

Math 110BH homework 3

Nathan Solomon

January 30, 2024

1

Prove that the operations in the ring of fractions are well defined.

In $\text{Frac}(R)$, we define multiplication by the formula

$$\frac{a_1}{b_1} \cdot \frac{a_2}{b_2} = \frac{a_1 a_2}{b_1 b_2}$$

and define addition by the formula

$$\frac{a_1}{a_2} + \frac{a_2}{b_2} = \frac{a_1 b_2 + a_2 b_1}{b_1 b_2}.$$

If we had instead chosen a different element $\frac{a'_1}{b'_1}$ from the same equivalence class as $\frac{a_1}{b_1}$ (meaning that $a_1 b'_1 = a'_1 b_1$) and similarly, chose $\frac{a'_2}{b'_2}$ instead of $\frac{a_2}{b_2}$, then we would get

$$\frac{a'_1}{b'_1} \cdot \frac{a'_2}{b'_2} = \frac{a'_1 a'_2}{b'_1 b'_2}.$$

But because $(a_1 b'_1)(a_2 b'_2) = (a'_1 b_1)(a'_2 b_2)$, that's in the same equivalence class as

$$\frac{a_1 a_2}{b_1 b_2}.$$

Doing the same thing for addition, we get

$$\frac{a'_1}{a'_2} + \frac{a'_2}{b'_2} = \frac{a'_1 b'_2 + a'_2 b'_1}{b'_1 b'_2}.$$

Once again, we use the equivalence relation that $a_1 a_2 b'_1 b'_2 = a'_1 a'_2 b_1 b_2$, so the sum simplifies to

$$\frac{a_1 b_2 + a_2 b_1}{b_1 b_2}.$$

Therefore addition and multiplication in $\text{Frac}(R)$ are both well-defined. If you really want to be thorough about this, you could repeat a super similar process twice more to show that subtraction and division (or equivalently, negation and multiplicative inversion) are also well defined.

2

Let R be the ring of all continuous functions on \mathbb{R} . Let I be the subset of all functions in R such that $f(0) = f(1) = 0$. Prove that I is an ideal in R . Is I a prime ideal?

- **I is closed under addition.** Let f, g be any two elements in I . Then $(f + g)(0) = f(0) + g(0) = 0 + 0 = 0$ and by the same logic, $(f + g)(1) = 0$, so $f + g$ is in I .
- **I is closed under left and right multiplication.** Let f be any element of I and h be any element of R . Then $(f \cdot h)(0) = f(0)h(0) = 0 \cdot h(0) = 0$ and similarly, $(f \cdot h)(1) = 0$. R is a commutative ring, so order does not matter – $f \cdot h$ and $h \cdot f$ are both in I .
- **I is not empty.** The zero function is in I .

Therefore I is an ideal of R , but it is not a prime ideal. For example, neither of the functions defined by $f(x) = x$ or by $g(x) = 1 - x$ are in I , but their product, the function which maps x to $x - x^2$, is in I .

3

Let R be a commutative ring, let I and J be ideals in R and P a prime ideal containing $I \cap J$. Prove that either I or J is contained in P .

Suppose neither I nor J is contained in P . Then there exists an element $i \in I$ and an element $j \in J$ such that $i \notin P$ and $j \notin P$. Since I and J are ideals, they must both contain the product ij . However, that means $ij \in I \cap J \subset P$. But since P is prime, $ij \in P$ implies either $i \in P$ or $j \in P$. This is a contradiction, so either I or J is contained in P .

4

Let R be a finite commutative ring. Prove that every prime ideal in R is maximal.

Let P be a prime ideal of R . This is equivalent to saying R/P is an integral domain, and since R is finite, R/P must also be finite. In homework 1, problem 6, we showed that every finite integral domain is a field, so R/P is a field, which means P is maximal.

A commutative ring R is called *local* if it has a unique maximal ideal M .

- (a) Prove that $R^\times = R \setminus M$.
- (b) Show that R has no nontrivial idempotents.
- (c) Prove that the set of all fractions $\frac{n}{m}$, $n, m \in \mathbb{Z}$, m is odd, is a local subring of \mathbb{Q} .
- (d) Determine all n such that the ring $\mathbb{Z}/n\mathbb{Z}$ is local.

- (a) Let u be any element of R^\times . Then u cannot be in M , because if it were, for any element $x \in R$, $(xu^{-1})u = x$ would have to also be in M , which would imply $R = M$ (and that's a contradiction, since we stated M is maximal).

Let u be any invertible element of R and let a be any noninvertible element of R . Then au is not invertible, because if it were, then $(au)^{-1}ua$ would be equal to one, which would imply $(au)^{-1}u$ is an inverse of a . However, since a is not invertible, we know au also is not invertible, so $R \setminus R^\times$ is an ideal.

Since M is the unique maximal ideal of R , it must contain $R \setminus R^\times$. In fact, M cannot contain any additional elements, because we already proved that no invertible element of R can be contained in M . Therefore $M = R \setminus R^\times$, so $R^\times = R \setminus M$.

- (b) Suppose e is a nontrivial idempotent of R . Then $e(1 - e) = 0$, so e and $1 - e$ are zero divisors. That means they are not invertible, so they must both be in $M = R \setminus R^\times$. Since M is closed under subtraction, $(1 - e) - e$ is in M , therefore every element of R is in M . This is a contradiction, so R cannot contain any nontrivial idempotents.
- (c) First, this is indeed a subring, because the multiplicative identity is $\frac{1}{1}$ in both \mathbb{Q} and in this new set, and because for any two fractions in that set, their sum and product (when fully simplified) will also both have odd denominators.

Let M be the subset of those fractions for which, when fully simplified, n is even and m is odd. We can easily show this is an ideal, and that it contains all of the elements which are not invertible (in the set of fractions with odd denominators). Therefore M is the only maximal ideal.

- (d) If n has multiple distinct prime factors p_1 and p_2 , then $p_1(\mathbb{Z}/n\mathbb{Z})$ and $p_2(\mathbb{Z}/n\mathbb{Z})$ are both maximal ideals (according to the result from homework 2, problem 7). If n is a power of some prime p , then using the same reasoning $p(\mathbb{Z}/n\mathbb{Z})$ is the only maximal ideal. Therefore $\mathbb{Z}/n\mathbb{Z}$ is local if and only if n is a prime power.

6

Let $R = \mathbb{Z}[i]$ be the ring of Gauss integers. Find a generator of the intersection of the two principal ideals $2R$ and $(3+i)R$.

Every Gauss integer can be written as $a + bi$, where a and b are integers. That implies every element of $2R$ can be written as $2a + 2bi$ and every element of $(3+i)R$ can be written as $(3c-d) + (c+3d)i$ (where $a, b, c, d \in \mathbb{Z}$). The latter is of the form $2a + 2bi$ if and only if c and d have the same parity. The set of pairs of integers (c, d) which have the same parity is the set of integer linear combinations of $(1, 1)$ and $(1, -1)$ (in other words, the set of pairs (c, d) which we are interested in are “spanned” by $91, 1$ and $(1, -1)$). Plugging that in for (c, d) , we see that the set of Gauss integers which are in both $2R$ and $(3+i)R$ is spanned by $4 - 2i$ and $2 + 4i$. That subset of $\mathbb{Z}[i]$ is generated by $2 + 4i$.

7

Determine the group $\mathbb{Z}[i]^\times$.

For any two complex numbers, the magnitude of their product is the product of their magnitudes. If z is an invertible element in \mathbb{C} , that implies either z or z^{-1} has magnitude less than or equal to one. There are no nonzero Gauss integers with magnitude less than one, so any unit in $\mathbb{Z}[i]$ must have magnitude one. There are only four such elements, so we can individually check that they are invertible in $\mathbb{Z}[i]$. They all are, so

$$\mathbb{Z}[i]^\times = \{1, i, -1, -i\}.$$

8

Prove that the polynomial ring $\mathbb{Z}[x]$ is not a PID

Let I be the subset of $\mathbb{Z}[x]$ for which the constant term is even. Adding two such polynomials gives another polynomial whose constant term is even, and multiplying any such polynomial by any other polynomial with integer coefficients gives a polynomial whose constant term is even. Therefore I is an ideal of $\mathbb{Z}[x]$.

Suppose I is a principal ideal, meaning there exists some polynomial p such that $I = p\mathbb{Z}[x]$. I does not contain 1, so p is not 1, but I does contain 2. 2 is an irreducible element in $\mathbb{Z}[x]$, so p must be 2. That implies every coefficient of every polynomial in $p\mathbb{Z}[x]$ is even, but I contains polynomials such as $x + 2$, so $I \neq p\mathbb{Z}[x]$. Since we have reached a contradiction, $\mathbb{Z}[x]$ is not a PID.

9

Prove that the ring $\mathbb{Z}[\sqrt{2}]$ is Euclidean.

Any element of $\mathbb{Z}[\sqrt{2}]$ can be written as $x + y\sqrt{2}$, where x and y are integers.

Let $\varphi : \mathbb{Z}[\sqrt{2}] \setminus \{0\} \rightarrow \mathbb{Z}^{\geq 0}$ be the function which takes $x + y\sqrt{2}$ to $|x^2 - 2y^2|$.

For any elements $a + b\sqrt{2}$ and $c + d\sqrt{2}$ in $\mathbb{Z}[\sqrt{2}]$, the exact value of $(a + b\sqrt{2})/(c + d\sqrt{2})$ is

$$\frac{a + b\sqrt{2}}{c + d\sqrt{2}} = \frac{(a + b\sqrt{2})(c - d\sqrt{2})}{c^2 - 2d^2} = \frac{ac - 2db}{c^2 - 2d^2} + \frac{bc - ad}{c^2 - 2d^2}\sqrt{2}.$$

Now let

$$q = \text{Round}\left(\frac{ac - 2db}{c^2 - 2d^2}\right) + \text{Round}\left(\frac{bc - ad}{c^2 - 2d^2}\right)\sqrt{2}.$$

If rounding didn't make a difference, then $a + b\sqrt{2} = q(c + d\sqrt{2})$, so we're done. Otherwise, let $r = (a + b\sqrt{2}) - q(c + d\sqrt{2})$. The last thing we need to show is that $\varphi(r) < \varphi(c + d\sqrt{2})$. By looking at how much q changed from the exact quotient when rounding, we see that

$$\frac{r}{c + d\sqrt{2}} = \left(\text{a fraction with magnitude} \leq \frac{1}{2}\right) + \left(\text{some other number with magnitude} \leq \frac{1}{2}\right) \cdot \sqrt{2}.$$

Multiplying both sides of that equation by $c + d\sqrt{2}$ shows that

$$r = cx + 2dy + (cy + dx)\sqrt{2}$$

for some x, y satisfying $|x| \leq \frac{1}{2}, |y| \leq \frac{1}{2}$ (and such that $|x|, |y|$ cannot both be $\frac{1}{2}$). Applying φ to both sides, we see that $\varphi(r) < |c^2 - 2d^2| = \varphi(c + d\sqrt{2})$.

10

Let R be a domain. Prove that R is a UFD if and only if every nonzero nonunit in R is a product of prime elements.

If R is a UFD, then any element $x \in R$ can be expressed as a product

$$x = up_1p_2 \dots p_n$$

where u is a unit and every p_i is irreducible. Of course, we can multiply p_1 by u , so we no longer have u in that expression. Since R is a UFD, every irreducible element is prime, so every element $x \in R$ is a product of prime elements.

If every nonzero nonunit in R is a product of prime elements, then since R is a domain, all of those primes are irreducible.