Some ring theory problems.

Problem 1. Let $d \in \mathbb{Z}$ be a integer with $\sqrt{d} \notin \mathbb{Z}$ and let $\mathbb{Z}[\sqrt{d}]$ be the ring

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}.$$

Define the ***conjugate*** of $\alpha = a + b\sqrt{d}$ as

$$\overline{\alpha} = a - b\sqrt{d}$$

and the ***norm*** of α as

$$N(\alpha) = \alpha\overline{\alpha} = a^2 - db^2.$$

(a) Show for $\alpha, \beta \in \mathbb{Z}[\sqrt{d}]$ that

$$\overline{\alpha\beta} = \overline{\alpha}\overline{\beta}$$
$$N(\alpha\beta) = N(\alpha)N(\beta).$$

(b) Show that $\alpha \in \mathbb{Z}[\sqrt{d}]$ is a unit if and only if $N(\alpha) = 1$.
(c) If $d < 0$, so that $N(a + b\sqrt{d}) = a^2 + |d|b^2$, show the only units are 1 and -1.
(d) In $\mathbb{Z}[\sqrt{-5}]$ show the elements $2, 3, 1 + \sqrt{-5}$ and $1 - \sqrt{-5}$ are all irreducible. *Hint:* In the case of 3 if $3 = \alpha\beta$, then $N(3) = 9 = N(\alpha)N(\beta)$, so if 3 is reducible there is an α with $N(\alpha) = 3$, but it is easy to check that $a^2 + 5b^2 = 3$ has no solutions.
(e) Show that $\mathbb{Z}[\sqrt{-5}]$ is not a unique factorization domain. *Hint:* $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. □

Here are some notes about Euclidean domains from a class I taught some time ago. There are very elementary, but if you need a quick review they may be useful.

1. Units and Associates in Commutative Rings

Definition 1. *Let R be a commutative ring. Then an element $a \in R$ is a **unit** or has an **inverse** b iff $ab = 1$. In this case we write $b = a^{-1}$.*

Thus when talking about elements of a commutative ring saying that a is a unit just means a has an inverse. It is also useful to give a name to elements that just differ by multiplication by a unit.

Definition 2. *Let R be a commutative ring. Then $a, b \in R$ are **associates** iff there is a unit $u \in R$ with $a = ub$.*

Note that if $a = ub$ with u a unit then u^{-1} is also a unit and thus $b = u^{-1}a$. So being associates is a symmetric relation. More generally

Proposition 3. *If R is a commutative ring and we define $a \sim b$ to mean that a and b are associates, then show this is an equivalence relation.*

1.1. Examples of Rings.

1.1.1. *The Integers.* The integers $\mathbf{Z}$ are as usual the numbers $0, \pm 1, \pm 2, \pm 3, \ldots$ with the addition and multiplication we all know and love. This is the main example you should keep in mind when thinking about rings. In $\mathbf{Z}$ the only units (that is elements with inverses) are 1 and -1. Thus the assocates of $n \in \mathbf{Z}$ are just n and $-n$.

1.1.2. *The Ring of Polynomials over a Field.* Let $\mathbf{F}$ be a field and let $\mathbf{F}[x]$ be the set of all polynomials

$$p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

where $a_0, \ldots, a_n \in \mathbf{F}$ and $n = 0, 1, 2 \ldots$. These are added, subtracted, and multiplied in the usual manner. This is the example that will be very important to us, so let's review a little about polynomials. First if $p(x)$ is not the zero polynomial and $p(x)$ is as above with $a_n \neq 0$ then n is the ***degree*** of $p(x)$ and this will be denoted by $n = \deg p(x)$. The the nonzero constant polynomials a have degree 0 and we do not assign any degree to the zero polynomial. If $p(x)$ and $q(x)$ are nonzero polynomials then we have

$$\deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x)).$$

Also if given $p(x)$ and $f(x)$ with $p(x)$ not the zero polynomial we can "divide"[1] $p(x)$ into $f(x)$. That is there are unique polynomials $q(x)$ (the ***the quotient***) and $r(x)$ (the ***the reminder***) so that

$f(x) = q(x)p(x)+r(x)$ where $\deg r(x) < \deg p(x)$ or $r(x)$ is the zero polynomial.

This is called the division algorithm. If $p(x) = x - a$ for some $a \in \mathbf{F}$ then this becomes

$$f(x) = q(x)(x - a) + r \quad \text{where } r \in \mathbf{F}.$$

By letting $x = a$ in this equation we get the fundamental

Proposition 4 (Remainder Theorem)**.** *If $x - a$ is divided into $f(x)$ then the remainder is $r = f(a)$. If particular $f(a) = 0$ if and only if $x - a$ divides $f(x)$. That is $f(a) = 0$ iff $f(x) = (x - a)q(x)$ for some polynomial $q(x)$ with* $\deg q(x) = \deg f(x) - 1$.

I am assuming that you know how to add, subtract and multiply polynomials, and that given $f(x)$ and $p(x)$ with $p(x)$ not the zero polynomial that you can divide $p(x)$ into $f(x)$ and find the quotient $q(x)$ and remainder $r(x)$.

Problem 2. Show that the units in $R := \mathbf{F}[x]$ are the nonzero constant polynomials and that the associates of $f(x)$ are $cf(x)$ where c is a nonzero elment of $\mathbf{F}$.

---

[1]Here we are using the word "divide" in a sense other than "multiplying by the inverse". Rather we mean "find the quotient and remainder". I will continue to use the word "divide" in both these senses and trust it is clear from the context which meaning is being used.

1.2. **Ideals in Rings.**

Definition 5. *Let R be a commutative ring. Then a nonempty subset $A \subset R$ is an **ideal** if and only if it is closed under addition and multiplication by elements of R. That is*

$$a, b \in A \quad \textit{implies} \quad a + b \in A$$

(this is closure under addition) and

$$a \in A,\ r \in R \quad \textit{implies} \quad ar \in A$$

(this is closure under multiplication by elements of R).

There are two trivial examples of ideals in any R. The set $A = \{0\}$ is an ideal as is $A := R$. Let R be a commutative ring and let $a \in R$. Let (a) be the set of all multiples of a by elements of R. That is

$$(a) := \{ra : r \in R\}.$$

Then $A := (a)$ is an ideal in R.

Definition 6. *If R is a commutative ring and $a \in R$, then (a) as defined in the last exercise is the **principle ideal** defined generated by a.*

2. Euclidean Domains

2.1. **The Definition of Euclidean Domain.** Two important examples of rings are the integers and the polynomials over a field. We now make a definition that captures many of the basic properties these two examples have in common.

Definition 7. *A commutative ring R is an **Euclidean domain** iff*

1. *R has no zero divisors[2]. That is if $a \neq 0$ and $b \neq 0$ then $ab \neq 0$. (Or in the contrapositive form $ab = 0$ implies $a = 0$ or $b = 0$.)*
2. *Then is a function $\delta : (R \setminus \{0\}) \to \{0, 1, 2, 3, \ldots\}$ (that is δ maps nonzero elements of R to nonnegative integers) so that*
   (a) *If $a, b \in R$ are both nonzero then $\delta(a) \leq \delta(ab)$.*
   (b) *The **division algorithm** holds in the sense that if $a, b \in R$ and $a \neq 0$ then we can divide a into b to get a **quotient** q and a **reminder** r so that*

$$b = aq + r \quad \textit{where } \delta(r) < \delta(a) \textit{ or } r = 0$$

[2]In general a commutative ring R with no zero divisors is called an *integral domain* or just a *domain*.

2.2. **The Basic Examples of Euclidean Domains.** Our two basic examples of Euclidean domains are the integers $\mathbf{Z}$ with $\delta(a) = |a|$, the absolute value of a and $\mathbf{F}[x]$, the ring of polynomials over a field $\mathbf{F}$ with $\delta(p(x)) = \deg p(x)$. We record this as theorems:

Theorem 8. *The integers $\mathbf{Z}$ with $\delta(a) := |a|$ is a Euclidean domain.*

Theorem 9. *The ring of polynomials $\mathbf{F}[x]$ over a field $\mathbf{F}$ with $\delta(p(x)) = \deg p(x)$ is a Euclidean domain.*

PROOFS: These follow form the usual division algorithms in $\mathbf{Z}$ and $\mathbf{F}[x]$. □

2.3. **Primes and Factorization in Euclidean Domains.** We now start to develop the basics of "number theory" in Euclidean domains. By this is meant that we will show that it is possible to define define things like "primes" and greatest "common divisors" and show that they behave just as in the case of the integers. Many of the basic facts about Euclidean domains are proven by starting with subset S of the Euclidean domain in question and then choosing an element a in S that minimizes $\delta(a)$. While it is more or less obvious that it is always possible to do this we record (without proof) the result that makes it all work.

Theorem 10 (Axiom of Induction)**.** *Let $\mathbf{N} := \{0, 1, 2, 3, \ldots\}$ be the natural numbers (which is the same thing as the nonnegative integers). Then any nonempty subset S of $\mathbf{N}$ has a smallest element.*

We start with some elementary definitions:

Definition 11. *Let R be a commutative ring. Let $a, b \in R$.*

1. *Then a is a **divisor** of b, (or a **divides** b, or a is a **factor** of b) iff there is $c \in R$ so that $b = ca$. This is written as $a \mid b$.*
2. *b is a **multiple** of a iff a divides b. That is iff there is $c \in R$ so that $b = ac$.*
3. *The element $b \neq 0$ is an **irreducible** iff b is not a unit and if $a \mid b$ then either a is a unit, or $a = ub$ for some unit $u \in R$.*
4. *The element $p \neq 0$ is a **prime** iff p is not a unit and $p \mid ab$ implies that $p \mid a$ or $p \mid b$. (That is p is a prime if it is not a unit and if p divides a product, then it divides one of the factors.)*
5. *The element c of R is a **greatest common divisor** of a and b iff $c \mid a$, $c \mid b$ and if $d \in R$ is any other element of R that divides both a and b then $d \mid c$. (Note that greatest common divisors are not unique. For example in the integers $\mathbf{Z}$ there both 4 and -4 are greatest common divisors of 12 and 20, while in the polynomial ring $\mathbf{R}[x]$ if element the $c(x-1)$ is a greatest common divisor of $x^2 - 1$ and $x^2 - 3x + 2$ for any $c \neq 0$.)*
6. *The elements a and b are **relatively prime** iff 1 is a greatest common divisor of a and b. Or what is the same thing the only elements that divide both a and b are units.*

There are commutative rings where some pairs of elements do not have any greatest common divisors. We now show that this is not the case in Euclidean domains.

Theorem 12. *Let R be a Euclidean domain. Then every ideal in R is principle. That is if I is an ideal in R then there is an $a \in R$ so that $I = (a)$. Moreover if $\{0\} \neq I = (a) = (b)$ then $a = ub$ for some unit u.*

Problem 3. Prove this along the following lines:

(1) By the Axiom of induction, Theorem 10, the set $S := \{\delta(r) : r \in I, r \neq 0\}$ has a smallest element. Let a be a nonempty element of I that minimizes $\delta(r)$ over nonzero elements of I. Then for any $b \in I$ show that there is a $q \in R$ with $b = aq$ by showing that if $b = aq + r$ with $r = 0$ or $\delta(r) < \delta(a)$ (such q and r exist by the definition of Euclidean domain) than in fact $r = 0$ so that $b = qa$.
(2) With a as in the last step show $I = (a)$, and thus conclude I is principle.
(3) If $(a) = (b)$ then $a \in (b)$ so there is a c_1 so that $a = c_1 b$. Likewise $b \in (a)$ implies there is a $c_2 \in R$ so that $b = c_2 a$. Putting these together implies $a = c_1 c_2 a$. Show this implies $c_1 c_2 = 1$ so that c_1 and c_2 are units. HINT: Use that $a(1 - c_1 c_2) = 0$ and that in a Euclidean domain there are no zero divisors. □

Theorem 13. *Let R be a Euclidean domain and let a and b be nonzero elements of R. Then a and b have at least one greatest common divisor. More over if c and d are both greatest common divisors of a and b then $d = cu$ for some unit $u \in R$. Finally if c is any greatest common divisor of a and b then there are elements $x, y \in R$ so that*

$$c = ax + by.$$

Problem 4. Prove this as follows:

(1) Let $I := \{ax + by : x, y \in R\}$. Then I is an ideal of R (we have shown this before, so you don't have to do it again).
(2) Because I is an ideal by the last theorem the ideal I is principle so $I = (c)$ for some $c \in R$. Show that c is a greatest common divisor of a and b and that $c = ax + by$ for some $x, y \in R$. HINT: That $c = ax + by$ for some $x, y \in R$ follows from the definition of I. From this show c is a greatest common divisor of a and b.
(3) If c and d are both greatest common divisors of a and b then by definition $c \mid d$ and $d \mid c$. Use this to show $d = uc$ for some unit u. □

Theorem 14. *Let R be a Euclidean domain and let $a, b \in R$ be relatively prime. Then there exist $x, y \in R$ so that*

$$ax + by = 1.$$

Problem 5. Prove this as a corollary of the last theorem. □

Theorem 15. *Let R be a Euclidean domain. Then $p \in R$ is prime if and only if p is irreducible.*

Problem 6. Prove this by showing that if p does not divide a then it must divide b. Do this by showing the following:

(1) Show that if p is prime it is irreducible by noting that if $p = ab$, than as p is prime $p \mid a$ or $p \mid b$. If $p \mid a$, then $a = cp$ for some $c \in R$. But then $p = ab = pcb$ which implies $bc = 1$ and thus b is unit and a is associate of p. Likewise if $p \mid b$, then a is a unit and b is a associate of p.

    So we now assume that p is an irreducible and show that this implies it is prime. That is we need to show that if $p \mid ab$, then $p \mid a$ or $p \mid b$. We do this by assuming that $p \mid ab$, but that p is not a factor of a and then showing that p is a factor of b.

(2) As p is irreducible and we are assuming p does not divide a then a and p are relatively prime.

(3) There are x and y in R so that $ax + py = 1$.

(4) As $p \mid ab$ there is a $c \in R$ with $ab = cp$. Now multiply both sides of $ax + py = 1$ by b to get $abx + pby = b$ and use $ab = cp$ to conclude p divides b. □

Corollary 16. *If p is a prime in the Euclidean domain R and p divides a product $a_1 a_2 \cdots a_n$ then p divides at least one of a_1, a_2, ..., a_n.*

Proof. This follows from the last proposition by a straightforward induction. □

Lemma 17. *Let R be a Euclidean domain. Then a nonzero element a of R is a unit iff $\delta(a) = \delta(1)$.*

Problem 7. Prove this. HINT: First note that if $0 \neq r \in R$ then $\delta(1) \leq \delta(1r) = \delta(r)$. Now use the division algorithm to write $1 = aq + r$ where either $\delta(r) < \delta(a) = \delta(1)$ or $r = 0$. □

Proposition 18. *Let R be a Euclidean domain and a and b nonzero elements of R. If $\delta(ab) = \delta(a)$ then b is a unit.*

Problem 8. Prove this. HINT: Use the division algorithm to divide ab into a. That is there are q and $r \in R$ so that $a = (ab)q + r$ so that either $r = 0$ or $\delta(r) < \delta(a)$. Then write $r = a(1 - bq)$ and use that if x and y are nonzero $\delta(x) \leq \delta(xy)$ to show $(1 - bq) = 0$. From this show b is a unit.) □

Theorem 19 (Fundamental Theorem of Arithmetic)**.** *Let a be a non-zero element of a Euclidean domain that is not a unit. Then a is a product $a = p_1 p_2 \cdots p_n$ of primes $p_1, p_2, \ldots, p_n$. Moreover we have the following uniqueness. If $a = q_1 q_2 \cdots q_m$ is anther expression of a as a product of primes, then $m = n$ and after a reordering of $q_1, q_2, \ldots, q_n$ there are units $u_1, u_2, \ldots, u_n$ so that $q_i = u_i p_i$ for $i = 1, \ldots, n$.*

Problem 9. Prove this by induction on $\delta(a)$ in the following steps.

(1) As a is not a unit the last lemma implies $\delta(a) > \delta(1)$. Let $k : \min\{\delta(r) : r \in R, \delta(r) > \delta(1)\}$. Show that if $\delta(a) = k$ than a is a prime. (This is the base of the induction.)
(2) Assume that $\delta(a) = n$ and that it has been shown that for any $b \neq 0$ with $\delta(b) < n$ that either b is a unit or b is a product of primes. Then show that a is a product of primes. HINT: If a is prime then we are done. Thus it can be assumed that a is not prime. In this case $a = bc$ where b and c are not units. a is a product $a = bc$ with both b and c not units. By the last proposition this implies $\delta(b) < \delta(a)$ and $\delta(c) < \delta(a)$. So by the induction hypothesis both b and c are products of primes. This shows $a = bc$ is a product of primes.
(3) Now show uniqueness in the sense of the statement of the theorem. Assume $a = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$ where all the p_i's and q_j's are prime. Then as p_1 divides the product $q_1 q_2 \cdots q_m$ by Corollary 16 this means that p_1 divides at least one of $q_1, q_2, \ldots, q_m$. By reordering we can assume that p_1 divides q_1. As both p_1 and q_1 are primes this implies $q_1 = u_1 p_1$ for some unit u_1. Continue in this fashion to complete the proof. □