Week 2: Euclidean Domains, P.I.D.s, and U.F.D.s

Let R be a commutative ring with identity.

Practice Problems

1. Consider the ring $\mathbb{Z}[\sqrt{-5}]$. Show that

$$\begin{aligned}
\left(2, 1-\sqrt{-5}\right)\left(2, 1+\sqrt{-5}\right) &= \left(4, 2+2\sqrt{-5}, 2-2\sqrt{-5}, 6\right) = (2), \\
\left(3, 1-\sqrt{-5}\right)\left(3, 1+\sqrt{-5}\right) &= \left(9, 3+3\sqrt{-5}, 3-3\sqrt{-5}, 6\right) = (3), \\
\left(2, 1+\sqrt{-5}\right)\left(3, 1+\sqrt{-5}\right) &= \left(6, 2+2\sqrt{-5}, 3+3\sqrt{-5}, -4+2\sqrt{-5}\right) = \left(1+\sqrt{-5}\right), \\
\left(2, 1-\sqrt{-5}\right)\left(3, 1-\sqrt{-5}\right) &= \left(6, 2-2\sqrt{-5}, 3-3\sqrt{-5}, -4-2\sqrt{-5}\right) = \left(1-\sqrt{-5}\right).
\end{aligned}$$

   Hint: First show that $(a, b)(c, d) = (ac, ad, bc, bd)$.

   It turns out that each ideal in $\mathbb{Z}[\sqrt{-5}]$ has a unique factorizaton as a product of prime ideals. Why doesn't the equality $(6) = (2)(3) = (1+\sqrt{-5})(1-\sqrt{-5})$ contradict this?

2. (a) Factor 1004913 in $\mathbb{Z}$ and in $\mathbb{Z}[i]$.
   (b) Factor 1004890 in $\mathbb{Z}$ and in $\mathbb{Z}[i]$.

3. (a) Determine all of the ways to write 1004913 as the sum of two squares.
   (b) Determine all of the ways to write 1004890 as the sum of two squares.

Presentation Problems

1. Suppose that R is a P.I.D. and let P be a prime ideal of R. Show that R/P is a P.I.D.

2. Let p be a prime.
   (a) Show that $\mathbb{Z}[i]/(p)$ has p^2 elements.
   (b) Show that if $p \equiv 3 \pmod 4$ then $\mathbb{Z}[i]/(p)$ is a field.
   (c) Show that if $p \equiv 1 \pmod 4$ then $\mathbb{Z}[i]/(p)$ is a product of two fields.

3. Let p be a prime and let $\zeta_p = e^{2\pi i/p}$.
   (a) Show that $x^p - 1 = (x-1)(x-\zeta_p)(x-\zeta_p^2)\dots(x-\zeta_p^{p-1})$
   (b) Show that $1 + x + \ldots + x^{p-1} = (x-\zeta_p)(x-\zeta_p^2)\dots(x-\zeta_p^{p-1})$.
   (c) Show that $p = (1-\zeta_p)(1-\zeta_p^2)\dots(1-\zeta_p^{p-1})$.

   Now suppose that p is odd and let $p^* = (-1)^{(p-1)/2}p$.

   (c) By pairing up the $(1-\zeta_p^k)$ term with the $(1-\zeta_p^{p-k})$ term, show that

$$p^* = \prod_{k=1}^{(p-1)/2} \zeta_p^{-k}(1-\zeta_p^k)^2.$$

   (d) Show that $\sqrt{p^*} \in \mathbb{Z}[\zeta_p]$.

4. We call a ring R *Noetherian* if every ascending chain of ideals of R

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

stabilizes, meaning $I_n = I_{n+1}$ for all sufficiently large n. Note that this implies that every nonempty set of ideals of R contains some maximal element.

Prove that every P.I.D. is Noetherian.

Module Theory Problem

1. Prove that a sequence

$$L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$$

of R-modules is exact if and only if the sequence

$$0 \longrightarrow \mathrm{Hom}_R(N,T) \xrightarrow{g^*} \mathrm{Hom}_R(M,T) \xrightarrow{f^*} \mathrm{Hom}_R(L,T) \longrightarrow 0$$

is exact for any R-module T.

2. Prove that a sequence

$$0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N$$

of R-modules is exact if and only if the sequence

$$0 \longrightarrow \mathrm{Hom}_R(T,L) \xrightarrow{f_*} \mathrm{Hom}_R(T,M) \xrightarrow{g_*} \mathrm{Hom}_R(T,N)$$

is exact for any R-module T.

3. Consider a commutative ladder diagram

$$\begin{tikzcd}
\cdots \arrow[r, "f_2"] & M_1 \arrow[r, "f_1"] \arrow[d, "\varphi_1"] & M_0 \arrow[r, "f_0"] \arrow[d, "\varphi_0"] & M_{-1} \arrow[r, "f_{-1}"] \arrow[d, "\varphi_{-1}"] & \cdots \\
\cdots \arrow[r, "g_2"] & N_1 \arrow[r, "g_1"] & N_0 \arrow[r, "g_0"] & N_{-1} \arrow[r, "g_{-1}"] & \cdots .
\end{tikzcd}$$

of R-modules. Suppose that all the vertical maps φ_i are isomorphisms. Show that the top sequence is exact if and only if the bottom sequence is exact.

Tricky Problems

1. Define the Dirichlet character $\chi\colon \mathbb{Z} \to \{-1,0,1\}$ by

$$\chi(n) = \begin{cases} 0 & n \equiv 0 \pmod 2, \\ 1 & n \equiv 1 \pmod 4, \\ -1 & n \equiv 3 \pmod 4. \end{cases}$$

   (a) Show that $\chi(mn) = \chi(m)\chi(n)$ for all integers m and n.

(b) Let n be a positive integer and write $n = 2^k p_1^{a_1} \dots p_r^{a_r} q_1^{b_1} \dots q_s^{b_s}$ where $p_1, \dots, p_r$ are distinct odd primes congruent to 1 modulo 4 and where $q_1, \dots, q_s$ are distinct odd primes congruent to 3 modulo 4. Show that

$$\begin{aligned}\sum_{d|n} \chi(d) &= \left(\sum_{d|2^k} \chi(d)\right)\left(\sum_{d|p_1^{a_1}} \chi(d)\right) \cdots \left(\sum_{d|p_r^{a_r}} \chi(d)\right)\left(\sum_{d|q_1^{b_1}} \chi(d)\right) \cdots \left(\sum_{d|q_s^{b_s}} \chi(d)\right) \\ &= \begin{cases}(a_1+1)\dots(a_r+1) & \text{every } b_i \text{ is even} \\ 0 & \text{otherwise}\end{cases} \\ &= \frac{1}{4}|\{(x,y) \in \mathbb{Z}^2 \colon x^2+y^2=n\}|.\end{aligned}$$

(c) Show that

$$\frac{|\{(x,y) \in \mathbb{Z}^2 \colon 1 \le x^2+y^2 \le n\}|}{4n} = \sum_{d=1}^{n} \frac{\lfloor n/d \rfloor}{n} \chi(d).$$

(d) Show (rigorously) that

$$\frac{\pi}{4} = \sum_{d=1}^{\infty} \frac{\chi(d)}{d} = \frac{1}{1} - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \dots$$

2. We call a ring R *Artinian* if every descending chain of ideals of R

$$I_1 \supseteq I_2 \supseteq I_3 \supseteq \cdots$$

stabilizes, meaning $I_n = I_{n+1}$ for all sufficiently large n. Note that this implies that every nonempty set of ideals of R contains some minimal element.

Suppose that R is Artinian.

(a) Prove that every prime ideal of R is maximal.
Hint: Reduce to the case where R is an integral domain.

(b) Show that R has finitely many prime ideals.

(c) Let $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_n$ be the prime ideals of R. Let $I = \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \dots \cap \mathfrak{p}_n$. Show that $1 - a$ is a unit for every $a \in I$.

(d) Show that $I^k = I^{k+1}$ for some positive integer k.

(e) Now suppose for contradiction that $I^k \neq 0$. Show that there is an ideal J of R such that $I^k J \neq 0$, and such that for any ideal $J' \subseteq J$, if $I^k J' \neq 0$ then $J = J'$.

(f) Show that the ideal J from part (d) satisfies $IJ = J$ and $J = (r)$ for some $r \in R$.

(g) Deduce from (f) that $r = ij$ for some $i \in I$ and $j \in J = (r)$. Apply part (c) to prove $r = 0$. Obtain a contradiction and conclude that $I^k = 0$.

(h) Show that $R \cong R/\mathfrak{p}_1^k \times \dots \times R/\mathfrak{p}_n^k$.

(i) Show that each ring $R/\mathfrak{p}_j^k$ is an Artinian ring with a unique maximal ideal $\mathfrak{m}$ satisfying $\mathfrak{m}^k = 0$.