Fall 2019, Math 620: Week 8 Problem Set
Due: Thursday, October 31st, 2019
A Hierarchy of Integral Domains

Discussion problems. The problems below should be completed in class.

(D1) *Euclidean domains.* In this problem, we introduce Euclidean domains.

(a) Let $R = \mathbb{Z}$. For each a, b below, find $q, r \in R$ so that $a = qb + r$ with $0 \le r < b$.

(i) $a = 17$, $b = 3$. (ii) $a = 15$, $b = 5$. (iii) $a = -17$, $b = 5$.

(b) Let $R = \mathbb{Q}[x]$. For each a, b below, find $q, r \in R$ so that $a = qb+r$ with $\deg(r) < \deg(b)$.

(i) $a = x^5 + 3x^4 + 4x + 1$, $b = x^2 + 2x + 3$. (ii) $a = x^3 + 3x^2 + 2x + 1$, $b = 2x^2 + x + 3$.

(c) Let $R = \mathbb{Z}_5[x]$. For each a, b below, find $q, r \in R$ so that $a = qb+r$ with $\deg(r) < \deg(b)$.

(i) $a = x^5 + 3x^4 + 4x + 1$, $b = x^2 + 2x + 3$. (ii) $a = x^3 + 3x^2 + 2x + 1$, $b = 2x^2 + x + 3$.

(d) Will the division algorithm work in $F[x]$ for any field F? Briefly justify your answer.

(e) Let $R = \mathbb{Z}[i]$. For each a, b below, find $q, r \in R$ so that $a = qb + r$ with $\|r\| < \|b\|$.

(i) $a = 1 + 21i$, $b = 2 + 3i$. (ii) $a = 10 + 15i$, $b = 4 + 6i$. (iii) $a = 2 + 23i$, $b = 1 + 2i$.

Are your remainders unique?

(f) A *Euclidean domain* is an integral domain R equipped with a *norm* $N : R\setminus\{0\} \to \mathbb{Z}_{\ge 0}$ such that for every $a, b \in R$ with $b \ne 0$, there exists $q, r \in R$ with $r = 0$ or $N(r) < N(b)$ so that $a = qb + r$. Identify the norm function of each ring above.

(g) Prove $\mathbb{Z}[i]$ is a Euclidean domain. Hint: choose q to be the closest point in $\mathbb{Z}[i]$ to a/b in the complex plane, write $r = b(a/b - q)$, and use $\|zz'\| = \|z\|\,\|z'\|$.

(h) Prove that in a Euclidean domain R with norm N, an element $a \in R$ is a unit if $N(a)$ is the smallest norm achieved by the nonzero elements of R.

(D2) *Greatest common divisors.* The goal of this problem is explore gcd() for Euclidean domains.

(a) Let $R = \mathbb{Z}$. Find $\gcd(42, 96)$ using the Euclidean algorithm.

(b) Show that the ideal $\langle 42, 96\rangle \subset \mathbb{Z}$ is principle.

(c) Let $R = \mathbb{Q}[x]$. Find $\gcd(x^6 + x^4 + x^2, x^4 + x^3 + x)$ using the Euclidean algorithm.

(d) Let $R = \mathbb{Z}_3[x]$. Find $\gcd(x^6 + x^4 + x^2, x^4 + x^3 + x)$ using the Euclidean algorithm.

(e) Show that the ideal $\langle x^6 + x^4 + x^2, x^4 + x^3 + x\rangle \subset \mathbb{Z}_3[x]$ is principle.

(f) Propose a definition for **a** (not **the**) "greatest common divisor" of $a, b \in R$ for any **integral domain** R.

(g) Prove that if R is a Euclidean domain, then the Euclidean algorithm applied to $a, b \in R$ returns a greatest common divisor of a and b. Why is it guaranteed to finish?

(h) Prove that any Euclidean domain is a PID.

Homework problems. You must submit *all* homework problems in order to receive full credit.

(H1) Fix $D \in \mathbb{Z}_{>0}$, and let $R = \mathbb{Z}[\sqrt{-D}]$. Consider the function $N : R \setminus \{0\} \to \mathbb{Z}$ given by

$$N\big(a + b\sqrt{-D}\big) = a^2 + Db^2$$

for $a, b \in \mathbb{Z}$.

(a) Prove that $N(zw) = N(z)N(w)$ for any $z, w \in R$.
(b) Prove that $z \in R$ is a unit if and only if $N(z) = 1$.
(c) Prove that if $D = -5$, then R is not a UFD.
(d) For $D = -2$, determine if R is a Euclidean domain, a PID, a UFD, or none of these.

(H2) Suppose F is a field, and fix $f(x) \in F[x]$ and $a \in F$. Prove that $f(a) = 0$ if and only if $f(x) = (x - a)g(x)$ for some $g(x) \in F[x]$.

(H3) Consider the ring

$$R = \{f(x) \in \mathbb{Q}[x] : f(n) \in \mathbb{Z} \text{ for all } n \in \mathbb{Z}\}$$

of *integer valued polynomials*.

(a) Prove that R is a ring with $\mathbb{Z}[x] \subsetneq R \subsetneq \mathbb{Q}[x]$.
(b) Prove that R is not a UFD.

(H4) Consider the ring

$$R = \{f(x) \in \mathbb{Q}[x] : f(0) \in \mathbb{Z}\}$$

of rational polynomials with integer constant term. Prove that $x \in R$ cannot be written as a product of finitely many irreducible elements of R (we say R is not *atomic*).

Challenge problems. Challenge problems are not required for submission, but bonus points will be awarded for submitting a partial attempt or a complete solution.

(C1) Prove or disprove: if $I \subset \mathbb{Z}[i]$ is any nontrivial ideal, then $\mathbb{Z}[i]/I$ has finitely many elements.