Problem Set 1

Due Thursday, January 22

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. Refresh your knowledge of Gauss' Lemma, and read the short Section 10.2 from the Math 817 lecture notes on Eisenstein's Criterion. Then

(a) Prove that the polynomial $x^2 + y^2 - 1$ is irreducible in $\mathbb{Q}[x, y]$.

Proof. Recall that $\mathbb{Q}[x, y] = \mathbb{Q}[x][y]$. Consider the prime ideal $P = (x - 1) \subseteq \mathbb{Q}[x]$; this is prime since $x - 1$ is irreducible and $\mathbb{Q}[x]$ is a UFD. Note that $x^2 - 1 = (x - 1)(x + 1) \in P$ since $x - 1 \mid x^2 - 1$ but $x^2 - 1 \notin P^2$ since $(x - 1)^2 \mid x^2 - 1$. Since $0 \in P$, and the leading coefficient of $x^2 + y^2 - 1$ as a polynomial in y is 1, the hypotheses of Eisenstein's criterion apply, so this polynomial is irreducible. □

(b) Prove[1] that $5x^4 + 7x^3 + 11x^2 + 6x + 1$ is irreducible in $\mathbb{Q}[x]$.

Proof. By Gauss' Lemma, it suffices to show that $f(x) = 5x^4 + 7x^3 + 11x^2 + 6x + 1$ is irreducible in $\mathbb{Z}[x]$. Suppose that $f = gh$, with $g, h \in \mathbb{Z}[x]$; we want to show that either g or h is a unit. Without loss of generality, we can consdier three cases: $\deg(g) = 0$ and $\deg(h) = 4$; $\deg(g) = 1$ and $\deg(h) = 3$; or $\deg(g) = 2$ and $\deg(h) = 2$.

We make some remarks before we separate the three cases. Note that the leading coefficient of g times that of h is 5, so the leading coefficients of g and h are ± 1 or ± 5.

Consider the surjective homomorphism $\pi : \mathbb{Z}[x] \to \mathbb{Z}/2[x]$ given by reducing the coefficients modulo 2. Since the leading coefficients of g and h are odd, the degree of $\pi(g)$ equals that of g, and likewise for h. We have

$$\pi(f) = x^4 + x^3 + x^2 + 1 = (x + 1)(x^3 + x + 1) \qquad \text{in } \mathbb{Z}/2[x].$$

The polynomial $x+1$ is irreducible for degree reasons, and $p(x) = x^3+x+1$ has no roots since $p(0) = p(1) = 0$, and thus $p(x)$ is irreducible in $\mathbb{Z}/2[x]$ since any factorization into nonunits would have a factor of degree one, which would have a root.

We now analyze the cases:

- $\deg(g) = 0$ and $\deg(h) = 4$: Based on the leading coefficients, we either have $g = \pm 1$ or $g = \pm 5$. If f were a multiple of 5, then each coefficient would be, but this is not so. Thus, in this case $g = \pm 1$, which is a unit.

[1] Hint: Consider this polynomial in $\mathbb{Z}[x]$ and go modulo 2.

- $\deg(g) = 1$ and $\deg(h) = 3$: In this case, g yields a root over $\mathbb{Q}$. By the Rational Root Theorem, any rational root of f is of the form ± 1 or $\pm 1/5$. Plugging each of these four into f shows that none is a root, so this case does not occur.
- $\deg(g) = \deg(h) = 2$: In this case, we have $\pi(f) = \pi(g)\pi(h)$ with $\deg(\pi(g)) = \deg(\pi(h)) = 2$. However, $\pi(f)$ factors as a product of irreducibles of degrees 1 and 3 in $\mathbb{Z}/2[x]$. As $p(x)$ is prime, $p(x)$ divides either $\pi(g)$ or $\pi(h)$. It follows that either $\pi(g)$ or $\pi(h)$ has degree at least 3, so this case does not occur.

This completes the proof. □

(c) Let p be a prime number. Prove[2] that the polynomial $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ is irreducible in $\mathbb{Q}[x]$.

Proof. We again apply Gauss' Lemma and aim to show that $f(x)$ is irreducible in $\mathbb{Z}[x]$. Consider the homomorphism $\phi : \mathbb{Z}[x] \to \mathbb{Z}[x]$ mapping $f(x) \mapsto f(x+1)$; this is an evaluation homomorphism. This is bijective since the map $f(X) \mapsto f(x-1)$ is its inverse. It follows that $f(x+1)$ is irreducible if and only if $f(x)$ is.

Now note that $f(x)(x-1) = x^p - 1$, so

$$f(x+1)x = (x+1)^p - 1 = x^p + \binom{p}{1}x^{p-1} + \cdots + \binom{p}{p-1}x,$$

and thus

$$f(x+1) = x^{p-1} + \binom{p}{1}x^{p-2} + \cdots + \binom{p}{p-1}.$$

Now, for p prime, we have $\binom{p}{i} = \frac{p!}{i!(p-i)!}$, so $i!(p-i)!\binom{p}{i} = p!$ in $\mathbb{Z}$. For $1 \leq i \leq p-1$, the factorials $i!(p-i)!$ are not multiples of p, since they are products of integers less than p; since p divides $p!$, we must have that p divides $\binom{p}{i}$ by definition of prime. Also, $\binom{p}{p-1} = p$ which is not a multiple of p^2. Thus, Eisenstein's criterion applies to $f(x+1)$, which is thus irreducible. □

Problem 2. Let R be a ring and let M be a left R-module. The **annihilator** of M is

$$\operatorname{ann}_R(M) := \{r \in R \mid rm = 0 \text{ for all } m \in M\}.$$

Show that $\operatorname{ann}_R(M)$ is a two-sided ideal of R.

Proof. Note that $0 \in \operatorname{ann}_R(M)$ since $0 \cdot m = 0$ for all $m \in M$.Let $a, b \in \operatorname{ann}_R(M)$. Then for any $m \in M$, $(a+b)m = am + bm = 0$, so $r + s \in M$. Let $a \in \operatorname{ann}_R(M)$ and $r \in R$. Then $(ra)m = r(am) = r0 = 0$, and $(ar)m = a(rm) = 0$. Thus, by the two-step test for ideals, the set $\operatorname{ann}_R(M)$ is a two-sided ideal. □

[2]Hint: Consider $f(x+1)$. You can use without proof that the binomial theorem holds in any commutative ring R: for any $A, B \in R$ and positive integer n,

$$(A+B)^n = \sum_{i=0}^{n} \binom{n}{i} A^i B^{n-i}, \qquad \text{where } \binom{n}{i} = \frac{n!}{i!(n-i)!} \in \mathbb{Z}_{\geq 0}.$$

Problem 3. Let R be a ring and M be a left R-module.

(a) Let I be a left ideal, and define

$$IM := \{\sum_i a_i m_i \mid a_i \in I, m_i \in M\}.$$

Show that IM is a submodule of M.

Proof. We use the two-step test. Note first that $0 \in I$ and $0 \in M$ yields $0 = o \cdot 0 \in IM$. Now for $\sum_i a_i m_i, \sum_j a'_j m'_j \in IM$, their sum is in IM. For $r \in R$, and $\sum_i a_i m_i \in IM$, we have $r\left(\sum_i a_i m_i\right) = \sum_i r(a_i m_i) = \sum_i (ra_i)m_i$, and since $ra_i \in I$, this is in IM. Thus, this is a submodule. □

(b) Show that if I is a two-sided ideal and $IM = 0$, then M is a left R/I-module by the rule $(r + I)m := rm$.

Proof. First we check that this operation is well-defined. Indeed, if $r + I = s + I$, then $r - s \in I$, so for $m \in M$, $rm - sm = (r - s)m = 0$, and hence $rm = sm$. The module axioms now follow from those for M as an R-module: Let $r + I, s + I \in R/I$ and $m, n \in M$.

- $(r + I + s + I)m = (r + s + I)m = (r + s)m = rm + sm = (r + I)m + (s + I)m$.
- $((r + I)(s + I))m = (rs + I)m = (rs)m = r(sm) = (r + I)(sm) = (r + I)((s + I)m)$.
- $(r + I)(m + n) = r(m + n) = rm + rn = (r + I)m + (r + I)n$.
- $(1 + I)m = 1m = m$.

□

(c) Show that if I is a two-sided ideal, then M/IM is an R/I-module.

Proof. Note that $I(M/IM) = 0$. The assertion then follows from the previous part. □

Problem 4. Let R be a commutative ring, M a module, and I an ideal.

(a) Prove that ${}_IM := \{m \in M \mid am = 0 \text{ for all } a \in I\}$ is a submodule of M.

Proof. We use the two-step test. Note first that $0 \in {}_IM$. Then let $m, n \in {}_IM$. Let $a \in I$. Then $a(m + n) = am + an = 0 + 0 = 0$. Thus, $m + n \in {}_IM$. Now let $m \in {}_IM$ and $r \in R$. Let $a \in I$. Then $a(rm) = (ar)m = (ra)m = r(am) = r0 = 0$. Thus $rm \in {}_IM$. It follows that ${}_IM$ is a submodule. □

(b) Prove that $\mathrm{Hom}_R(R/I, M) \cong {}_IM$.

Proof. Consider the map

$$\begin{aligned} \mathrm{Hom}_R(R/I, M) &\xrightarrow{\Psi} N \\ f &\longmapsto f(1 + I). \end{aligned}$$

We claim that this is a well-defined isomorphism of R-modules.

- Given any $f \in \mathrm{Hom}_R(R/I, M)$, we need to check that $\Psi(f) \in N$. Consider $a \in I$ and $f \in \mathrm{Hom}_R(R/I, M)$. Then $a + I = 0 + I$, and since f is a homomorphism of R-modules, we have
$$a\Psi(f) = af(1 + I) = f(a + I) = f(0 + I) = 0.$$
Thus $\Psi(f) \in N$.
- We claim that Ψ is an R-module homomorphism. Given $f, g \in \mathrm{Hom}_R(R/I, M)$, we have
$$\begin{aligned}\Psi(f + g) &= (f + g)(1 + I) \\ &= f(1 + I) + g(1 + I) \quad \text{by definition of } f + g \\ &= \Psi(f) + \Psi(g).\end{aligned}$$
Moreover, for any $r \in R$ we have
$$\begin{aligned}\Psi(rf) &= (rf)(1 + I) \\ &= f(r(1 + I)) && \text{by definition of } rf \\ &= rf(1 + I) && \text{since } f \text{ is a homomorphism of } R\text{-modules} \\ &= r\Psi(f).\end{aligned}$$
- We claim that Ψ is injective. Indeed, given $f, g \in \mathrm{Hom}_R(R/I, M)$,
$$\Psi(f) = \Psi(g) \implies f(1 + I) = g(1 + I),$$
but the image of $1 + I$ completely determines the homomorphism, so this implies that $f = g$.
- We claim that Ψ is surjective. Given $n \in N$, consider the function
$$\begin{aligned}R/I &\xrightarrow{f} M \\ r &\longmapsto rn.\end{aligned}$$
Given any $r + I = s + I$ in R/I, we have $r - s \in I$. Since $n \in N$, we conclude that
$$(r - s)n = 0 \implies rn = sn.$$
Thus $f(r+I) = f(s+I)$, and f is a well-defined function. Moreover, for any $r+I, s+I \in R/I$ and any $t \in R$, we have
$$f((r + I) + (s + I)) = f((r + s) + I) = (r + s)n = rn + sn = f(r + I) + f(s + I),$$
and
$$f(t(r + I)) = f(tr + I) = (tr)n = t(rn) = tf(n).$$
Therefore, f is a homomorphism of R-modules. By construction, we see that
$$\Psi(f) = f(1 + I) = 1n = n.$$
We conclude that Ψ is indeed surjective

We have shown that Ψ is an isomorphism of R-modules. □