HOMEWORK 4

Due date: Tuesday of Week 5

Exercises: 4.1, 4.2, 4.3, 4.5, 4.6, 4.9, 4.16, 4.17, 4.18, 5.1, 5.2, 5.3, 5.6, 5.7, 5.10, pages 380-381, Exercises: 1.1, 1.3, 1.4, 2.1, 2.2, 2.4, page 437.

Exercise 5.9, page 381 is hard. You can give it a try. For Ex.1.3, page 437, the answer should be m^n, where n is the degree of α, or the degree of its minimal polynomial. For Ex. 2.1, page 437, the answer is no. Think about the reason. Ex. 2.4 page 437 is related to Exercise 2.1 page 437.

Problem 1. *Let p be a prime integer. Show that the polynomial $f = x^7 - p^2 \in \mathbb{Q}[x]$ is irreducible.*

Hint: You can imitate the proof of Eisenstein criterion.

Problem 2. *Let $\mathfrak{p}$ be a nonzero prime ideal of the Gauss integer ring $\mathbb{Z}[i]$. Show that $\mathbb{Z}[i]/\mathfrak{p}$ is a field and thus $\mathfrak{p}$ is a maximal ideal. Determine the order of $\mathbb{Z}[i]/\mathfrak{p}$.*

Hint: Show that $\mathbb{Z}[i]/\mathfrak{p}$ is finite integral domain and thus is a field. See Ex.7.1, page 357 and Ex. 1.3, page 437.

Problem 3. *Consider the polynomial $f = x^4 - 10x^2 + 1 \in \mathbb{Z}[x]$. Show that f is irreducible. Moreover, for each prime p, show that $\psi_p(f) \in \mathbb{F}_p[x]$ is reducible,*

Hint: See this link and this link.

Let R be a commutative ring and let M be an R-module. For $m \in M$, define $\operatorname{Ann}(m) = \{r \in R : rm = 0\}$.

Problem 4. *Show that $\operatorname{Ann}(m)$ is an ideal of R. Moreover, the map $\phi : R \to M$ defined by $\phi(r) = rm$ defines an isomorphism $R/\operatorname{Ann}(m) \cong \langle m \rangle$, where $\langle m \rangle$ denotes the submodule of M generated by m, namely, $\langle m \rangle = \{rm : r \in R\}$.*

In particular, if $M = R$, then $R/\operatorname{Ann}(a) \cong (a)$, where (a) denotes the principal ideal generated by a. So when is (a) a free module?

Let R be a ring and let $S \subset R$ be a multiplicative set (which means $1 \in S$, and if $a, b \in S$, then $ab \in S$). We have defined $S^{-1}R$. This construction can also be defined on modules. Let M be an R-module and we define an equivalence relation on $M \times S$ by

$$(m, s) \sim (n, t) \iff u(tm - sn) = 0, \text{ for some } u \in S.$$

Problem 5. *Show that $\sim$ is an equivalence relation.*

Let m/s denotes the equivalence class of (m, s) for $m \in M, s \in S$ and let $S^{-1}M$ denotes the set of all equivalence classes. Define an abelian group structure on $S^{-1}M$ by

$$m/s + n/t = (tm + sn)/(st).$$

Define a module structure on $S^{-1}M$ over the ring $S^{-1}R$ by

$$(r/s)(m/t) = (rm)/(st), r \in R, s, t \in S, m \in M.$$

Check that the above definitions are well-defined and indeed defines a $S^{-1}R$ module structure on $S^{-1}M$. If $\mathfrak{p}$ is a prime ideal and $S = R - \mathfrak{p}$, then we write $S^{-1}M$ as $M_{\mathfrak{p}}$, which is called the localization of M at $\mathfrak{p}$. When is an element $x/s \in M_{\mathfrak{p}}$ zero?

Problem 6. *Let R be a ring $S \subset R$ be a multiplicative subset. Let M, N be two modules.*

(1) *Show that the map $\iota_M : M \to S^{-1}M$ defined by $m \mapsto m$ is an R-module homomorphism.*

(2) *Suppose* $f \in \mathrm{Hom}_R(M,N)$ *be a module homomorphism. Consider the map* $S^{-1}(f) : S^{-1}M \to S^{-1}N$ *defined by*

$$S^{-1}(f)(m/s) = f(m)/s.$$

Show that $S^{-1}(f)$ *is well-defined and it defines a homomorphism in* $\mathrm{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N)$. *Moreover, the following diagram*

$$\begin{tikzcd} M \arrow[r, "\iota_M"] \arrow[d, "f"] & S^{-1}M \arrow[d, "S^{-1}(f)"] \\ N \arrow[r, "\iota_N"] & S^{-1}N \end{tikzcd}$$

is commutative

(3) *Suppose that for any* $s \in S$, *the map* $\phi_s : N \to N$ *defined by* $\phi_s(n) = sn$ *is an* R*-module isomorphism. Given* $f \in \mathrm{Hom}_R(M,N)$, *show that there exists a unique homomorphism* $\theta : S^{-1}M \to N$ *such that the following diagram*

$$\begin{tikzcd} M \arrow[rr, "\iota_M"] \arrow[dr, "f"'] & & S^{-1}M \arrow[dl, "\theta"] \\ & N & \end{tikzcd}$$

is commutative.

Problem 7. *Let* M *be an* R*-module. Show that the following are equivalent:*

(1) $M = 0$;
(2) $M_{\mathfrak{p}} = 0$ *for every prime ideal* $\mathfrak{p}$ *of* R;
(3) $M_{\mathfrak{m}} = 0$ *for every maximal ideal* $\mathfrak{m}$ *of* R.

Hint: For (3) $\implies$ (1), by contradiction, take $x \in M$ and $x \neq 0$. Then consider $I = \mathrm{Ann}(x) = \{a \in R : ax = 0\}$. The assumption $x \neq 0$ implies that $I \neq R$. Thus I is contained in a maximal ideal $\mathfrak{m}$. By assumption, $x/1$ is zero in $M_{\mathfrak{m}}$...

Problem 8. *Let* $\phi : M \to N$ *be a homomorphism of* R*-modules. Let* $S \subset R$ *be a multiplicative subset. Define* $S^{-1}(\phi) : S^{-1}M \to S^{-1}N$ *by* $S^{-1}(\phi)(m/s) = \phi(m)/s$. *See Problem 6. Show that* $\ker(\phi_S) = S^{-1}\ker(\phi)$.

$S = A - \mathfrak{p}$ for a prime ideal $\mathfrak{p}$, we write the above $S^{-1}(\phi)$ as $\phi_{\mathfrak{p}}$.

Problem 9. *Let* $\phi \in \mathrm{Hom}_R(M,N)$. *Show the following are equivalent.*

(1) ϕ *is injective;*
(2) $\phi_{\mathfrak{p}}$ *is injective for every prime ideal* $\mathfrak{p}$ *of* R;
(3) $\phi_{\mathfrak{m}}$ *is injective for every maximal ideal* $\mathfrak{m}$ *or* R.

A property on modules and/or its homomorphisms is called a local property if it only depends on localizations. The above problem shows that being injective is a local property. Localization are very important tools in studying modules.

Problem 10. *Let* R *be a ring and* $I \subset R$ *be an ideal. Let* $f \in R$. *Suppose that* $f \in IR_{\mathfrak{m}}$ *for every maximal ideal* $\mathfrak{m}$, *show that* $f \in I$. *Here* $IR_{\mathfrak{m}} = \{ax : a \in I, x \in R_{\mathfrak{m}}\}$.

The condition $f \in IR_{\mathfrak{p}}$ says that f is locally in I at the prime $\mathfrak{p}$. Hint: There are two ways to prove the above. (1) Consider the quotient ring R/I and use an argument similar to Problem 7. (2) The assumption $f \in IR_{\mathfrak{m}}$ says that there exists $a_{\mathfrak{m}} \in I$ and $s_{\mathfrak{m}} \notin \mathfrak{m}$ such that $f = a_{\mathfrak{m}}/s_{\mathfrak{m}}$ for each $\mathfrak{m}$. Consider the ideal J generated by $\{s_{\mathfrak{m}}\}$ as $\mathfrak{m}$ runs through all maximal ideals. Show that $J = R$. The result should follow easily.

The following is an analogue/generalization. Let R be a ring and $\mathfrak{a} \subset R$ be an ideal. Let M be an R-module and let $f \in M$. Suppose that $f \in \mathfrak{a}M_{\mathfrak{p}}$ for every prime ideal $\mathfrak{p}$, is it true that $f \in \mathfrak{a}M$? Here $\mathfrak{a}M = \left\{\sum_{finite} a_i m_i : a_i \in \mathfrak{a}, m_i \in M\right\}$, which is a submodule of M. Actually, one can also pass to the quotient $M/\mathfrak{a}M$. Now a natural question is: is it true that $(M/\mathfrak{a}M)_{\mathfrak{p}} \cong M_{\mathfrak{p}}/\mathfrak{a}M_{\mathfrak{p}}$? The answer should be yes and the proof is not hard.