Hugo *Rincon Galeana*

TU Wien, Winter 2019
104.272 Discrete Mathematics, Group 1 (Professor Gittenberger)
11. Exercise, Due 15 January, 2020

101. Show that $(\mathbb{Z}[x], +, \cdot)$ is a ring and that $1 \notin \langle\{x, x+2\}\rangle$

Proof. Let $p(x)$ and $q(x)$ be polynomials. Their product is a finite Cauchy product (which we have already observed to behave like a product during the generating functions chapter).

Notice that $\langle\{x, x+2\}\rangle$ only generates polynomials with an even independent coefficient.

Therefore 1 can not be generated. □

102. Let $p(x) = x^4 + 1$

(a) Is $p(x)$ irreducible over $\mathbb{R}$? If yes, prove it. If no, find a way to write $p(x)$ as a product of two (non-constant) real polynomials.

Proof. $x^4 + 1 = (x^2 + \sqrt{2}x + \sqrt{2})(x^2 - \sqrt{2}x + \sqrt{2})$
These roots are obtained from calculating the square roots of $i = \frac{\sqrt{2}}{2}(1+i)$
□

(b) is $p(x)$ irreducible over $\mathbb{Q}$?
Notice that the following map $x \mapsto x + 1$ induces a ring automorphism $\varphi : \mathbb{Q}[x] \to \mathbb{Q}[x]$.
Consider $\varphi(x^4 + 1) = (x+1)^4 + 1 = x^4 + 4x^3 + 6x^2 + 4x + 2$. It follows from Eisenstein's criterion for $p = 2$ that the polynomial is irreducible. $p|2, 4, 6, 4,\ 2$ does not divide 1 and 4 does not divide 2. Therefore the polynomial is irreducible in $\mathbb{Q}[x]$

103. Describe all real polynomials which are irreducible over $\mathbb{R}$.

Proof. The only irreducible polynomials are the polynomials of degree 1 or 2 without roots.

Let $p(x)$ be a polynomial of degree at least 3. Notice that $p(x)$ has a root $w \in \mathbb{C}$, then $\bar{w}$ is also a root in $\mathbb{C}$. Therefore $(x - w)(x - \bar{w}) \in \mathbb{R}[x]$. □

104. Let I be the following ideal of $\mathbb{Z} : I = \langle 14, 21\rangle$. Show that I is a principal ideal. Generalize for $I = \langle a, b\rangle$

Proof. Notice that $I = \{\alpha 14 + \beta 21 \mid \alpha, \beta \in \mathbb{Z}\}$. Recall that $\gcd(14, 21)$ divides any linear combination of 14 and 21 while the Euclidean algorithm yields the gcd as a linear combination. This shows that $I = \langle 7\rangle$. For the more general case $I = \langle \gcd(a, b)\rangle$. □

105. Let I be the following ideal of $(\mathbb{Z}[x], +, \cdot) : I = \langle x, 2\rangle$. Show that I is not a principal ideal.

Proof. Assume for a contradiction that $I = \langle p(x)\rangle$. Since it generates 2, then $p(x)$ should be a divisor of 2. Notice that $p(x) \neq 2$ since 2 cannot generate x. It cannot be 1, since it would generate $\mathbb{Z}[x]$. However, if $p(x) \in I$, then its independent term is even. □

106. Let $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$

(a) Determine the invertible elements of $\mathbb{Z}[i]$

Proof. Notice that for all $z \in \mathbb{Z}[i], \|z\| \geq 1$. Therefore $\|\|$ is an euclidian function in $\mathbb{Z}[i]$. Therefore the only invertible elements should have an euclidian function of at most 1. The only elements of $\mathbb{Z}[i]$ with this characteristic are $i, -i, 1, -1$ □

(b) Is $\mathbb{Z}[i]$ an integral domain?

Proof. Notice that since $\mathbb{Z}[i] \subset \mathbb{C}$ which is a field, and thus an integral domain, $\mathbb{Z}[i]$ is also an integral domain. □

107. Show that the set $S = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ with the usual addition and multiplication is a field. Compute $(6 + 4\sqrt{2})^{-1}$

Proof. Notice that since it is embedded on $\mathbb{R}$ which is already a field, then the product and sum satisfy all the field properties except for closure and existence of $0, 1$ and product inverses.

$0 = 0 + 0\sqrt{2}$;

$1 = 1 + 0\sqrt{2}$

Closure of $+$

Consider $(a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{2} \in S$

Closure of $\cdot$

$(a_1 + b_1\sqrt{2}) \cdot (a_2 + b_2\sqrt{2}) = (a_1a_2 + 2 \cdot b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2} \in S.$

Closure under multiplicative inverse Consider $(a + b\sqrt{2})(a - b\sqrt{2}) = a^2 + 2b^2$. This shows that $(a + b\sqrt{2}) \cdot a - b\sqrt{2}/a^2 + 2b^2 = 1$.

Therefroe $(6 + 4\sqrt{2})^{-1} = (6 - 4\sqrt{2})/68$ □

108. Determine whether the set $T = \{a + b\sqrt{2} + c\sqrt{3} \mid a, b \in \mathbb{Q}\}$ with the usual addition and multiplication is a field. If yes, prove it. If not, describe the smallest field (a subfield of $\mathbb{R}$) that contains T.

Proof. Notice that it is not algebraically closed since $\sqrt{2} \cdot \sqrt{3} = \sqrt{6} \notin \mathbb{Q}, \sqrt{2} \notin \mathbb{Q}, \sqrt{3} \notin \mathbb{Q}$.

The smallest subfield is given by $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \ : \ a, b, c, d \in \mathbb{Q}$.

Since the smallest field extension of $\mathbb{Q}[\sqrt{2}]$ that conatins $\sqrt{3}$ is given by $\mathbb{Q}[\sqrt{2}] + \mathbb{Q}[\sqrt{2}]\sqrt{3}$ □

109. Determine the minimal polynomial of $\sqrt{3} + i$:

(a) Over $\mathbb{Q}$

$$(x^2 + 4 - 2\sqrt{3}x)(x^2 + 4 + 2\sqrt{3}x) = x^4 + 8x^2 + 16 - 12x^2 = x^4 - 4x^2 + 16$$

(b) Over $\mathbb{R}$

$$(x - \sqrt{3})^2 + 1 = x^2 - 2\sqrt{3}x + 4$$

(c) Over $\mathbb{C}$

$$x - \sqrt{3} + i$$

110. Determine the minimal polynomial of $\sqrt{2} + \sqrt{3}$:

(a) Over $\mathbb{Q}$

Consider $(x - \sqrt{3})^2 - 2 = x^2 - 2\sqrt{3}x + 1$. Now consider $(x^2 + 1 - 2\sqrt{3}x)(x^2 + 1 + 2\sqrt{3}x) = (x^2 + 1)^2 - 12x = x^4 + 2x^2 + 1 - 12x^2$

$$x^4 - 10x^2 + 1$$

(b) Over $\mathbb{R}$

$$x - (\sqrt{2} + \sqrt{3})$$

(c) Over $\mathbb{C}$

$$x - (\sqrt{2} + \sqrt{3})$$