

Problem Set 13

Due Wednesday, December 10

Instructions: You are encouraged to work together on these problems, but each student should hand in their own final draft, written in a way that indicates their individual understanding of the solutions. Never submit something for grading that you do not completely understand. You cannot use any resources besides me, your classmates, and our course notes.

I will post the .tex code for these problems for you to use if you wish to type your homework. If you prefer not to type, please *write neatly*. As a matter of good proof writing style, please use complete sentences and correct grammar. You may use any result stated or proven in class or in a homework problem, provided you reference it appropriately by either stating the result or stating its name (e.g. the definition of ring or Lagrange's Theorem). Please do not refer to theorems by their number in the course notes, as that can change.

Problem 1. Consider the ring $R = \mathbb{Z}[x]$ and the ideal $I = (3, x^3 + x + 1)$.

(a) Show that $R/I \cong (\mathbb{Z}/3)[x]/(x^3 + x + 1)$.

Proof. Using the Third Isomorphism Theorem, we have

$$\mathbb{Z}[x]/I \cong (\mathbb{Z}[x]/(3))/(x^3 + x + 1).$$

Now consider the map quotient map $\pi: \mathbb{Z} \rightarrow \mathbb{Z}/3$, and let

$$\varphi: \mathbb{Z}[x] \longrightarrow (\mathbb{Z}/3)[x]$$

be the ring homomorphism defined by

$$\varphi(a_0 + a_1x + \cdots + a_nx^n) = \pi(a_0) + \pi(a_1)x + \cdots + \pi(a_n)x^n.$$

A polynomial is in $\ker(\varphi)$ if and only if all its coefficients are multiples of 3, and thus $\ker(\varphi) = (3)$. Moreover, φ is surjective by construction. By the First Isomorphism Theorem, we conclude that

$$\mathbb{Z}[x]/(3) \cong (\mathbb{Z}/3)[x].$$

Therefore,

$$\mathbb{Z}[x]/I \cong (\mathbb{Z}/3)[x]/(x^3 + x + 1). \quad \square$$

(b) Find, with proof, all the ideals of R that contain I .

Proof. By the Lattice Isomorphism Theorem, the ideals of $(\mathbb{Z}/3)[x]/(x^3 + x + 1)$ correspond to the ideals of $(\mathbb{Z}/3)[x]$ that contain $x^3 + x + 1$. Since $\mathbb{Z}/3$ is a field, $\mathbb{Z}/3[x]$ is a PID. Given any $f \in \mathbb{Z}/3[x]$, $(f) \supseteq (x^3 + x + 1)$ if and only if f divides $x^3 + x + 1$.

The ring $\mathbb{Z}/3$ is a field, and over $\mathbb{Z}/3$ the polynomial $x^3 + x + 1$ factors as

$$x^3 + x + 1 = (x - 1)(x^2 + x - 1).$$

The polynomial $x^2 + x - 1$ has no roots in $\mathbb{Z}/3$, which we can check by explicitly evaluating it at all the three elements of $\mathbb{Z}/3$. Hence, by degree considerations, $x^2 + x - 1$ must be irreducible, as any factor would have degree 1 and lead to a root.

Thus the ideals of $\mathbb{Z}/3[x]$ that contain $x^3 + x + 1$ are (1) , $(x^3 + x + 1)$, $(x - 1)$ and $(x^2 + x - 1)$. This gives 4 ideals of $\mathbb{Z}[x]$ that contain I : $\mathbb{Z}[x]$, I , $(3, x - 1)$ and $(3, x^2 + x + 1)$. \square

Problem 2. Let $R = \mathbb{Z}[\sqrt{-5}]$ where $\sqrt{-5} = \sqrt{5} \cdot i \in \mathbb{C}$ and $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$.

(a) Prove that $R \cong \mathbb{Z}[x]/(x^2 + 5)$ and, for integers $p \geq 2$, $R/(p) \cong (\mathbb{Z}/p)[x]/(x^2 + [5]_p)$.

Proof. Consider the evaluation homomorphism $\phi : \mathbb{Z}[x] \rightarrow R$ that sends $f(x) \mapsto f(\sqrt{-5})$. Since $\phi(ax + b) = a\sqrt{-5} + b$ for all $a, b \in \mathbb{Z}$ we see that ϕ is onto. Let $f \in \ker(\phi)$. Then by long division $f(x) = (x^2 + 5)q(x) + r(x)$ for some $q, r \in \mathbb{Z}[x]$ such that either $r = 0$ or $\deg(r) \leq 1$. Thus $r(x) = ax + b$ for some $a, b \in \mathbb{Z}$ and so $0 = f(\sqrt{-5}) = a\sqrt{-5} + b$. If $a \neq 0$ then we obtain $\sqrt{-5} = -b/a \in \mathbb{Q}$, a contradiction, so it must be that $a = 0$ and consequently $b = 0$. This shows that $\ker(\phi) = (x^2 + 5)$ and by the First Isomorphism Theorem we conclude that there is an isomorphism $\bar{\phi} : \mathbb{Z}[x]/(x^2 + 5) \rightarrow R, \bar{\phi}(f(x) + (x^2 + 5)) = f(\sqrt{-5})$.

Now the image of (p) under $\bar{\phi}$ is the ideal $(p) + (x^2 + 5)/(x^2 + 5)$ of $\mathbb{Z}[x]/(x^2 + 5)$, therefore there is an induced isomorphism

$$R/(p) \cong \frac{\mathbb{Z}[x]/(x^2 + 5)}{(p) + (x^2 + 5)/(x^2 + 5)}$$

and the third isomorphism theorem can be applied to deduce

$$R/(p) \cong \mathbb{Z}[x]/(x^2 + 5)/(p) + (x^2 + 5)/(x^2 + 5) \cong \mathbb{Z}[x]/(p, x^2 + 5).$$

Finally, consider the composition of the reduction homomorphism $r : \mathbb{Z}[x] \rightarrow (\mathbb{Z}/p)[x]$ and the quotient map $q' : (\mathbb{Z}/p)[x] \rightarrow (\mathbb{Z}/p)[x]/(x^2 + 5)$. Then $\ker(q' \circ r) = (p, x^2 + 5)$ and since r and q' are onto so is $q' \circ r$. Thus again by the first isomorphism theorem we obtain

$$\mathbb{Z}[x]/(p, x^2 + 5) \cong (\mathbb{Z}/p)[x]/(x^2 + 5).$$

Putting this together with the isomorphism displayed above gives

$$R/(p) \cong (\mathbb{Z}/p)[x]/(x^2 + 5).$$

□

(b) Show that the integer 7 is irreducible¹ in R , but is not a prime element in R .

Proof. First we show that 7 is irreducible. Suppose that $7 = \alpha\beta$ for some $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$. Note that for $a + b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$, we have $N(a + b\sqrt{-5}) = a^2 + 5b^2 \in \mathbb{Z} \geq 0$. Then, following the hint, we have $49 = N(7) = N(\alpha)N(\beta)$ with $N(\alpha), N(\beta) \in \mathbb{Z} \geq 0$. Thus without loss of generality we either have $N(\alpha) = N(\beta) = 7$ or $N(\alpha) = 49$ and $N(\beta) = 1$.

The first case is impossible, since we would have $\alpha = a + b\sqrt{-5}$ with $a, b \in \mathbb{Z}$ and $a^2 + 5b^2 = 7$, but no such integers a, b exist, as we would have $|a|, |b| \leq 2$, and none of the nine possible cases yields a norm of 7. In the second case, $N(\beta) = 1$ implies $\beta = a + b\sqrt{-5}$ with $a^2 + 5b^2 = 1$, so $b = 0$ and $a = \pm 1$; thus $\beta = \pm 1$, which in either case is a unit, since $1 = 1^{-1}$ and $-1 = (-1)^{-1}$. We conclude that 7 is an irreducible element.

Now we show that 7 is not prime. We know that 7 is prime if and only if the ideal (7) of R is prime if and only if $R/(7)$ is a domain. By part (a), we have $R/(7) \cong (\mathbb{Z}/7)[x]/(x^2 + [5]_7)$,

¹Hint: Consider the complex norm $N : \mathbb{C} \rightarrow \mathbb{R}$ given by $N(a + bi) = (a + bi)(a - bi) = a^2 + b^2$. You can use without proof that $N(\alpha\beta) = N(\alpha)N(\beta)$.

and since being a domain is an isomorphism invariant, it suffices to show that $(x^2 + [5]_7)$ is not a prime ideal. Indeed, $x^2 + [5]_7 = (x - [3]_7)(x + [3]_7)$ shows that $x^2 + [5]_7$ is reducible, so the ideal it generates is not prime. \square

Problem 3. Let $R = \mathbb{Z}[\sqrt{-2}]$ where $\sqrt{-2} = \sqrt{2} \cdot i \in \mathbb{C}$ and $\mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} \mid a, b \in \mathbb{Z}\}$.

(a) Show that R is a Euclidean domain.

Proof. Let $\alpha, \beta \in \mathbb{Z}[\sqrt{-2}]$ and let $\frac{\alpha}{\beta} = p + q\sqrt{-2} \in \mathbb{Q}(\sqrt{-2})$ (here we use that the fraction field of $\mathbb{Z}[\sqrt{-2}]$ is $\mathbb{Q}(\sqrt{-2})$). Now pick $s, t \in \mathbb{Z}$ so that $|p - s| \leq 1/2$ and $|q - t| \leq 1/2$. We have

$$\alpha = \beta(s + t\sqrt{-2}) + \beta(p + q\sqrt{-2}) - \beta(s + t\sqrt{-2}).$$

Set $q = s + t\sqrt{-2}$ and set $r = \beta(p + q\sqrt{-2}) - \beta(s + t\sqrt{-2}) = \beta(s + t\sqrt{-2} - (p + q\sqrt{-2}))$ and notice that $q \in \mathbb{Z}[\sqrt{-2}]$ because $s, t \in \mathbb{Z}$ and $r \in \mathbb{Z}[\sqrt{-2}]$ by closure. If $r = 0$ we're good, and if $r \neq 0$ then, using that the complex squared norm is multiplicative as well as the Pythagorean Theorem and the choice for s, t , we have

$$\begin{aligned} N(r) &= N(\beta(s + t\sqrt{-2} - (p + q\sqrt{-2}))) = N(\beta)N(s + t\sqrt{-2} - (p + q\sqrt{-2})) \\ &\leq N(\beta) \cdot (1/4 + 2 \cdot 1/4) = N(\beta) \cdot \frac{3}{4} < N(\beta). \end{aligned}$$

Thus the norm function N makes $\mathbb{Z}[i]$ into a Euclidean domain. \square

(b) Show that $R/(5)$ is a field.

Proof. We claim that 5 is irreducible in R . Indeed, if $5 = \alpha\beta$, we have $25 = N(\alpha)N(\beta)$ with $N(\alpha), N(\beta) \in \mathbb{Z}_{\geq 0}$. We can see that $N(\alpha) = 5$ is impossible by an analysis of cases, and if $N(\alpha) = 1$ then $\alpha = \pm 1$ is a unit, similarly to above. We conclude that 5 is irreducible. Since R is a Euclidean domain, and hence a PID, we then know that (5) is a maximal ideal, so $R/(5)$ is a field. \square

(c) Show that for any nonzero ideal $I \subseteq R$, the quotient ring R/I is finite.

Proof. Since R is a PID, we can write $I = (f)$ and note that $f \neq 0$ since $I \neq \{0\}$. We claim that for any element $x \in R/I$ there is some $g \in R$ such that $x = g + I$ and $N(g) \leq N(f)$ or $g = 0$. Indeed, by division, if $x = r + I$, we have $r = qf + g$ with $N(g) \leq N(f)$; then $x = g + I$ since $r - g = qf \in I$.

Now, we note that for any $n \in \mathbb{Z}_{\geq 0}$, the set $S_n = \{\alpha \in R \mid N(\alpha) < n\}$ is finite: indeed, if $N(a + b\sqrt{-2}) < n$, then $a^2 + 2b^2 < n$ implies $|a|, |b| < n$. By the previous claim, the map $S_n \cup \{0\} \rightarrow R/I$ given by $r \mapsto r + I$ is surjective, so R/I is finite. \square