

# Workshop 3

## Algebra 2

2026 Semester 1

You must be able to justify (prove) every claim you make, no matter how “trivial” it seems. If you cannot justify it, please ask me or your demonstrator. If you can justify it but are not satisfied with the proof (too long, too messy, or something else), please ask. It is possible that there is a better way, and you will benefit from knowing it.

### Warm-up

1. Is  $\mathbf{Z}[i]/(11)$  an integral domain? A field?

The ring  $\mathbf{Z}[i]$  is a Euclidean domain, hence a principal ideal domain. The element 11 is prime in  $\mathbf{Z}[i]$ , since there do not exist integers  $a, b$  such that  $a^2 + b^2 = 11$ . In a principal ideal domain, every non-zero prime ideal is maximal, so  $(11)$  is maximal. Thus  $\mathbf{Z}[i]/(11)$  is a field.

2. Find primes  $p \in \mathbf{Z}$  which do and do not remain primes in  $\mathbf{Z}[\sqrt{2}]$ .

A prime  $p$  remains prime in  $\mathbf{Z}[\sqrt{2}]$  if and only if  $p$  is not of the form  $a^2 - 2b^2$ , that is,  $2 \not\equiv x^2 \pmod{p}$  for some  $x \in \mathbf{Z}$ .

3. Let  $F \subset K$  be fields and  $\alpha \in K$ . Recall the definition of the irreducible polynomial (also called *minimal polynomial*) of  $\alpha$  over  $F$ . Given any  $f(x) \in F[x]$  such that  $f(\alpha) = 0$ , how will you find the minimal polynomial?

The minimal polynomial of  $\alpha$  over  $F$  is the unique monic irreducible polynomial  $m_\alpha(x) \in F[x]$  such that  $m_\alpha(\alpha) = 0$ . Factorise  $f(x)$  and find the unique monic factor that vanishes at  $\alpha$ .

## Field extensions and irreducible polynomials

1. Let  $F = \mathbf{Q}[2^{1/6}]$ .
  - (a) Find the kernel of the map  $\mathbf{Q}[x] \rightarrow F$  that sends  $x$  to  $2^{1/6}$ .  
 $(x^6 - 2)$
  - (b) What is the irreducible (= minimal) polynomial of  $2^{1/6}$  over  $\mathbf{Q}$ ?  
 $x^6 - 2$
  - (c) Write a basis of  $F$  as a  $\mathbf{Q}$ -vector space.  
 Let  $\alpha = 2^{1/6}$ . Then the basis is  $\{1, \alpha, \alpha^2, \dots, \alpha^5\}$ .
  
2. Let  $\zeta = e^{2\pi i/6}$ . Let  $L = \mathbf{Q}[2^{1/6}\zeta]$  and  $F = \mathbf{Q}[2^{1/6}]$  as above. We consider both as subfields of  $\mathbf{C}$ .
  - (a) Is  $F = L$ ? No.  $F \subset \mathbf{R}$  and  $i \in L$ .
  - (b) Is there an isomorphism  $F \rightarrow L$ ? Are there multiple isomorphisms? How many?  
 Two isomorphisms.  $2^{1/6} \mapsto 2^{1/6}\zeta$  and  $2^{1/6} \mapsto -2^{1/6}\zeta$
  - (c) Observe that  $K = \mathbf{Q}[\sqrt{2}]$  is contained in both  $F$  and  $L$ . How many isomorphisms  $F \rightarrow L$  are  $K$ -isomorphisms?  
 One:  $2^{1/6} \mapsto -2^{1/6}\zeta$
  - (d) Find the degrees of  $F$  over  $\mathbf{Q}$ ; of  $L$  over  $\mathbf{Q}$ ; of  $F$  over  $K$ ; and of  $L$  over  $K$ . 6, 6, 3, 3
  
3. Let  $\alpha, \beta \in \mathbf{C}$  be algebraic over  $\mathbf{Q}$ . Consider the map  $\mathbf{Q}[x, y] \rightarrow \mathbf{C}$  that sends  $x \rightarrow \alpha$  and  $y \rightarrow \beta$ . Let  $I \subset \mathbf{Q}[x, y]$  be the kernel of this map.
  - (a) Let  $f(x) \in \mathbf{Q}[x]$  be the irreducible polynomial of  $\alpha$ . Show that  $f(x) \in I$ . Similarly, for the irreducible polynomial  $g(y) \in \mathbf{Q}[y]$ , we have  $g(y) \in I$ . Conclude that  $I$  cannot be principal.  
 $f(\alpha) = 0, g(\beta) = 0$ . There does not exist  $h(x, y) \in \mathbf{Q}[x, y]$  such that  $h(x, y)|f(x)$  and  $h(x, y)|g(y)$ , thus  $I$  cannot be principal.
  - (b) Is  $I$  generated by  $f(x)$  and  $g(y)$ ? Find examples where it is not.  
 Let  $\alpha = \beta = \sqrt{2}$ , then  $I = (x^2 - 2, y^2 - 2, x - y)$ .
  
4. Let  $F \subset K$  be fields and let  $\alpha \in K$  be algebraic over  $F$  with irreducible polynomial  $f(x) \in F[x]$ . Find a bijection between the following two sets:
  - (a)  $F$ -homomorphisms  $F[\alpha] \rightarrow K$  (ring homomorphisms that restrict to the identity on  $F$ )

(b) solutions to  $f(x) = 0$  in  $K$ .

Since  $\phi$  is an  $F$ -homomorphism, it fixes  $F$ , so

$$f(\beta) = f(\phi(\alpha)) = \phi(f(\alpha)) = \phi(0) = 0.$$

Define the bijection as  $\phi \mapsto \phi(\alpha)$  from (a) to (b) and  $\beta \mapsto \phi_\beta$  from (b) to (a) where  $\phi_\beta(\alpha) = \beta$ .