Algebra II: Homework 2

Due on February 10, 2021

Professor Walton

Gabriel Gress

Last edited February 10, 2021

Problem 1

Collaborated with the Yellow group on this problem. *Claim.*

(a). Show that $x^4 + 10x + 5$ is irreducible over $\mathbb{Z}$.

(b). Show that $x^6 + 30x^5 - 15x^3 + 6x - 120$ is irreducible over $\mathbb{Z}$.

(c). Show that $x^{p-1} + x^{p-2} + \ldots + x + 1$ is irreducible over $\mathbb{Z}$ for p prime.

Proof. 1. Eisenstein's criterion applies in this case with $p = 5$. Every coefficient is divisible by 5, and the constant is not divisible by $5^2 = 25$.

2. Eisenstein's criterion applies in this case with $p = 3$– every coefficient is divisible by 3, but $3^2 = 9 \not| 120$.

3. Recall that if $f(x+1)$ is irreducible, then $f(x)$ is irreducible. Then we substitute $x+1$ to get:

$$(x+1)^{p-1} + (x+1)^{p-2} + \ldots + (x+1) + 1$$

The binomial theorem allows us to expand

$$\sum_{i=0}^{p-1} \sum_{j=0}^{i} \binom{j}{i} x^j$$

From here, one can observe that the coefficient of the constant term is 1 for each expansion, and hence the new constant term has the value p. Furthermore, each coefficient is divisible by p, and so Eisenstein's criteria applies! Because this expansion is irreducible, the original polynomial must also be irreducible.

□

Problem 2

Claim.

Let M be a module over the ring R. Then for all $r \in R$ and $m \in M$, prove that

(a). $0m = r0 = 0$.

(b). $r(-m) = -(rm) = (-r)m$.

(c). If R has a multiplicative identity and M is unital, then $(-1)m = -m$.

Proof. (a). Recall that $(r+s)m = (rm) + (sm)$. Choose $r = 1_R$, $s = 0_R$. Then $(1+0)m = (1m) + (0m) \implies m = m + 0m \implies 0m = 0$. Now let r be arbitrary and $m = 0_M, n \in M$ arbitrary. Then

$$\begin{aligned} r * (0_M + n) = (r * 0_M) + (r * n) \implies \\ rn = (r0) + rn \implies (r0) = 0 \end{aligned}$$

as desired.

Problem 2 continued on next page...

(b). Observe that $r(m-m) = rm + r(-m)$. This gives us $r(-m) = -(rm)$. Now observe that $(r-r)m = (rm) + (-r)m \implies (-r)m = -(rm)$.

(c). One can verify this by observing $(1-1)m = (1m) + (-1)m = m + (-1)m \implies (-1)m = -m$.

□

Problem 3

Collaborated with the Yellow group on this problem. *Claim.* Let R be a ring, and let M be a left R-module. Take $\{N_i\}_{i\in I}$ to be a nonempty collection of (left R-)submodules of M.

(a). Show that $\bigcap_{i\in I} N_i$ is a submodule of M.

(b). Is $\bigcup_{i\in I} N_i$ is a submodule of M? Prove this statement or provide a counterexample.

Proof.

1. Consider if $\bigcap_{i\in I} N_i \neq 0$. Then consider
$$n + rn' \tag{1}$$
for $n, n' \in \bigcap_{i\in I} N_i$. Recall that for any $i \in I$, $n, n' \in N_i$. Then because N_i is a submodule, we know that $n + rn' \in N_i$, and therefore $n + rn' \in \bigcap_{i\in I} N_i$.
2. The statement is false. Counterexample: $N_1 = \{(x,0) \mid x \in \mathbb{R}\}$ and $N_2 = \{(0,y) \mid y \in \mathbb{R}\}$. These are submodules of $\mathbb{R}$-modules over $\mathbb{R}^2$, as they are vector spaces. However, their union is the x and y-axes in $\mathbb{R}^2$. But this is not closed under the operations of the submodule, as $(x,0) + (0,y) = (x,y) \notin X, Y$ if $x, y \neq 0$.

□

Problem 4

Claim. Show that $(x-1)(x-2)\dots(x-n) - 1$ is irreducible over $\mathbb{Z}$, for each $n \in \mathbb{N}$.

Proof. Assume for the sake of contradiction that $f(x) = (x-1)(x-2)\dots(x-n) - 1$ decomposes into some $g(x)h(x)$, where $g(x), h(x)$ are polynomials with degree $< n$. Then we observe that $g(i)h(i) = -1$ for $1 \le i \le n$ with i an integer. This implies that $g(i) = \pm 1$ and $h(i) = \mp 1$. Then observe that $g(i) + h(i) = 0$ for each i, and hence the polynomial given by $g(x) + h(x)$ has at least n roots. But $g(x)$ and $h(x)$ are both polynomials with degree $< n$, so it cannot possibly have $\ge n$ roots. Thus, $f(x)$ cannot be decomposed into the product of two polynomials. □

Problem 4 continued on next page...

Problem 5

Claim. If M is a finite abelian group then M is naturally a $\mathbb{Z}$-module. Can this action be extended to make M into a $\mathbb{Q}$-module?

Proof. No, if such an action existed it would be inconsistent with the natural action of the $\mathbb{Z}$-module. Because M is a finite abelian group, it has some finite order n. Then $nm = 0$ for all $m \in M$. If we try to extend to a $\mathbb{Q}$-module, we must satisfy

$$m = (\frac{1}{n}n)m = \frac{1}{n}(nm) = \frac{1}{n}0 = 0$$

and so it can only extend when M is trivial. □

Problem 6

Claim.

An element m of the R-module M is called a **torsion element** if $rm = 0$ for some nonzero element $r \in R$. The set of torsion elements is denoted

$$\text{Tor}(M) = \{m \in M \mid rm = 0 \text{ for some nonzero } r \in R\}.$$

(a). Prove that if R is an integral domain then $\text{Tor}(M)$ is a submodule of M.

(b). Give an example of a ring R and an R-module M such that $\text{Tor}(M)$ is not a submodule.

(c). If R has zero divisors show that every nonzero R-module has nonzero torsion elements.

Proof. (a). We need to show that $\text{Tor}(M)$ is a subgroup and is closed under the R-action. If $m_1, m_2 \in \text{Tor}(M)$, then $r(m_1m_2) = (rm_1)m_2 = (0)m_2 = 0$ for some $r \in R$ by hypothesis, and hence $m_1m_2 \in \text{Tor}(M)$. Now we verify that it is closed under the action of R. Assume $m \in \text{Tor}(M)$. We want to show that $rm \in \text{Tor}(M)$ for arbitrary R. Let r_1 be the non-zero element such that $r_1m = 0$. Then $r_1(rm) = (r_1r)m = (rr_1)m = r(r_1m) = r(0) = 0$. Note that we are using that R is an integral domain here via commutativity. Ergo, it is closed under the R-action, which gives us that $\text{Tor}(M)$ is a submodule, as desired.

(b). Consider the module over a ring R of 2×2 matrices with entries in R. This fails because it is not an integral domain– to see this, observe that

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

are in $\text{Tor}(R)$. But their sum is the identity matrix in R, which is clearly not a torsion element. Hence, it is not a subgroup and therefore a submodule.

(c). If R has zero divisors, then that implies that there exists $rs = 0$ where $r, s \neq 0$. Now consider (sm) for m non-zero. This is an element in M. If it is zero, then we are done, as s is non-zero, and so m is a torsion element. If it is not, then (sm) is a non-zero element in M, and we know that $r(sm) = 0$. Ergo, (sm) is a non-zero element in M that is a torsion element. One of these cases must hold, and so if R has zero divisors there always exist nonzero torsion elements in every nonzero R-module.

□

Problem 6 continued on next page...

Problem 7

Claim. Let M, N be R-modules. Prove:

(a). If $\varphi \in \mathrm{Hom}_R(M, N)$, then $\ker(\varphi)$ is a submodule of M and $\varphi(M)$ is a submodule of N.

(b). If $\varphi \in \mathrm{Hom}_R(M, N)$ and $\psi \in \mathrm{Hom}_R(N, P)$, then $\psi \circ \varphi \in \mathrm{Hom}_R(M, P)$.

Proof. (a). It holds from basic group theory (because R-module homomorphisms are group homomorphisms) that $\mathrm{Ker}\varphi$ and $\mathrm{Im}\varphi$ are subgroups of their respective domain. It remains to show that they are closed under the R-action. Let $m \in \mathrm{Ker}\varphi, n \in \mathrm{Im}\varphi$, and $r \in R$ be arbitrary. Then

$$\varphi(rm) = r\varphi(m) = r(0) = 0 \implies rm \in \mathrm{Ker}\varphi$$
$$rn \in M \implies rn = m_1 \in M \implies \varphi(rn) = \varphi(m_1) \in \mathrm{Im}(\varphi)$$

as desired.

(b). From basic group theory, we know that $\psi \circ \varphi$ is a group homomorphism from $M \to P$. Once again, it remains to check that it respects the R-action.

$$\psi \circ \varphi(rm) = \psi(r\varphi(m)) = r\psi(\varphi(m)) = r(\psi \circ \varphi)(m)$$

as desired.

□