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. Note in the notation of the statement, $x^3 + x + 1 \in I$ denotes a polynomial in $\mathbb{Z}[x]$ and $x^3 + x + 1$ in the right-hand side of the isomorphism denotes the polynomial in $(\mathbb{Z}/3)[x]$ whose corresponding coefficients are $[1]_3$.

Consider the homomorphism $\pi : \mathbb{Z}[x] \to (\mathbb{Z}/3)[x]/(x^3+x+1)$ given by $f(x) \mapsto \overline{f}(x) + (x^3 + x + 1)$, where $\overline{f}$ denotes the polynomial f with coefficients taken modulo 3, and $(x^3 + x + 1)$ is the principal ideal generated by $x^3 + x + 1$ in $(\mathbb{Z}/3)[x]$. This is a composition of two surjective homomorphisms, namely the map $\mathbb{Z}[x] \to (\mathbb{Z}/3)[x]$ reducing coefficients modulo 3, and the quotient map $(\mathbb{Z}/3)[x] \to (\mathbb{Z}/3)[x]/(x^3 + x + 1)$, so π is a surjective ring homomorphism. We claim that the kernel is I. Indeed, we have

$$\begin{aligned}\pi(f) = 0 &\iff \overline{f}(x) + (x^3 + x + 1) = (x^3 + x + 1) \text{ in } (\mathbb{Z}/3)[x]/(x^3 + x + 1)\\ &\iff \overline{f}(x) \in (x^3 + x + 1) \text{ in } (\mathbb{Z}/3)[x]\\ &\iff \overline{f}(x) = \overline{g}(x)(x^3 + x + 1) \text{ for some } \overline{g} \in (\mathbb{Z}/3)[x]\end{aligned}$$

9 Taking representatives in $\mathbb{Z}$ for the coefficients of $\overline{g}$, we can find a polynomial g with image $\overline{g}$ in $(\mathbb{Z}/3)[x]$. Then

$$\begin{aligned}\overline{f}(x) = \overline{g}(x)(x^3 + x + 1) &\iff f(x) = g(x)(x^3 + x + 1) + 3h(x) \in \mathbb{Z}[x] \text{ for some } h \in \mathbb{Z}[x]\\ &\iff f(x) \in (3, x^3 + x + 1).\end{aligned}$$

Thus $\ker(\pi) = I$. The isomorphism results from the First Isomorphism Theorem. □

Alternative proof. We prepare with a Lemma.

LEMMA: If $\phi : R \cong S$ is a ring isomorphism and $J \subseteq R$ is a proper ideal, then $R/J \cong S/\phi(J)$.

PROOF: The map $R \xrightarrow{\phi} S \xrightarrow{\pi} S/\phi(J)$ is a composition of two surjective ring homomorphisms, and hence is a surjective ring homomorphism. The kernel of this map is $\phi^{-1}(\phi(J)) = J$, since J is bijective. The Lemma follows by the First Isomorphism Theorem.

We continue with the proof. Consider $\mathbb{Z}[x] \supseteq I \supseteq (3)$. By the Cancelling Isomorphism Theorem, we have

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

Note that the ideal $I/(3)$ of $\mathbb{Z}[x]/(3)$ is a principal ideal generated by $x^3+x+1+(3)$, since any element $3f(x)+(x^3+x+1)g(x)+(3)$ can be written as $\big(x^3+x+1+(3)\big)\big(g(x)+(3)\big)$.

From a Theorem in class, we have $\mathbb{Z}[x]/(3) \cong (\mathbb{Z}/3)[x]$ by the map $f(x)+(3) \mapsto \overline{f}$ where $\overline{f}$ denotes the polynomial f with coefficients taken modulo 3. We note that if $\phi : R \cong S$ is an isomorphism and $J \subseteq R$ is a proper ideal, then $R/J \cong S/\phi(J)$: the map $R \xrightarrow{\phi} S \to S/\phi(J)$ is a surjective ring homomorphism with kernel J, and the First Isomorphism Theorem gives the result. Then, the image of $I/(3)$ under this isomorphism is the multiples of x^3+x+1 in $\mathbb{Z}/3[x]$, namely (x^3+x+1) in $\mathbb{Z}/3[x]$. Then we have $R/I \cong \frac{\mathbb{Z}[x]/(3)}{(x^3+x+1+(3))} \cong \frac{\mathbb{Z}/3[x]}{(x^3+x+1)}$. □

(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 $f \in \mathbb{Z}/3[z]$, $(f) \supseteq (x^3+x+1)$ 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 $(3, x^2+x+1)$. □

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 $\phi : \mathbb{Z}[x] \to R$ 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 since the leading coefficient of f is a unit, we can apply the division algorithm to write $f(x) = (x^2+5)q(x)+r(x)$ 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 $\overline{\phi} : \mathbb{Z}[x]/(x^2+5) \to R, \overline{\phi}(f(x)+(x^2+5)) = f(\sqrt{-5})$.

For the latter isomorphism, let us replace R by $\mathbb{Z}[x]/(x^2+5)$ and (p) by $(p+(x^2+5))$, as $R/(p) \cong \frac{\mathbb{Z}[x]/(x^2+5)}{(p+(x^2+5))}$ by the Lemma above. Now, consider $\psi : \mathbb{Z}[x]/(x^2+5) \mapsto (\mathbb{Z}/p)[x]/(x^2+[5]_p)$ given by $f(x)+(x^2+5) \mapsto \overline{f}(x)+(x^2+[5]_p)$. We can see that this is a well-defined surjective ring homomorphism by the universal mapping property of quotients starting with the homomorphism $\phi' : \mathbb{Z}[x] \to (\mathbb{Z}/p)[x]/(x^2+[5]_p)$ given by $f(x) \mapsto \overline{f}(x)+(x^2+[5]_p)$, which is a composition of two surjective ring homomorphisms (along similar lines to problem 1), and noting that (x^2+5) is contained in the kernel ψ'.

We claim that $\ker(\psi)$ is the principal ideal generated by p (more properly $p+(x^2+5)$) in $\mathbb{Z}[x]/(x^2+5)$. Indeed, we have (along the lines of problem 1, but quicker)

$$\begin{aligned}\psi(f)=0 &\iff \overline{f}(x)=\overline{g}(x)(x^2+[5]_p) \text{ in } (\mathbb{Z}/p)[x],\ \text{for some } g(x)\in\mathbb{Z}[x]\\ &\iff f(x)=g(x)(x^2+5)+ph(x) \text{ in } \mathbb{Z}[x],\ \text{for some } g(x),h(x)\in\mathbb{Z}[x]\\ &\iff f(x)+(x^2+5)=ph(x)+(x^2+5) \text{ in } \frac{\mathbb{Z}[x]}{(x^2+5)},\ \text{for some } h(x)\in\mathbb{Z}[x]\\ &\iff f(x)+(x^2+5)=(p+(x^2+5))(h(x)+(x^2+5)) \text{ in } \frac{\mathbb{Z}[x]}{(x^2+5)},\ \text{for } h(x)+(x^2+5)\in\frac{\mathbb{Z}[x]}{(x^2+5)}\\ &\iff f(x)+(x^2+5)\in(p+(x^2+5)) \text{ in } \frac{\mathbb{Z}[x]}{(x^2+5)}.\end{aligned}$$

The result then follows by the First Isomorphism Theorem. □

Alternative proof for latter isomorphism. We can argue again by the Cancelling Isomorphism Theorem. First, by the Lemma above, we have

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

Observe that the ideal $\frac{(p,x^2+5)}{(x^2+5)}$ is the principal ideal in $\mathbb{Z}[x]/(x^2+5)$ generated by $p+(x^2+5)$, along the same lines as argued in problem 1. Thus, by the Cancelling Isomorphism Theorem we can write

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

On the other hand, we can use the Cancelling Isomorphism Theorem to obtain

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

We apply the Lemma one more time with the isomorphism $\mathbb{Z}[x]/(p)\cong\mathbb{Z}/p[x]$ from class and the ideal $I=(x^2+5+(p))$ to get

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

The desired isomorphism is the composition of those given above. □

(b) Show that the integer 7 is irreducible[1] 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 $N(\beta)=1$.

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

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 $R/(7) \cong (\mathbb{Z}/7)[x]/(x^2 + [5]_7)$, 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. □

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

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

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

(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. □

(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 $S_n = \{\alpha \in R \mid N(r) < n\}$ 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 $S_n \cup \{0\} \to R/I$ given by $r \mapsto r + I$ is surjective, so R/I is finite. □