

1. **An idempotent in a ring  $R$  is an element  $e$  such that  $e^2 = e$ . What are the idempotents in  $\mathbb{Z} \oplus \mathbb{Z}$ ?  $\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}$ ?**

We need  $(a, b)$  with  $(a, b)^2 = (a, b)$ . This says  $(a^2, b^2) = (a, b)$ , so  $a^2 = a$  and  $b^2 = b$ . We need  $a = 0$  or  $1$ , and  $b = 0$  or  $1$ , so there are four idempotents in  $\mathbb{Z} \oplus \mathbb{Z}$ :  $(0, 0)$ ,  $(1, 0)$ ,  $(0, 1)$ , and  $(1, 1)$ . There are 8 idempotents in  $\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}$ , I'll let you use your imagination to get them.

2. **Find the sizes of the following rings.**

a.  $\mathbb{Z}[\sqrt{-2}] / \langle \sqrt{-2} \rangle$

Let  $I = \langle \sqrt{-2} \rangle$ . Since  $\sqrt{-2} \sqrt{-2} = -2$ , we have that  $2 \in I$ . Thus, the cosets of  $I$  are  $a + b\sqrt{-2} + I = a + I$  (since  $b\sqrt{-2} \in I$ ), and we can reduce  $a \pmod 2$  to get  $\mathbb{Z}[\sqrt{-2}] / \langle \sqrt{-2} \rangle = \{I, 1 + I\}$ . There are two cosets, so the factor ring has size 2.

b.  $\mathbb{Z}[\sqrt{-2}] / \langle 2 + \sqrt{-2} \rangle$

Let  $J = \langle 2 + \sqrt{-2} \rangle$ . The first step is always to find the smallest positive integer in  $J$ . Since  $(2 + \sqrt{-2})(a + b\sqrt{-2}) = 2a - 2b + (a + 2b)\sqrt{-2}$ , to be an integer, we need  $a = -2b$ , so  $2a - 2b = -6b$ . The integers in  $J$  are multiples of 6. Now  $a + b\sqrt{-2} + J = a + b\sqrt{-2} - b(2 + \sqrt{-2}) + J = a - 2b + J$ . This shows all cosets have the form  $n + J$  for some integer  $n$ . Since  $6 \in J$ , we can limit  $n$  to  $0, 1, 2, 3, 4, 5$ , these are all from different cosets since 6 is the smallest positive integer in  $J$ . Thus,  $\mathbb{Z}[\sqrt{-2}] / \langle 2 + \sqrt{-2} \rangle$  has size 6.

c.  $\mathbb{Z}[\sqrt{-2}] / \langle 1 + 2\sqrt{-2} \rangle$  (Hint: This is trickier than (b), but note that  $-\sqrt{-2}(1 + 2\sqrt{-2}) = 4 - \sqrt{-2}$ .)

Let  $K = \langle 1 + 2\sqrt{-2} \rangle$ . As above,  $(1 + 2\sqrt{-2})(a + b\sqrt{-2}) = a - 4b + (2a + b)\sqrt{-2}$ , and this is an integer only when  $b = -2a$ . In this case,  $a - 4b = 9a$ , so the integers in  $K$  are multiples of 9. Since  $-\sqrt{-2}(1 + 2\sqrt{-2}) = 4 - \sqrt{-2}$ ,  $4 - \sqrt{-2} \in K$ . Using this,  $a + b\sqrt{-2} + K = a + b\sqrt{-2} + b(4 - \sqrt{-2}) + K = a + 4b + K$ , and again, all cosets have the form  $n + K$ . Since 9 is the smallest positive integer in  $K$ , there are exactly 9 such cosets, so the ring has size 9.



6. **Show that for any  $n \geq 1$ , there is an irreducible polynomial over  $\mathbf{Q}$  of degree  $n$ .**

Use an Eisenstein polynomial! In fact,  $x^n + 2$  is irreducible of degree  $n$ .

7.  $\mathbf{Z} \left[ \sqrt[3]{2} \right] = \left\{ a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbf{Z} \right\}.$

a. **Show that  $\langle \sqrt[3]{2} \rangle$  is a maximal ideal of  $\mathbf{Z}[\sqrt[3]{2}]$ .**

Two approaches: Let  $I = \langle \sqrt[3]{2} \rangle$ . Since  $(\sqrt[3]{2})^2 = \sqrt[3]{4}$ , and  $(\sqrt[3]{2})^3 = 2$ ,

$a + b\sqrt[3]{2} + c\sqrt[3]{4} + I = a + I$ , and we can reduce  $a$  mod 2 to 0 or 1. Thus,  $\mathbf{Z}[\sqrt[3]{2}] / \langle \sqrt[3]{2} \rangle = \{I, 1 + I\}$ , the field with two elements. In particular, it is a field, so  $I$  is maximal.

Alternatively, if  $I \subseteq J \subseteq \mathbf{Z}[\sqrt[3]{2}]$ , and the first containment is proper, then let  $a + b\sqrt[3]{2} + c\sqrt[3]{4} \in J - I$ . Since  $\sqrt[3]{2}, \sqrt[3]{4} \in I$ , it must be that  $a \notin I$  but  $a \in J$ . Again since  $2 \in I$ , all even numbers are in  $I$  so  $a$  is odd. This means that  $a - 1 \in J$  since it is even, so  $a - (a - 1) = 1 \in J$  showing  $J = \mathbf{Z}[\sqrt[3]{2}]$ .

b. **Show that  $\langle \sqrt[3]{4} \rangle$  is not a maximal ideal of  $\mathbf{Z}[\sqrt[3]{2}]$ .**

$\langle \sqrt[3]{4} \rangle \subseteq \langle \sqrt[3]{2} \rangle \subseteq \mathbf{Z}[\sqrt[3]{2}]$ , and each containment is proper. To see this,

$(a + b\sqrt[3]{2} + c\sqrt[3]{4})\sqrt[3]{4} = a\sqrt[3]{4} + 2b + 2c\sqrt[3]{2} = 2b + 2c\sqrt[3]{2} + a\sqrt[3]{4}$ . This means

that  $x + y\sqrt[3]{2} + z\sqrt[3]{4} \in \langle \sqrt[3]{4} \rangle$  only when  $x$  and  $y$  are even. In particular,

$\sqrt[3]{2} \notin \langle \sqrt[3]{4} \rangle$ . Similarly,  $1 \notin \langle \sqrt[3]{2} \rangle$  since  $(a + b\sqrt[3]{2} + c\sqrt[3]{4})\sqrt[3]{2}$

$= 2c + a\sqrt[3]{2} + b\sqrt[3]{4}$  has even constant term.

**What happens in  $\mathbf{Q}(\sqrt[2]{2})$ ? This should have been **What happens in  $\mathbf{Q}(\sqrt[3]{2})$ ?****

This is sort of a trick question:  $\mathbf{Q}(\sqrt[3]{2})$  is a field so for any  $a \neq 0$ ,  $\langle a \rangle = \mathbf{Q}(\sqrt[3]{2})$

That is, no ideals are maximal here.

8. **Show that  $\mathbb{Z}[\sqrt[3]{2}]$  is a Euclidean ring. Hint: use  $N(a + b\sqrt[3]{2} + c\sqrt[3]{4}) = |a^3 + 2b^3 + 4c^3 - 6abc|$ . You may use the properties:  $N(x)$  is always an ordinary integer,  $N(x) = 0$  only if  $x = 0$ , and  $N(xy) = N(x)N(y)$ .**

This just follows the standard method: Let  $d(x) = N(x)$ . Then  $d(xy) = d(x)d(y)$  shows that  $d(x) \leq d(xy)$  for all  $x, y$ . Next, given  $x, y$  in the ring,  $xy^{-1} \in \mathbb{Q}(\sqrt[3]{2})$

so  $xy^{-1} = a + b\sqrt[3]{2} + c\sqrt[3]{4}$  for rational  $a, b, c$ . Pick the nearest integers

$m, n, k$  to  $a, b, c$  respectively and let  $q = m + n\sqrt[3]{2} + k\sqrt[3]{4}$ . Then

$x = yq + r$ , where  $r = x - yq$  is in the ring, and

$r = ((a-m) + (b-n)\sqrt[3]{2} + (c-k)\sqrt[3]{4})y = (u + v\sqrt[3]{2} + w\sqrt[3]{4})y$  with

$-\frac{1}{2} \leq u, v, w \leq \frac{1}{2}$ . Finally,  $N(r) = N(y)N(u + v\sqrt[3]{2} + w\sqrt[3]{4})$

$= N(y) |u^3 + 2v^3 + 4w^3 - 6uvw|$ . The analysis of  $|u^3 + 2v^3 + 4w^3 - 6uvw|$  is a bit pesky: if  $u, v, w$  are all positive, then ignoring  $6uvw$ , this is at most  $\frac{7}{8}$ .

But if  $u$ , say, were negative with  $v, w = \frac{1}{2}$ , this would be  $|u^3 + \frac{1}{4} + \frac{1}{2} - \frac{3}{4}u|$

which has a max of 1 at  $u = -\frac{1}{2}$ . This is, in fact the worst case: if it were

$v$  or  $w$  that were negative,  $|u^3 + 2v^3 + 4w^3 - 6uvw| < 1$ . To salvage the

case where  $u$  is negative, when picking  $m$ , always pick it so that  $a - m > -\frac{1}{2}$ .

(That is, if we could pick  $m$  with  $a - m = -\frac{1}{2}$ , then using  $m' = m - 1$ ,

$a - m' = \frac{1}{2}$ . Given a choice, use the  $+\frac{1}{2}$  rather than the  $-\frac{1}{2}$ .) This analysis is

too involved for a final exam.

9. **Show that  $\mathbb{Q}(\sqrt[6]{2}) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ .**

We show  $\mathbb{Q}(\sqrt[6]{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$  and  $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt[6]{2})$ . This is

equivalent to showing that  $\sqrt[6]{2} \in \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$  and  $\sqrt{2}, \sqrt[3]{2} \in \mathbb{Q}(\sqrt[6]{2})$ .

For these second two, since  $\sqrt[6]{2} \in \mathbb{Q}(\sqrt[6]{2})$ , so is  $(\sqrt[6]{2})^2$  and  $(\sqrt[6]{2})^3$ . For

the other direction,  $\sqrt{2}, \sqrt[3]{2} \in \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$  so their quotient  $\frac{\sqrt{2}}{\sqrt[3]{2}} = \sqrt[6]{2}$

is as well.

10. **Find the splitting field for  $x^4 - x^2 + 1$  over each of the following fields. (In each case, you may write the answer in the form  $F(a, b, c, \dots)$  where  $a, b, c, \dots$  are zeros of specified irreducible polynomials.)**

I tend to do all of these by various (trick?) methods of completing the square, where the field dictates the method. With  $x^4 - x^2 + 1$ , there are two obvious choices:  $x^4 - x^2 + 1 = x^4 + 2x^2 + 1 - 3x^2 = (x^2 + 1)^2 - 3x^2$ , and

$$x^4 - x^2 + 1 = x^4 - 2x^2 + 1 + x^2 = (x^2 - 1)^2 + x^2$$

- a. **Q:**  $x^4 - x^2 + 1 = x^4 + 2x^2 + 1 - 3x^2 = (x^2 + 1)^2 - 3x^2$   
 $= (x^2 - \sqrt{3}x + 1)(x^2 + \sqrt{3}x + 1)$ . To continue, we can use the quadratic formula. For  $x^2 - \sqrt{3}x + 1$ , for example, the zeros are  $\frac{\sqrt{3} \pm \sqrt{3-4}}{2}$ . A similar thing happens for  $x^2 + \sqrt{3}x + 1$ , so the polynomial splits in  $\mathbb{Q}(\sqrt{3}, i)$ .
- b. **R** Since  $x^4 - x^2 + 1$  has complex roots, the splitting field here must be  $\mathbb{R}(i)$ , better known as  $\mathbb{C}$ .
- c.  **$Z_2$**  This is a bit of a tricky case, since in  $Z_2$ ,  $x^4 + x^2 + 1 = (x^2 + x + 1)^2$  (In  $Z_2$ ,  $(a + b + c + \dots)^2 = a^2 + b^2 + c^2 + \dots$ ) We've seen  $x^2 + x + 1$  over  $Z_2$  enough to know that it is irreducible. If  $a$  is a zero of this polynomial in some extension of  $Z_2$ , then the splitting field is  $Z_2(a)$ .
- d.  **$Z_3$**  Since  $3 = 0$  in  $Z_3$ , the first factorization,  $x^4 - x^2 + 1 = (x^2 + 1)^2 - 3x^2$  is called for, since this is just  $x^4 - x^2 + 1 = (x^2 + 1)^2$ . Since  $x^2 + 1$  has no zeros in  $Z_3$ , it is irreducible. We may call  $i$  a zero for it, and write the splitting field  $Z_3(i)$ .
- e.  **$Z_5$**  Here, we use the second factorization:  $x^4 - x^2 + 1 = (x^2 - 1)^2 + x^2$ . The reason is that  $2^2 = 4 = -1$ , so we can write this:  
 $(x^2 - 1)^2 - 4x^2 = (x^2 - 2x - 1)(x^2 + 2x - 1)$ . Now  $x^2 - 2x - 1 = x^2 - 2x + 1 - 2 = (x - 1)^2 - 2$ , and  $x^2 + 2x - 1 = (x + 1)^2 - 2$ . If 2 were a perfect square in  $Z_5$ , these would both factor and  $Z_5$  would have been the splitting field. But 2 is not a square, so the splitting field is  $Z_5(\sqrt{2})$  in this case. (It was conceivable that  $x^4 - x^2 + 1$  could have factored into two irreducible quadratics that each required a different square root to factor, making the splitting field  $Z_5(\sqrt{a}, \sqrt{b})$ , but this did not happen here as  $\sqrt{2}$  was needed for both polynomials.)

11. **There is still room for elementary algebra in a class like this. Suppose that  $p(x)$  is an irreducible cubic over  $\mathbb{Q}$ . If  $p(x)$  has one real root, show that the splitting field,  $E$ , of  $p(x)$  over  $\mathbb{Q}$  has  $[E : \mathbb{Q}] = 6$ .**

Let  $a$  be the real zero of  $p(x)$  in some extension of  $\mathbb{Q}$ . Then we know  $[Q(a) : \mathbb{Q}] = 3$ , so if  $E$  is the splitting field,  $[E : \mathbb{Q}] = [E : Q(a)][Q(a) : \mathbb{Q}] \geq 3$ . We also know that  $p(x) = (x - a)(\text{quadratic})$  over  $Q(a)$ , and this quadratic has complex roots. This means it can't factor over  $Q(a)$  since everything in  $Q(a)$  is real. Thus, the quadratic is irreducible over  $Q(a)$ ,  $E$  is a proper extension of  $Q(a)$ , and the degree of the extension is 2. Hence,  $[E:\mathbb{Q}] = [E:Q(a)][Q(a):\mathbb{Q}] = 2 \cdot 3 = 6$ .

For irreducible cubics with three real roots, the analysis is MUCH harder. If  $a$  is a zero of  $p(x)$ , then  $p(x)$  still is  $(x - a)(\text{some quadratic})$ . Sometimes the quadratic factors over  $Q(a)$ , sometimes it does not.

12. **Let  $a = \sqrt{2 + \sqrt{2 + \sqrt{2}}}$  and  $b = \sqrt{2 + \sqrt{2}}$ . Find, with proof, the minimal polynomials of  $a$ ,  $b$ ,  $a + b$  over  $\mathbb{Q}$ .**

Let  $x = b = \sqrt{2 + \sqrt{2}}$ . Then  $x^2 = 2 + \sqrt{2}$ , so  $(x^2 - 2)^2 = 2$ . Multiplying this out,  **$b$  is a zero of  $x^4 - 4x^2 + 2$** . This polynomial is irreducible by

Eisenstein's criteria (with  $p = 2$ ). For  $a$ ,  $x = \sqrt{2 + \sqrt{2 + \sqrt{2}}}$ , so  $x^2 = 2 + \sqrt{2 + \sqrt{2}}$ ,  $(x^2 - 2)^2 = 2 + \sqrt{2}$ , or  $x^4 - 4x^2 + 2 = \sqrt{2}$ .

Thus,  **$a$  is a zero of  $(x^4 - 4x^2 + 2)^2 - 2 = x^8 - 8x^6 + 20x^4 - 16x^2 + 2$** , which is again irreducible by Eisenstein's criteria.

For  $a + b$ , we may write  $x = a + b$ , so  $x - b = a$ , or  $(x - b)^2 = 2 + b$  or

$x^2 - 2\sqrt{2 + \sqrt{2}}x + 2 + \sqrt{2} = 2 + \sqrt{2 + \sqrt{2}}$ . Rewriting,

$x^2 + \sqrt{2} = (2x + 1)\sqrt{2 + \sqrt{2}}$ , so  $x^4 + 2\sqrt{2}x^2 + 2 = (4x^2 + 4x + 1)(2 + \sqrt{2})$ .

We isolate  $\sqrt{2}$ :  $x^4 + 2 - 2(4x^2 + 4x + 1) = \sqrt{2}(4x^2 + 4x + 1 - 2x^2)$ .

Squaring one last time,  $(x^4 - 8x^2 - 8x)^2 = 2(2x^2 + 4x + 1)^2$ ,

$x^8 + 64x^4 + 64x^2 - 16x^6 - 16x^5 + 128x^3 = 8x^4 + 32x^2 + 2 + 32x^3 + 8x^2 + 16x$ ,

or  $x^8 - 16x^6 - 16x^5 + 56x^4 + 96x^3 + 24x^2 - 16x^2 - 2 = 0$ . Thus, the polynomial for  $a + b$  is  $x^8 - 16x^6 - 16x^5 + 56x^4 + 96x^3 + 24x^2 - 16x^2 - 2$ , again irreducible by Eisenstein's criteria. I actually checked, by the way, that  $a + b$  is a zero of this last polynomial.

13. Find, with proof, the minimal polynomial of  $\sqrt{2} + \sqrt[3]{2}$  over each of the following fields:

a.  $E_1 = \mathbb{Q}(\sqrt[3]{2})$

Here  $\sqrt[3]{2}$  is in  $E_1$ , so we may set  $x = \sqrt{2} + \sqrt[3]{2}$ ,  $x - \sqrt[3]{2} = \sqrt{2}$ , and so  $x^2 - 2\sqrt[3]{2}x + \sqrt[3]{4} - 2 = 0$ . The minimal polynomial is  $x^2 - 2\sqrt[3]{2}x + \sqrt[3]{4} - 2$ .

b.  $E_2 = \mathbb{Q}(\sqrt{2})$

In this case, we write  $x - \sqrt{2} = \sqrt[3]{2}$ , and cube:  $x^3 - 3x^2\sqrt{2} + 6x - 2\sqrt{2} = 2$ , so the polynomial will be  $x^3 - 3x^2\sqrt{2} + 6x - 2\sqrt{2} - 2$ .

c.  $\mathbb{Q}$

We can take either of the polynomials above and isolate a radical. For example, if  $x^3 - 3x^2\sqrt{2} + 6x - 2\sqrt{2} - 2 = 0$ , then  $x^3 + 6x - 2 = \sqrt{2}(3x^2 + 2)$ , or  $x^6 + 12x^4 - 4x^3 + 36x^2 - 24x + 4 = 18x^4 + 24x^2 + 8$ .

That is,  $x^6 - 6x^4 - 4x^3 + 18x^2 - 24x - 4 = 0$ .

For the justifications, we need the three polynomials to be irreducible over their respective fields. For  $E_1$ , we require that  $\sqrt{2} \notin E_1$ . Theory helps here!

We know  $[E_1:\mathbb{Q}] = 3$ . If  $\sqrt{2} \in E_1$ , then  $\mathbb{Q}(\sqrt{2}) \subseteq E_1$ , meaning that

$3 = [E_1:\mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}):\mathbb{Q}]$ , so 3 is even, a contradiction. Similarly, we can

show that the polynomial in (b) is irreducible by showing that  $\sqrt[3]{2} \notin E_2$ . Part c

is the hardest. If the polynomial were an Eisenstein polynomial, we would be done, but it isn't. This would be hard, using Chapter 17 stuff: we would have to rule out linear factors (easy), irreducible quadratics, and irreducible cubic factors. Using Chapter 21 stuff instead, it is just tricky! If we can show that

$[\mathbb{Q}(\sqrt{2} + \sqrt[3]{2}):\mathbb{Q}] = 6$ , then the minimal polynomial for  $\sqrt{2} + \sqrt[3]{2}$  must have degree 6, as well. Here is the approach I'm going to take: Show that

$\mathbb{Q}(\sqrt{2} + \sqrt[3]{2})$  contains both  $\sqrt{2}$  and  $\sqrt[3]{2}$ . In this case, by problem 9, this

field will contain  $\mathbb{Q}(\sqrt[6]{2})$ , so it must be at least degree 6 (the minimal polynomial

for  $\sqrt[6]{2}$  is  $x^6 - 2$ , irreducible by Eisenstein.) Now by part b, if  $a = \sqrt{2} + \sqrt[3]{2}$ ,

then  $a^3 - 3a^2\sqrt{2} + 6a - 2\sqrt{2} = 2$ , which we can rewrite  $\sqrt{2} = \frac{a^3 + 6a - 2}{3a^2 + 2}$ .

Since  $a \in Q(a)$ , and  $Q(a)$  is a field,  $\sqrt{2} \in Q(a)$ . But then  $a - \sqrt{2} = \sqrt[3]{2} \in Q(a)$  as well, so we are done.

14. **Let  $F$  be any field of characteristic  $\neq 2$  and let  $E$  be an extension of  $F$  such that  $[E:F] = 2$ . Show that  $E = F(\sqrt{a})$  for some  $a \in F$ . Hint: complete the square of an appropriate quadratic.**

Let  $b$  be some element of  $E$  which is not in  $F$ . Since  $[E:F] = 2$ ,  $b$  is algebraic of degree 2 over  $F$ . Hence,  $b$  is the zero of a quadratic,  $x^2 + ux + v$ , for some

$u, v$  in  $F$ . If we complete the square,  $x^2 + ux + v = \left(x + \frac{u}{2}\right)^2 + v - \frac{u^2}{4}$   
 $= \left(x + \frac{u}{2}\right)^2 - \frac{u^2 - 4v}{4}$ . Since this is irreducible,  $u^2 - 4v$  can't be a square in  $F$ ,

so let  $a = u^2 - 4v$ . Then  $b = -\frac{u}{2} \pm \frac{\sqrt{a}}{2}$  (we don't know which sign to choose, but it is one or the other) so  $E \subseteq F(\sqrt{a})$ . Since  $\sqrt{a}$  can be written in terms of  $b$  (eg  $\sqrt{a} = \pm(2b + u)$ ) we have  $F(\sqrt{a}) \subseteq E$  as well, so these are equal.