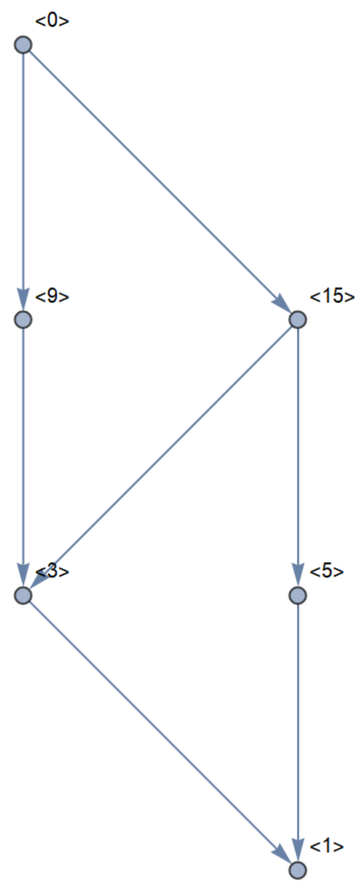
Math 320 Homework #12

Joseph C. McGuire
Dr. J. Morris

November 29, 2018

(100.) Construct a lattice of principal ideals for the ring $\mathbb{Z}_{45}$. Which of the ideals in your lattice are maximal ideals?

First, note that the principal ideals for the ring $\mathbb{Z}_{45}$ are just the factors of 45, that is the principal ideals of $\mathbb{Z}_{45}$ are $< 1 >, < 3 >, < 5 >, < 9 >, < 15 >$, and $< 0 >$. Thus we have the following lattice for the ring $\mathbb{Z}_{45}$:



In Problems 101 - 104, perform the given task in the factor ring $R = \mathbb{Z}_3[x]/I$, where $I = \langle x^2 + x + 1 \rangle$

(101.) Calculate $(2x + 1 + I)(x + 2 + I)$, and write your answer in the form $a + bx + I$, where $a, b \in \mathbb{Z}_3$.

Note that since we are working in the factor $\mathbb{Z}_3[x]/I$, we have $I = 0$; that is I is the additive identity. Hence $x^2 + x + 1 = 0$ iff $x^2 + x = -1$ iff $x^2 + x = 2$ iff $2x^2 + 2x = 4$ iff $2x^2 + 2x = 1$ Then consider the following:

$$\begin{aligned}
(2x + 1 + I)(x + 2 + I) &= (2x + 1)(x + 2) + I, \ \textit{by Theorem } 14.2 \\
&= 2x^2 + 4x + x + 2 + I \\
&= 2x^2 + 5x + 2 + I \\
&= 2x^2 + 2x + 2 + I \\
&= 1 + 2 + I, \ \textit{by above fact} \\
&= 3 + I \\
&= 0 + I \\
&= I
\end{aligned}$$

Thus $(2x + 1 + I)(x + 2 + I) = I$.

(102.) Calculate $(x^3 + I)(2x^2 + I)$, and write your answer in the form $a + bx + I$, where $a, b \in \mathbb{Z}_3$.

Similar to (101.) note that $x^2 + x + 1 = 0$. From here we get $x^2 + x + 1 = 0$ iff $x^2 = -x - 1$ iff $x^2 = 2x + 2$. Then consider the following:

$$
\begin{aligned}
(x^3+I)(2x^2+I) &= (x^3)(2x^2)+I, \ \textit{by Theorem } 14.2.\\
&= x^3(2)(2x+2)+I, \ \textit{by above fact}\\
&= x^2(x)(4x+4)+I\\
&= x^2(4x^2+4x)+I\\
&= (2x+2)(4x^2+4x)+I\\
&= 8x^3+8x+8x^2+8x+I\\
&= 8x(x^2)+8(x^2)+16x+I\\
&= 8x(2x+2)+8(2x+2)+16x+I\\
&= 16x^2+16x+16x+16+16x+I\\
&= 16(2x+2)+48x+16+I\\
&= 32x+32+48x+16+I\\
&= 2x+2+0x+1+I\\
&= 2x+3+I\\
&= 2x+I
\end{aligned}
$$

(103.) Find $(1+x+I)^{-1}$, and write your answer in the form $a+bx+I$, where $a, b \in \mathbb{Z}_3$

First, note that this is equivalent to finding solutions to the following equations:

$$(1+x+I)(a+bx+I) = 1+I$$

where $a, b \in \mathbb{Z}_3$. So we will do that in the following work:

$$
\begin{aligned}
(1+x+I)(a+bx+I) &= (1+x)(a+bx)+I, \ \textit{by Theorem } 14.2,\\
&= a+bx+ax+bx^2+I\\
&= a+bx+ax+b(2x+2)+I, \ \textit{by our previous work from } (102.)\\
&= a+bx+ax+2bx+2b+I\\
&= a+2b+ax+3bx+I\\
&= a+2b+ax+I
\end{aligned}
$$

Since we want this to be the identity element of our factor ring, $1+I = 1+0x+I$, we have the system of equations $a+2b=1$ and $ax=0$, hence $a=0$ and now we have $2b=1$, the only such $b \in \mathbb{Z}_3$ is $b=2$.

Hence $(1+x+I)^{-1} = (2x+I)$, we will demonstrate this with the following:

$$\begin{aligned}
(1+x+I)(2x+I) &= (1+x)(2x)+I,\ by\ Theorem\ 14.2 \\
&= 2x+2x^2+I \\
&= 2x+2(2x+2)+I,\ by\ fact\ from\ (102.) \\
&= 2x+4x+4+I \\
&= 4+6x+I \\
&= 1+0x+I \\
&= 1+I
\end{aligned}$$

Hence $(1+x+I)^{-1} = (2x+I)$.

(104.) Show that $2+x+I$ is a zero divisor.

Note that this is equivalent to finding solutions to the following equation:

$$(2+x+I)(a+bx+I) = 0+I$$

such that $a, b \in \mathbb{Z}_3$. So we will solve for a and b, then show that our solution times $2+x+I$ is zero, hence making $2+x+I$ a zero divisor.

$$\begin{aligned}
(2+x+I)(a+bx+I) &= (2+x)(a+bx)+I,\ by\ Theorem\ 14.2 \\
&= 2a+2bx+ax+bx^2+I \\
&= 2a+2bx+ax+b(2x+2)+I,\ by\ the\ fact\ from\ (102.) \\
&= 2a+2bx+ax+2bx+2b+I \\
&= 2a+2b+4bx+ax+I \\
&= 2a+2b+bx+ax+I
\end{aligned}$$

Setting this equal to $0+I$, again we end up with a system of equations in $2a+2b=0$ and $a+b=0$. Since $a, b \in \mathbb{Z}_3$, our only solutions our if $a=1$ and $b=2$ or $a=2$ and $b=1$. Thus we have the element $2+x+I \in R$ will be our zero divisor. We will show this below:

$$\begin{aligned}
(2+x+I)(2+x+I) &= (2+x)(2+x)+I,\ by\ Theorem\ 14.2 \\
&= 4+4x+x^2+I \\
&= 1+x+(2x+2)+I,\ by\ fact\ from\ (102.) \\
&= 3+3x+I \\
&= 0+I
\end{aligned}$$

Since $0+I$ is the zero element of our factor ring, we have $(2+x+I)$ is a zero-divisor in R.

(105.) Let I be an ideal of $\mathbb{Z}_2[\sqrt{2}]$ such that $3-2\sqrt{2} \in I$. Prove that $I = \mathbb{Z}[\sqrt{2}]$

Proof. Let I be an ideal of $\mathbb{Z}[\sqrt{2}]$ such that $3-2\sqrt{2} \in I$. So this means that for all $a \in \mathbb{Z}[\sqrt{2}]$, $a(3-2\sqrt{2}) \in I$. Since $a \in \mathbb{Z}[\sqrt{2}]$ we have a is of the form $a = b + c\sqrt{2}$. Hence $(a+b\sqrt{2})(3-2\sqrt{2}) = 3b + 3c\sqrt{2} - 2b\sqrt{2} - 2c(\sqrt{2})^2 = (3b-4c) + (3c-2b)\sqrt{2}$. If we can show that the system of equations $3b - 4c = d$ and $-2b + 2c = f$, for any integer $d, f \in \mathbb{Z}$, has integer solutions in c and b. Then that will show that $\mathbb{Z}[\sqrt{2}] \subseteq I$, and since we already have $I \subseteq \mathbb{Z}[\sqrt{2}]$, by the definition of an ideal, we will be done. Thus we need to show that the matrix:

$$\begin{bmatrix} 3 & -4 \\ -2 & 3 \end{bmatrix} = \begin{bmatrix} d \\ f \end{bmatrix}$$

Has integer solutions for all $f, d \in \mathbb{Z}$. Reducing this we get:

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 4f + 3d \\ 3f + 2d \end{bmatrix}$$

Leaving us with $b = 4f + 3d$ and $c = 3f + 2d$. Since these are all integers involved, we that the above equation will always have solutions in the integers. Thus, if we take any element $x \in \mathbb{Z}[\sqrt{2}]$, then x is of the form $x = f + d\sqrt{2}$. Furthermore, by the above work $x = (4f + 3d + (3f + 2d)\sqrt{2})(3 - 2\sqrt{2})$. Note that if we expand this we get
$x = (4f+3d+3f\sqrt{2}+2d\sqrt{2})(3-2\sqrt{2}) = 12f+9d+9f\sqrt{2}+6d\sqrt{2}-8f\sqrt{2}-6d\sqrt{2}-12f-8d = f+d\sqrt{2}$. Hence $x \in I$. Thus $\mathbb{Z}[\sqrt{2}] \subseteq I$. Hence $I = \mathbb{Z}[\sqrt{2}]$

□

(106.) If A and B are ideals of a ring, show that the sum of A and B, $A + B = \{a + b : a \in A, b \in B\}$, is an ideal.

Proof. Let A and B be ideals of the ring R, then let $A + B = \{a + b : a \in A \textit{ and } b \in B\}$. Then we will show that $A + B$ is an ideal of R using Theorem 14.1, the Ideal Test.

(A + B is non empty)

Let $r \in R$, then since A and B are both ideals we have $ar \in A$ and $br \in B$ for all $r \in R$. Then note that $ar + br = (a + b)r \in A + B$, by definition of the set, hence $A + B$ is nonempty.

($f - g \in A + B$)

Let $f, g \in A + B$. Then for some $a, c \in A$ and $b, d \in B$, we have $f = a + b$ and $g = c + d$. So then $f - g = (a + b) - (c + d) = a - c + b - d = (a - c) + (b - d)$. Since a and c are elements of A and b and d are elements of B, and both A and B are ideals, we have $(a - c) + (b - d) \in A + B$.

(rf and fr are in A whenever $f \in A + B$ and $r \in R$)

Let $r \in R$ and $f \in A + B$. Then for some $a \in A$ and $b \in B$ we have $f = a + b$. So $rf = r(a + b) = ra + rb$, and since both A and B are ideals we have $ra \in A$ and $rb \in B$, thus by the definition of the set we have $rf = ra + rb \in A + B$. Similarly $fr = (a + b)r = ar + br$ and since A and B are both ideals we have $ar \in A$ and $br \in B$. Hence $fr = ar + br \in A + B$.

Thus by Theorem 14.1, we have that $A + B$ is an ideal of R. □

(107.) Consider the factor ring $\mathbb{Z}_2[x]/\langle x^2+x+1\rangle$

(a.) Construct a Cayley Table for multiplication in the factor ring $\mathbb{Z}_2[x]$. (<u>Hint</u>: $\mathbb{Z}_2[x]/I = \{I, 1+I, x+I, 1+x+I\}$, where $I = \langle x^2+x+1\rangle$).

First note that from $< x^2+x+1 >= 0+I$, we have $x^2+x+1 = 0$ iff $x^2 = x+1$. Hence when we take the elements $(x+I)^2$ we get $x^2+I = x+1+I$ and for $x(x+1)+I$ we can obtain $x^2+x+I = 2x+1+I = 1+I$. Finally for $(1+x)^2+I = (x^2+2x+1)+I = (x+1+1) = x+I$. And since $1+I$ is the identity elements since 1 is the identity element for multiplication over polynomials, and that $0+I$ is the zero-element we have the following table:

*	I	1 + I	x + I	1 + x + I
I	I	I	I	I
1 + I	I	1 + I	x + I	1 + x + I
x + I	I	x + I	1 + x + I	1 + I
1 + x + I	I	1 + x + I	1 + I	x + I

(b.) Is $\langle x^2+x+1\rangle$ a maximal ideal in $\mathbb{Z}_2[x]$? Justify your answer.

Yes, since every element in our above Cayley table has a multiplicative inverse (note that $1+I$ is the unity), we have that $\mathbb{Z}_2[x]/\langle x^2+x+1\rangle$ is a field. Hence, by Theorem 14.4, $I = \langle x^2+x+!\rangle$ is a maximal ideal.

(c.) Is $\langle x^2+x+1\rangle$ a prime ideal in $\mathbb{Z}_2[x]$? Justify your answer.

Yes, since we have that $\mathbb{Z}_2[x]/\langle x^2+x+1\rangle$ is a integral domain, that is there are no non-zero zero-divisors (where our zero element is $0+I = I$). Thus by Theorem 14.3, we have $< x^2+x+1 >$ is a prime Ideal.

(108.) Prove that $I = \langle x^2+1\rangle$ is <u>not</u> a maximal ideal in the ring $\mathbb{Z}_{13}[x]$ in the two following ways:

(a.) Directly; that is, by finding an ideal I' of $\mathbb{Z}_{13}[x]$ such that $I \subsetneq I' \subsetneq \mathbb{Z}_{13}$. (<u>Hint</u>: $x^2+1=0$ has solutions in $\mathbb{Z}_{13}[x]$. Find them, and use them to help you factor the polynomial x^2+1.)

Proof. Let $I =< x^2+1 >$ be an ideal in the ring $\mathbb{Z}_{13}[x]$. Then note that when we look at the equation $x^2+1=0$ in our ring we have $x^2+1=0$ iff $x^2=12$, doing the calculations we find the only solutions to this are $x=5$ and $x=8$. Then we have $(x+5)(x+8) = x^2+13x+40 = x^2+40 = x^2+1$. Hence we have the set $< x^2+1 >= \{(x^2+1)r : r \in \mathbb{Z}_{13}[x]\}$ is equivalent to $\{(x+5)(x+8)r : r \in \mathbb{Z}_{13}[x]\}$. Hence, let $y \in \langle x^2+1\rangle$. Then for some $r \in \mathbb{Z}_{13}[x]$ we have $y = r(x^2+1) = r(x+5)(x+8)$. Hence we have both $y \in< x+5 >$ and $y \in< x+8 >$. Thus $< x^2+1 > \subseteq < x+5 >$ and $< x^2+1 > \subseteq < x+8 >$. Then note that while $7(x+5) \in< x+5 >$ we have $7(x+5) \notin< x^2+1 >$, since the equation $7x+35 = a(x^2+1)$ has no solutions in $a \in \mathbb{Z}_{13}[x]$. Thus $< x^2+1 > \subsetneq < x+5 >$. Finally, note that $1 \notin< x+5 >$, since the equation $1 = a(x+5)$ for any $a \in \mathbb{Z}_{13}[x]$ Therefore $< x^2+1 >$ isn't a maximal ideal of this ring. $\square$

(b.) By showing that $\mathbb{Z}_{13}[x]/\langle x^2+1\rangle$ is not a field and using Theorem 14.4.

Proof. Let $I = \langle x^2+1\rangle$, then consider the factor ring $\mathbb{Z}_{13}[x]/\langle x^2+1\rangle$. That from part(a.) we have $x^2+1 = (x+5)(x+8)$. Note that in this factor ring, we have $x^2+1+I = 0+I$, hence $x^2+1 = (x+5)(x+8) = 0$. Subsequently, $(x+5+I)(x+8+I) = (x+5)(x+8)+I = (x^2+13x+40)+I = (x^2+1)+I = 0+I = I$. Hence we have the elements $x+5$ and $x+8$ are non-zero zero-divisors. Hence our factor ring is not an integral domain, hence not a field, thus $< x^2+1 >$ is not a maximal ideal. □