MATH 7210 Homework 9

Andrea Bourque

November 2021

1 Problem 2

Let $z \in \mathbb{C}$.

a) Show that there is a unique irreducible monic polynomial $p_z \in \mathbb{R}[X]$ of degree ≤ 2 such that $p_z(z) = 0$.

Proof. Let $z = a + bi$. Suppose $b \neq 0$. Consider $p_z(X) = (X - (a+bi))(X - (a-bi)) = X^2 - 2aX + a^2 + b^2$. Since the roots are both non-real and the polynomial is degree 2, there is no way to factor over $\mathbb{R}$, since that would imply p_z has real roots. By construction, $p_z(z) = 0$.

If $b = 0$, so that $z = a \in \mathbb{R}$, then $p_z(X) = X - a$ is clearly satisfies the required conditions. $\square$

b) Let $\phi_z : \mathbb{R}[X] \to \mathbb{C}$ be the unique homomorphism extending $\mathbb{R} \hookrightarrow \mathbb{C}$ with $\phi_z(X) = z$. Show that $\ker \phi_z = (p_z)$.

Proof. Note that a polynomial $f(X) = a_0 + a_1 X + ... + a_n X^n$ is mapped to $\phi_z(f(X)) = a_0 + a_1 z + ... + a_n z^n = f(z)$. Thus $f \in \ker \phi_z$ iff $f(z) = 0$. Then any multiple of p_z is in $\ker \phi_z$, since $\phi_z(z) g(z) = 0$ for any $g \in \mathbb{R}[X]$. If $f(z) = 0$, then $\overline{f(z)} = f(\overline{z}) = 0$. Thus $f(X)$ is divisible by both $X - z$ and $X - \overline{z}$, so it is divisible by p_z. Thus the kernel is exactly all multiples of p_z; $\ker \phi_z = (p_z)$. $\square$

c) Show that $\mathbb{R}[X]/(p_z)$ is isomorphic to $\mathbb{R}$ if $z \in \mathbb{R}$ and to $\mathbb{C}$ otherwise.

Proof. By isomorphism theorem and part b, the quotient is equal to the image of ϕ_z. Clearly, the image contains $\mathbb{R}$, since $\phi_z(\mathbb{R}) = \mathbb{R}$. If $z \in \mathbb{R}$, then $\phi_z(X) \in \mathbb{R}$, and thus any element of $\mathbb{R}[X]$ is mapped into $\mathbb{R}$. Then the image is just $\mathbb{R}$. Otherwise, $\phi_z(X)$ is nonreal. If $z = a + bi$, then $\phi_z((X-a)/b) = i$, so the image contains i and therefore every complex number, so the image is $\mathbb{C}$. $\square$

2 Problem 3

a) Show that (x, y) is a maximal ideal in $\mathbb{Q}[x, y]$ and that it is not principal.

Proof. The quotient $\mathbb{Q}[x, y]/(x, y) \cong \mathbb{Q}$, which is a field, so (x, y) is maximal. It cannot be principal, since the ideal contains x and y, which are independent variables and cannot be expressed as multiples of some other element in (x, y). $\square$

b) Show that (x, y) is a prime ideal in $\mathbb{Z}[x, y]$ which is not maximal. Find a maximal ideal containing (x, y).

Proof. The quotient $\mathbb{Z}[x, y]/(x, y) \cong \mathbb{Z}$ is an integral domain but not a field, so (x, y) is prime but not maximal. Now consider the ideal $(x, y, 2)$. Then the quotient $\mathbb{Z}[x, y]/(x, y, 2) \cong \mathbb{Z}/2\mathbb{Z}$, which is a field, so $(x, y, 2)$ is a maximal ideal. It contains (x, y) since it is (x, y) with an extra generator. $\square$

3 Problem 8.3.6

a) Prove that the quotient ring $\mathbb{Z}[i]/(1+i)$ is a field of order 2.

Proof. In $\mathbb{Z}[i]$, the only relation is $i^2 = -1$. Taking the quotient by $(1+i)$ adds the relation $i = -1$. Squaring both sides gives $-1 = 1$, so $2 = 0$. Thus $\mathbb{Z}[i]/(1+i) \cong \mathbb{Z}/2\mathbb{Z}$. $\square$

b) Let $q \in \mathbb{Z}$ be a prime with $q \equiv 3 \bmod 4$. Prove that the quotient ring $\mathbb{Z}[i]/(q)$ is a field with q^2 elements.

Proof. The quotient only has q^2 distinct elements, which are the equivalence classes of $a+bi$ for $a = 0, 1, ..., q-1$ and $b = 0, 1, ..., q-1$, with equivalence given by congruence mod q. Consider the standard method for computing inverses of complex numbers, i.e. by multiplying by the conjugate: $(a+bi)^{-1} = (a^2 + b^2)^{-1}(a - bi)$. Suppose $a + bi \not\equiv 0$. Then $a \not\equiv 0$ or $b \not\equiv 0$. If either is congruent to 0, then the other will be not congruent to 0 and will square to not zero, since q is prime. (In other words, $x^2 \equiv 0$ mod prime implies $x \equiv 0$). Thus, assume both $a, b \not\equiv 0$. $a^2 + b^2 \equiv 0$ then implies $(ab^{-1})^2 \equiv -1$, where b^{-1} exists mod q since $b \not\equiv 0$. But then ab^{-1} is an order 4 element in $(\mathbb{Z}/q\mathbb{Z})^*$, which has order $q - 1 \equiv 2 \bmod 4$. This is a contradiction. Thus if $a + bi \not\equiv 0$, $a^2 + b^2 \not\equiv 0$. Then we can compute $(a^2 + b^2)^{-1}(a - bi) \bmod q$, so that every nonzero element has an inverse. $\square$

c) Let $p \in \mathbb{Z}$ be a prime with $p \equiv 1 \bmod 4$ and write $p = \pi\overline{\pi}$ as in Proposition 18. Show that the hypotheses for the Chinese Remainder Theorem are satisfied and that $\mathbb{Z}[i]/(p) \cong \mathbb{Z}[i]/(\pi) \times \mathbb{Z}[i]/(\overline{\pi})$ as rings. Show that the quotient $\mathbb{Z}[i]/(p)$ has order p^2 and conclude that $\mathbb{Z}[i]/(\pi)$ and $\mathbb{Z}[i]/(\overline{\pi})$ are both fields of order p.

Proof. First we show that $(\pi) + (\overline{\pi}) = \mathbb{Z}[i]$. Observe that for $\pi = a + bi$, a, b must be coprime. Indeed, since $a^2 + b^2 = p$ is prime, the square of $\gcd(a, b)$ divides p, implying the gcd is 1. Thus for integers x, y, we can find integers x_1, x_2, y_1, y_2 such that $ax_1 + bx_2 = x$ and $ay_1 + by_2 = y$. Now, a, b cannot have the same parity, as then $a^2 + b^2$ would be even. Thus one is even, one is odd. WLOG, let a be even and b odd. We then modify x_i, y_i such that $x_1 \equiv y_2 \bmod 2$, and $x_2 \equiv y_1$. The modification is given by adding $ab - ba = 0$ to either equation, which has the effect of changing the parity of the first variable, and keeping the parity of the second. Thus we can assume $x_1 \equiv y_2 \bmod 2$, and $x_2 \equiv y_1$. With this in mind, let $c = (x_1 + y_2)/2$, $e = (x_1 - y_2)/2$, $d = (y_1 - x_2)/2$, and $f = (y_1 + x_2)/2$; they are all integers. The merit of all of this work is that $(c + di)(a + bi) + (e + fi)(a - bi) = x + yi$, as can be checked by computation. The left hand side is an element of $(\pi) + (\overline{\pi})$, while the right hand side is an arbitrary element of $\mathbb{Z}[i]$, so we have $(\pi) + (\overline{\pi}) = \mathbb{Z}[i]$.

Next, we show that $(\pi)(\overline{\pi}) = (p)$. Elements of the left hand side are sums of terms of the form $\pi x \overline{\pi} y = pxy$, so that $(\pi)(\overline{\pi}) \subset (p)$. On the other hand, obviously $p = \pi\overline{\pi} \in (\pi)(\overline{\pi})$, so $(p) \subset (\pi)(\overline{\pi})$. Thus we have the conditions for CRT, so that $\mathbb{Z}[i]/(p) \cong \mathbb{Z}[i]/(\pi) \times \mathbb{Z}[i]/(\overline{\pi})$.

As in part b, $\mathbb{Z}[i]/(p)$ has p^2 distinct elements, namely the equivalence classes of $x + yi$ for $x, y = 0, ..., p-1 \bmod p$. Since the order of (finite) rings is multiplicative, we have that the order of $\mathbb{Z}[i]/(\pi)$ is either $1, p$, or p^2. The order is 1 iff $(\pi) = \mathbb{Z}[i]$. This is clearly not the case by considering the norm $N(x+yi) = x^2 + y^2$ on $\mathbb{Z}[i]$. It is multiplicative, so that if π divides an element x, $N(\pi)$ divides $N(x)$. We have $N(\pi) = a^2 + b^2 = p$, while $N(1) = 1$, so clearly $(\pi) \neq \mathbb{Z}[i]$. Similarly, $(\overline{\pi}) \neq \mathbb{Z}[i]$, which excludes the order of either quotient ring being p^2. Thus both have order p. $\square$

4 Problem 8.3.8

Let $R = \mathbb{Z}[\sqrt{-5}]$ and let $I_2 = (2, 1+\sqrt{-5})$, $I_3 = (3, 2+\sqrt{-5})$, $I_3' = (3, 2-\sqrt{-5})$.

a) Prove that $2, 3, 1+\sqrt{-5}$, and $1-\sqrt{-5}$ are irreducibles in R, no two of which are associate in R, and that $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ are two distinct factorizations of 6 into irreducibles in R.

Proof. We use the norm $N(a+b\sqrt{-5}) = a^2 + 5b^2$. The norm is multiplicative, i.e. $N(xy) = N(x)N(y)$. Thus we can check irreducibility by looking at factorizations of the norm. Note that $N(a+b\sqrt{-5}) = 1$ iff $a + b\sqrt{-5} = \pm 1$, since $b \neq 0$ implies $N(a+b\sqrt{-5}) \geq 5$, so we must have $a^2 = 1$ and $b = 0$. Thus, elements with norm 1 are units in R. Conversely, ± 1 are the only units in R. To show this, suppose $(a+b\sqrt{-5})(c+d\sqrt{-5}) = 1$. Taking norms gives $N(a+b\sqrt{-5})N(c+d\sqrt{-5}) = 1$, so $N(a+b\sqrt{-5}) = 1$. Thus $N(x) = 1$ iff x is a unit.

Now, suppose $2 = xy$ with x, y not units. $N(2) = 4 = N(x)N(y)$ implies $N(x) = 2$. This is impossible; if $x = a + b\sqrt{-5}$, $N(x) < 5$ implies $b = 0$, and then $a^2 = 2$ is not solvable in $\mathbb{Z}$. Similar logic works for the other elements. If $3 = xy$ with x, y not units, then $N(3) = 9 = N(x)N(y)$ implies $N(x) = 3$, which implies $x = a \in \mathbb{Z}$ with $a^2 = 3$, again impossible. If $1 \pm \sqrt{-5} = xy$ with x, y non units, $N(1 \pm \sqrt{-5}) = 6 = N(x)N(y)$ implies $N(x) = 2$ or 3, both of which have been seen to be impossible.

Since the only units in R are ± 1, x, y are associates iff $y = \pm x$. Thus it is obvious that none of $2, 3, 1+\sqrt{-5}$, and $1-\sqrt{-5}$ are associates. Since none of these elements are units nor associates of each other, $2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ give unique factorizations of 6. □

b) Prove that I_2, I_3, and I_3' are prime ideals in R.

Proof. Write $\alpha = \sqrt{-5}$. The only relation in R is $\alpha^2 = -5$. Taking a quotient by I_2 gives extra relations $2 = 0$ and $\alpha = -1$. Squaring the second equation gives $-5 = 1$, which is $6 = 0$, which is also implied by $2 = 0$, so there is no extra information. Thus we just get $R/(1+i) \cong \mathbb{Z}/2\mathbb{Z}$, which is an integral domain, so I_2 is prime.

Taking a quotient by I_3 gives extra relations $3 = 0$ and $\alpha = -2$. Squaring the latter gives $-5 = 4$ or $9 = 0$, which is implied by $3 = 0$. Thus $R/I_3 \cong \mathbb{Z}/3\mathbb{Z}$, which is an integral domain, so I_3 is prime.

Taking a quotient by I_3' gives extra relations $3 = 0$ and $\alpha = 2$. Squaring the latter gives $-5 = 4$ or $9 = 0$, which is implied by $3 = 0$. Thus $R/I_3 \cong \mathbb{Z}/3\mathbb{Z}$, which is an integral domain, so I_3 is prime. □

c) Show that the factorizations in part a imply the equality of ideals $(6) = (2)(3)$ and $(6) = (1+\sqrt{-5})(1-\sqrt{-5})$. Show that these two ideal factorizations give the same factorization of the ideal (6) as the product of prime ideals.

Proof. An element of (2) is of the form $2x$, and an element of (3) is of the form $3y$. Thus elements in $(2)(3)$ are of the form $2x_1 3y_1 + ... 2x_n 3y_n = 6(x_1 y_1 + ... x_n y_n) \in (6)$. Thus $(2)(3) \subset (6)$ Since $6 = 2 \cdot 3 \in (2)(3)$, we have $(6) \subset (2)(3)$. Thus $(6) = (2)(3)$. Similar logic follows for $1 \pm \sqrt{-5}$, since $(1+\sqrt{-5}) \cdot (1-\sqrt{-5}) = 6$ in R, so as ideals we have $(6) = (1+\sqrt{-5})(1-\sqrt{-5})$.

We now decompose each of the principal ideals into their prime factors. I_2^2 has terms that are sums of terms $(2a + b(1+\sqrt{-5})(2c + d(1+\sqrt{-5})) = 2(2ac + ad + bc - 2bd + (ad + bd + bc)\sqrt{-5}) \in (2)$, so we have $I_2^2 \subset (2)$. On the other hand, $2 = (1+\sqrt{-5})(2-(1+\sqrt{-5})) + (-2)(2) \in I_2^2$, so $(2) \subset I_2^2$. Thus $I_2^2 = (2)$. A similar argument shows that $I_3 I_3' = (3)$, since $(3a + 2b + b\sqrt{-5})(3c + 2d - d\sqrt{-5}) = 3(3ac + 2ad + 2bc + 3bd + (bc - ad)\sqrt{-5}) \in (3)$ and $3 \in I_3 I_3'$. Thus we have $(6) = (2)(3) = I_2^2 I_3 I_3'$.

We do similar computations for the other ideals. $I_2 I_3$ is generated by sums of terms of the form $(2a+b+b\sqrt{-5})(3c+2d+d\sqrt{-5}) = [(ac+ad+bc)(1+\sqrt{-5}) - 2ad - 3bc - 3bd](1-\sqrt{-5}) \in (1-\sqrt{-5})$. Again, we also have $1-\sqrt{-5} \in I_2 I_3$ (Sorry grader I am too lazy to actually show this), so $(1+\sqrt{-5}) = I_2 I_3$. For $I_2 I_3'$ we have $(2a+b+b\sqrt{-5})(3c+2d-d\sqrt{-5}) = [(ac+ad+bd)(1-\sqrt{-5}-2ad+bd+3bc)](1+\sqrt{-5}) \in (1+\sqrt{-5})$. Again, $1+\sqrt{-5} \in I_2 I_3'$, so $I_2 I_3' = (1+\sqrt{-5})$. Thus $(6) = (1+\sqrt{-5})(1-\sqrt{-5}) = I_2^2 I_3 I_3'$. Thus, the two factorizations of (6) give the same prime factorization. $\square$

5 Problem 9.6.7

Order the monomials $x^2z, x^2y^2z, xy^2z, x^3y, x^3z^2, x^2, x^2yz^2, x^2z^2$ for the lexicographic ordering $x > y > z$, for the corresponding grlex order, and for the grevlex ordering.

Proof. Lexicographic: $x^3y, x^3z^2, x^2y^2z, x^2yz^2, x^2z^2, x^2z, x^2, xy^2z$.

Grlex: $x^3z^2, x^2y^2z, x^2yz^2, x^3y, x^2z^2, xy^2z, x^2z$.

Grevlex: $x^2y^2z, x^3z^2, x^2yz^2, x^3y, xy^2z, x^2z^2, x^2z$. □