

**MATH 123: ABSTRACT ALGEBRA II**  
**SOLUTION SET # 3**

GREGG MUSIKER

1. CHAPTER 11, SECTION 6

**Problem 8**

a) Let  $S = \mathbb{Z}[\alpha]$ , where  $\alpha$  is a complex root of a monic polynomial of degree 2. Prove that  $S$  is a lattice in the complex plane.

Let  $f(x) = x^2 + bx + c \in \mathbb{C}[X]$  have  $\alpha$  as a root. By Prop. 10.5.7  $\{1, \alpha\}$  or  $\{1\}$  is a basis for  $S$ . This is because  $\alpha^2 = -b \cdot \alpha - c$  hence further powers of  $\alpha$  can be rewritten in terms of  $\alpha$ . (Many people got points off for missing this step.) Thus  $S = \{1 \cdot \mathbb{Z} + \alpha \cdot \mathbb{Z}\}$ , and is a lattice by definition.

b) Prove the converse, a subring  $S$  of  $\mathbb{C}$  which is a lattice has the form given in (a).

Since  $S$  is a subring of  $\mathbb{C}$ ,  $1 \in S$ . Since  $S$  is a lattice, suppose  $S = \alpha \cdot \mathbb{Z} + \beta \cdot \mathbb{Z}$  where  $\alpha, \beta \in \mathbb{C}$ . Let  $m\alpha + n\beta = 1$ . Then  $zm\alpha + zn\beta = z \in S$  for any integer  $z$ , thus  $\mathbb{Z} \subset S$ . Furthermore,  $\beta$  can be rewritten as  $\frac{1}{n} - \frac{m}{n}\alpha$ . Assuming  $n > 1$ ,  $\beta^k \in S$  for any  $k$ , and consequently,  $\frac{1+\gamma}{n^k} \in S$  where  $\gamma \in \mathbb{Z}[\alpha]$ . However, this means that  $S$  is not discrete even though  $S$  is a lattice.  $\Rightarrow \Leftarrow$

Another way of saying this is that  $1 \in S$  is a basis element of the lattice for the following reason: if 1 were not of minimal norm, there would exist  $\gamma$  s.t.  $|\gamma| < 1$  but then taking powers of  $\gamma$ , one gets arbitrarily small elements, which again contradicts the fact that  $S$  is discrete.

Many people got points off because they asserted that 1 is a basis element without proving it.

Thus  $m\alpha + \beta = 1$ , and  $\beta$  can be rewritten in terms of the basis  $\{1, \alpha\}$ .  $S$  is a lattice so it can only have two basis elements. Lastly,  $\alpha^2 \in S$  which implies there is a way to write  $\alpha^2 = (-b)\alpha + (-c)$  for integers  $b$  and  $c$ . Thus  $f(\alpha) = 0$ .

2. CHAPTER 11, SECTION 7

**Problem 7.d** Use the method of Prop (7.9) to describe the ideals in  $\mathbb{Z}[\sqrt{-7}]$ .

Like the proof of Theorem 11.7.9, let  $A$  be a nonzero ideal of  $R$  and let  $\alpha \in A$  be a nonzero element of  $A$  of minimal absolute value  $d$ . The principal ideal  $(\alpha) = R\alpha$  contains complex numbers of the form  $(a + b\sqrt{-7}) \cdot \alpha$  where  $a, b \in \mathbb{Z}$ . Thus it has the lattice basis  $(\alpha, \alpha\sqrt{-7})$ .  $A$  contains  $(\alpha)$  thus  $A = (\alpha)$ .

Let  $A$  be an ideal that contains more than  $(\alpha)$ , e.g.  $\beta \in A$  but  $\beta \notin (\alpha)$ . Using the same trick as Artin, we create a rectangle with vertices  $0, \alpha, \alpha\sqrt{-7}$ , and  $\alpha + \alpha\sqrt{-7}$ . Letting  $n = 2$ , we draw disks of radius  $\frac{r}{2}$  around the points  $\frac{\alpha\sqrt{-7}}{2}, \frac{\alpha + \alpha\sqrt{-7}}{2}$ , and  $\alpha + \frac{\alpha\sqrt{-7}}{2}$  and also draw disks of radius  $r$  around the four vertices of the rectangle.

These disks will cover the entire rectangle.  $\beta$  must be in the rectangle by Lemma 5.4.14. By Lemma 11.7.11,  $\beta$  must be one of the points at the center of these disks and  $\beta$  is not in  $(\alpha)$ , hence  $\beta$  is one of the three points in the center.

Assume  $\frac{\alpha\sqrt{-7}}{2} \in A$ . Multiplying by  $\sqrt{-7}$ ,  $\frac{-7\alpha}{2} \in A$  hence  $\frac{\alpha}{2} \in A$ . But  $\alpha$  was chosen to be the element of minimum absolute value.  $\Rightarrow\Leftarrow$

$\alpha + \frac{\alpha\sqrt{-7}}{2} \in A$  also implies  $\frac{\alpha}{2} \in A$  which leaves us with the fact  $\beta = \frac{\alpha + \alpha\sqrt{-7}}{2} \in A$ . Consequently,  $A = (\alpha, \beta) = (\alpha, \frac{\alpha\sqrt{-7}}{2})$ .

**Problem 7.f** Use the method of Prop (7.9) to describe the ideals in  $\mathbb{Z}[\sqrt{-10}]$ .

This proof follows the same logic as 7.d except one use the three original circles and needs to add eight circles of radius  $r/3$  around points with coordinates in  $(\sqrt{-10}\alpha/3, 2\sqrt{-10}\alpha/3) \times (0, \alpha/4, 3\alpha/4, \alpha)$ . Otherwise, the circles will not cover the rectangle.

Then analyzing the cases<sup>1</sup>, one finds that if  $\beta = \sqrt{-10}\alpha/3$ , then multiplying by  $\sqrt{-10}$ ,  $-10\alpha/3 \in A \Rightarrow \alpha/3 \in A$ . This contradicts the fact that  $\alpha$  was chosen to be the element of minimal norm. Using a similar technique one finds that most of the centers of the circles cannot be  $\beta \in A$ . But,  $\frac{1}{2}\sqrt{-10} \cdot \alpha$  will work.

Thus the possible ideals are multiples of  $(\alpha)$  and  $(\alpha, \frac{1}{2}\sqrt{-10} \cdot \alpha)$ .

**Problem 9** Let  $d \leq -3$ . Prove that 2 is not a prime element in the ring  $\mathbb{Z}[\sqrt{d}]$ , but that 2 is irreducible in this ring.

If 2 was prime, then  $2|ab \Rightarrow 2|a$  OR  $2|b$ .

If  $d$  is odd, let  $2\alpha = (1 + \sqrt{d})(1 - \sqrt{d}) = 1 - d$ . Thus  $\alpha = \frac{1-d}{2} \in \mathbb{Z}$  and  $\geq 2$  for  $d \leq -3$ .

and 2 does not divide  $(1 + \sqrt{d})$  or  $(1 - \sqrt{d})$ .

If  $d$  is even, let  $2\alpha = (2 + \sqrt{d})(2 - \sqrt{d}) = 2 - d$  OR  $\sqrt{d} \cdot (-\sqrt{d})$ .

However, 2 is irreducible because  $N(2) = 4 = N(\alpha)N(\beta)$  if  $\alpha\beta = 2$ .

$N(\alpha) = N(a + b\sqrt{d}) = a^2 + b^2|d| > |d| \geq 4$  whenever  $b \neq 0$  and  $a \neq 0$ . If  $b \neq 0$ ,  $\alpha$  is an integer, but 2 is irreducible over the integers. If  $a \neq 0$ ,  $\alpha^2$  is a multiple of  $d \in \mathbb{Z}$  which will not divide 2. We would need  $N(\alpha) = 2$  so that  $N(\alpha)N(\beta) = 2 \cdot 2$ .

### 3. CHAPTER 11, SECTION 8

**Problem 1** Let  $R = \mathbb{Z}[\sqrt{-6}]$ . Factor the ideal  $(6)$  into prime ideals explicitly.

$(6) = (2)(3) = (\sqrt{-6})(-\sqrt{-6})$ . For a common refinement, consider  $A = (2, \sqrt{-6})$ ,  $B = (3, \sqrt{-6})$ . In fact,  $\overline{A} = A$  and  $\overline{B} = B$  since  $-\sqrt{-6} \in (\sqrt{-6})$ .

Now we need to show  $A$  and  $B$  are prime ideals. The usual way to prove  $P$  is a prime ideal is to prove  $R/P$  is a field. In this case  $R/A \cong \mathbb{F}_2$ ,  $R/B \cong \mathbb{F}_3$ . Another way to do this is to show the norms of elements in this ideal are prime, thus the elements will be irreducible.

Also, we can show by linear identities that  $A^2 = (2)$ ,  $B^2 = (3)$ , and  $AB = (\sqrt{-6})$ . So  $(6) = A^2B^2$ .

<sup>1</sup>Thanks to Elizabeth Schemm

**Problem 2** Let  $\delta = \sqrt{-3}$  and  $R = \mathbb{Z}[\delta]$ . (This is not the ring of integers in the imaginary quadratic number field  $\mathbb{Q}[\delta]$ .) Let  $A$  be the ideal  $(2, 1 + \delta)$ . Show that  $A\bar{A}$  is not a principal ideal, hence that the Main Lemma is not true for this ring.

$A\bar{A} = (4, 2 + 2\delta, 2 - 2\delta)$  since the product of two ideals is the ideal which is the product of its generators. Clearly  $A\bar{A} \supset (4)$  and 2 divides all the generators so  $(2) \supseteq A\bar{A}$ . But since  $2 \notin A\bar{A}$  by virtue of the fact no linear combination (using integers and integer multiples of  $\delta$ ) of the generators equals 2.

**Problem 3** Let  $R = \mathbb{Z}[\sqrt{-5}]$ . Determine whether or not 11 is an irreducible element of  $R$  and whether or not  $(11)$  is a prime ideal in  $R$ .

To prove 11 is irreducible, use the same method as problem 11.7.9. Namely a nontrivial factorization  $\alpha\beta = 11 \Rightarrow N(\alpha)N(\beta) = 11^2 \Rightarrow N(\alpha), N(\beta) = 11$ .

However, if  $\alpha = a + b\sqrt{-5}$ , then  $N(\alpha) = a^2 + 5b^2 \neq 11$  for any choice of  $a, b$ .

To prove  $(11)$  is a prime ideal, here are two good strategies:

- Any ideal is a sublattice. One can show using norms, and geometry,  $(11)$  is a maximal sublattice which implies it is a prime ideal.

- We could show  $R/(11)$  is a field.  $R/(11) \cong \mathbb{Z}[\sqrt{-5}]/(11) \cong \mathbb{Z}[x]/(x^2 + 5, 11) \cong \mathbb{F}_{11}[x]/(x^2 + 5)$ . This last ring is a field  $\Leftrightarrow x^2 + 5$  is irreducible modulo 11. By inspection, one can find  $6 \equiv -5$  is not a square modulo 11.