2 & 1 & 0 \\ X & 0 & 1 \end{bmatrix} \rightarrow \left(R_1+2X^3\cdot R_2\right)$$

$$\begin{bmatrix} X^3+X+2 & 1 & 2X^3 \\ X & 0 & 1 \end{bmatrix} \rightarrow \left(R_1+2X^2\cdot R_2\right)$$

$$\begin{bmatrix} X+2 & 1 & 2X^3+2X^2 \\ X & 0 & 1 \end{bmatrix} \rightarrow \left(R_1+2\cdot R_2\right)$$

$$\begin{bmatrix} 2 & 1 & 2X^3+2X^2+2 \\ X & 0 & 1 \end{bmatrix} \rightarrow \left(R_1-R_2\right)$$

First we notice that $degree\left(gcd\left(X, \langle X^4+X^3+X+2\rangle\right)\right)=0$, so an inverse does exist.
We get that:

$2=(1)\cdot\left(X^4+X^3+X+2\right)+\left(2X^3+2X^2+2\right)\cdot(X)$

We notice that $2^{-1}=2$, since $2\cdot_3 2=1$.

$2\cdot 2=2\cdot(1)\cdot\left(X^4+X^3+X+2\right)+2\cdot\left(2X^3+2X^2+2\right)\cdot(X) \Rightarrow$

$1=(2)\cdot\left(X^4+X^3+X+2\right)+\left(X^3+X^2+1\right)\cdot X \Rightarrow$

$1+\langle X^4+X^3+X+2\rangle=\left(X^3+X^2+1\right)\cdot X+\langle X^4+X^3+X+2\rangle$

So $\left(X^3+X^2+1\right)+\langle X^4+X^3+X+2\rangle$ is the multiplicative inverse of $X+\langle X^4+X^3+X+2\rangle$, in $\left(F_3[X]\,/\,\langle X^4+X^3+X+2\rangle, 0, \cdot\right)$.

correct answer and correct strategy!

b) Determine the total number of zero-divisors in the quotient ring $(\mathbb{F}_3[X]/\langle X^4+X^3+X+2\rangle,+,\cdot)$. You may use that in $\mathbb{F}_3[X]$ it holds that $X^4+X^3+X+2=(X^2+X+2)\cdot(X^2+1)$.

According to theorem 187, $(F_3[X] \,/\, \langle X^4 + X^3 + X + 2\rangle, 0, \cdot)$ is a field iff $X^4 + X^3 + X + 2$ is irreducible in $F_3[X]$.

We know that $X^4 + X^3 + X + 2 = (X^2 + X + 2)\cdot(X^2 + 1)$. This means that $X^2 + X + 2$ is a zero divisor for $X^2 + 1$ and vice versa, since

$(X^2 + X + 2)\cdot(X^2 + 1) + \langle X^4 + X^3 + X + 2\rangle = 0 + \langle X^4 + X^3 + X + 2\rangle$.

If either $X^2 + X + 2$ or $X^2 + 1$ is reducible we could have more zero-divisors. Since we are now dealing with 2nd degree polynomials, we know that if they are reducible it means they have a root in F_3. Since it is only 3 elements, we can simply check:

$(X^2 + X + 2)$

0: $0^2 +_3 0 +_3 2 = 2$

1: $1^2 +_3 1 +_3 2 = 1$

2: $2^2 +_3 2 +_3 2 = 2$

$(X^2 + 1)$

0: $0^2 +_3 1 = 1$

1: $1^2 +_3 1 = 2$

2: $2^2 +_3 1 = 2$

Finally we need to check if we can write $X^4 + X^3 + X + 2$ as a factor of a 1st and 3rd degree polynomial. For this to be the case, $X^4 + X^3 + X + 2$ must have a root in F_3 directly. We therefore check this:

0: $0^4 +_3 0^3 +_3 0 +_3 2 = 2$

1: $1^4 +_3 1^3 +_3 1 +_3 2 = 2$

2: $2^4 +_3 2^3 +_3 2 +_3 2 = 1$

We see that we cannot reduce any of these zero-divisors further, nor can we factorize $X^4 + X^3 + X + 2$ using a 1st and 3rd degree polynomial.Thus we do not have any more zero-divisors. The number of zero-divisors is therefore 2.

Unfortunately your solution is not correct. Let me explain why. First of all recall that every coset can be written in standard form, meaning as g(x)+<x^4+x^3+x+2> where deg(g(x))<=3. Also different choices of g(x) give different cosets. When is g(x)+<x^4+x^3+x+2> a zero-divisor? This is true if and only if 1<=deg(GCD(g(x),x^4+x^3+x+2))<=3. Since you showed that the two given factors g1(x)=x^2+1 and g2(x)=x^2+x+2 are irreducible, g(x)+<x^4+x^3+x+2> is a zero-divisor if and only if GCD(g(x),x^4+x^3+x+2) is either g1(x) or g2(x).
How many g(x) of degree at most 3 can we construct with this property? All multiples g(x)=h(x)*g1(x) and g(x)=h(x)*g2(x) where h(x) has degree either zero (not being the zero-polynomial) or 1. Hence h(x) is one of the following 8 polynomials: 1,2,x,x+1,x+2,2x,2x+1,2x+2. This creates a total number of 16 different zero-divisors.

VERY GOOD (MARIA)