

4400/6400 PROBLEM SET 1

Key: (E) denotes easy. If you honestly feel the problem is *too* easy, just write “okay”, but try to solve some harder problems as well.

1.1)(E) Prove the Division Theorem: If $a \geq b > 0$ are integers, then there exist unique non-negative integers q and r such that $a = qb + r$ and $0 \leq r < b$. Hint: It suffices to take q to be the largest non-negative integer such that $a - qb \geq 0$.

1.2)(E) In the notation of Problem 1.1), show that $b|a \iff r = 0$.

1.3) Prove the converse of Euclid’s Lemma: suppose d is a positive integer such that whenever $d|ab$, $d|a$ or $d|b$. Then d is prime.

Remark: Among other things, this allows us to generalize the notion of primes to not-necessarily principal ideals.

1.4)a)(E) “To contain is to divide”: for integers a and b , we have $a|b \iff (a) \supset (b)$.

b) Confirm that part a) holds true for elements a and b in any commutative ring.

c) For elements a, b in an integral domain R , show that the following are equivalent:

(i) There exists a unit $u \in R^\times$ such that $b = ua$.

(ii) There exist units $u, v \in R^\times$ such that $b = ua, a = vb$.

(iii) $a | b$ and $b | a$.

(iv) There is an equality of principal ideals $(a) = (b)$.

d)* Find a commutative ring R (not an integral domain) and elements a and b such that in part c) above, (iii) and (iv) hold but (i) and (ii) do not. In other words, in a general commutative ring, being associates is a stronger relation than generating the same principal ideal.¹

1.5) Prove or disprove: The $\gcd(0, 0)$ does not exist. In other words, when $a = b = 0$, there is no integer d such that for all integers e , if $e | a$ & $e | b$, then $e | d$.

The next exercise concerns the ring $\mathbb{E} = 2\mathbb{Z}$ of all even integers.

1.6) Give a necessary and sufficient condition on a positive element $x \in \mathbb{E}$ to have two different factorizations into positive \mathbb{E} -primes. Hint: pay attention to $\text{ord}_2(x)$ and also to the number of odd primes dividing x .

1.7) Prove Proposition 12 in <http://math.uga.edu/~pete/4400intro.pdf>, about the basic properties of the ord_p functions.

1.8) Complete the proof that $S_n = 1 + \frac{1}{2} + \dots + \frac{1}{n}$ is never an integer by showing

Thanks to Kelly Edenfield, Erik Jacobson and Laura Nunley for pointing out typos.

¹Ted Shifrin told me about this, so you could ask him...

that for all $n \geq 1$, $\text{ord}_2(S_n) \neq \text{ord}_2(\frac{1}{n+1})$.

1.9)** Show that except for $n = 1, 2, 6$, the decimal expansion of S_n is non-terminating. (I.e., show that except for these values, $\text{ord}_p(S_n) < 0$ for some prime $p \neq 2, 5$.)²

1.10) For any nonzero integers a and b , show that

$$\gcd(a, b) \cdot \text{lcm}(a, b) = ab.$$

1.11) For integers a and b , show that the intersection of the two ideals $(a) \cap (b)$ is an ideal of \mathbb{Z} . In fact, if you know the definition of an ideal in a commutative ring, show that the intersection of any two (or more...) ideals is always an ideal.³ Because \mathbb{Z} is a PID, we must have $(a) \cap (b) = (c)$ for some $c \in \mathbb{Z}$, well-determined up to a sign. What is c in terms of a and b ?

1.11.5) a) Let a_1, \dots, a_n be a (finite) set of integers. Define the *greatest common divisor* $\gcd(a_1, \dots, a_n)$ of the set, and show that it exists and is unique up to a sign. In fact, show that the set

$$(a_1, \dots, a_n) = \{x_1 a_1 + \dots + x_n a_n \mid x_i \in \mathbb{Z}\}$$

is an ideal of \mathbb{Z} , and that the positive generator of this (necessarily principal!) ideal is the gcd we are looking for.

b) Define $\text{lcm}(a_1, \dots, a_n)$, show it exists, and explain how to get it from the ideals $(a_1), \dots, (a_n)$.

1.12) Show that $\gcd(a_1, a_2, a_3) = \gcd(\gcd(a_1, a_2), a_3)$.

2.13)* Find an identity relating $\gcd(a_1, a_2, a_3)$, $\text{lcm}(a_1, a_2, a_3)$ and $a_1 a_2 a_3$. Can you extend this to more than three numbers? (Hint: inclusion/exclusion.)

1.14) One says that a set of integers a_1, \dots, a_n is **relatively prime in pairs** if for all $i \neq j$, $\gcd(a_i, a_j) = 1$.

a) Show that if a_1, \dots, a_n are relatively prime in pairs, then $\gcd(a_1, \dots, a_n) = 1$.

b) Show that the converse does not hold when $n \geq 3$: indeed, find the smallest example of three integers which are not simultaneously divisible by any $d > 1$ but for which any two have a nontrivial common divisor.⁴

Remark: The phrase “let a_1, \dots, a_n be relatively prime integers” is therefore ambiguous when $n \geq 3$. Probably it ought to mean the weaker condition that $\gcd(a_1, \dots, a_n) = 1$ but careful authors rephrase to avoid the ambiguity. If you hear someone say it, stop and ask them which one they mean!

²Note the double-star: this is quite difficult.

³It is a metatheorem of algebra that if H_1 and H_2 are some substructures of a structure G , then $H_1 \cap H_2$ is also a substructure. Unions do not work nearly as nicely.

⁴This is reminiscent of the fact that a set of vectors can be linearly dependent even when any two of them are linearly independent from each other, a fact that gives linear algebra students no end of trouble.

1.15) Prove the rational roots theorem: if

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

is a polynomial with integer coefficients, the only possible rational roots are of the form $\pm \frac{c}{d}$ where $c \mid a_0$ and $d \mid a_n$. Explain how this gives yet another proof of, e.g., the irrationality of $\sqrt{2}$.

1.16) a) Show that $\log_2 10$ is irrational.

b)* Let $a, b \in \mathbb{Z}^+$. Give a criterion for the irrationality of $\log_a b$.

G1.1) Let F be a field and let $v : F^\times \rightarrow \mathbb{Z}$ be a surjective map satisfying properties a) and b) of Proposition 12; v is said to be a **discrete valuation** of F .

a) Let $R_v := \{x \in F^\times \mid v(x) \geq 0\} \cup \{0\}$. Show that R_v is a subring of F , the **valuation ring**. (It is common to formally set $v(0) = \infty$ to avoid having to keep “manually inserting 0.”)

b) Since v is surjective, there is an element $\pi \in R_v$ with $v(\pi) = 1$.⁵ Show that for any $n \geq 1$,

$$\{x \in F^\times \mid v(x) \geq n\} \cup \{0\} = (\pi^n),$$

the principal ideal of R_v generated by π^n (of course $\pi^0 = 1$).

c) Show that every ideal of R_v is of the form (π^n) for a suitable $n \in \mathbb{N}$. In particular, every ideal of R_v is principal, and there is a unique maximal ideal, (π) .

d) When $F = \mathbb{Q}$, $v = \text{ord}_p$, what is the valuation ring R_v ?

e) Suppose k is a field, and consider $F = k(t)$, the quotient field of the ring of polynomials $k[t]$ with coefficients in k . Show that the map v which takes a rational function $\frac{p(x)}{q(x)}$ to $\deg(q(x)) - \deg(p(x))$ is a discrete valuation of $k(t)$. Note that this is consistent with our previous convention that the degree of the zero polynomial is $-\infty$!

⁵Denoting this element by π is traditional. Needless to say (?) it has nothing to do with 3.1415926535897...