

*In the higher dimensions you cannot see everything, so you must have something, some tool, to guess or formulate things. And the tool was algebra, unquestionably algebra.*

H. Hironaka

1. a) State the Eisenstein irreducibility criterion.  
b) Use the Eisenstein criterion to prove  $\Phi_p(T) = \frac{T^p-1}{T-1} = 1 + T + \dots + T^{p-1}$  is irreducible in  $\mathbf{Q}[T]$ .  
c) Let  $\zeta_n$  be a primitive  $n$ th root of unity. Explain why  $\mathbf{Q}(\zeta_n)/\mathbf{Q}$  is a Galois extension and construct – with details – an injective group homomorphism  $\text{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q}) \rightarrow (\mathbf{Z}/n\mathbf{Z})^\times$ .  
d) For a prime  $p$ , use parts b and c to show there is a group isomorphism  $\text{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q}) \cong (\mathbf{Z}/p\mathbf{Z})^\times$ .  
e) The group  $(\mathbf{Z}/19\mathbf{Z})^\times$  is cyclic (a generator is 2). Use this and part d to construct a cyclic Galois extension of  $\mathbf{Q}$  with degree 9.
2. (Minimal polynomial)  
a) Show minimal polynomials are irreducible. More precisely, show the minimal polynomial in  $F[T]$  of a number in a finite extension of  $F$  is irreducible.  
b) Show every ideal in  $F[T]$  is principal. What does this tell you about polynomials in  $F[T]$  with a fixed root?  
c) Use part a and field theory to prove  $T^5 - 2$  is irreducible in  $\mathbf{Q}(\sqrt[4]{3})[T]$ . (Don't try to use reduction mod  $p$  or Eisenstein's criterion in  $\mathbf{Q}(\sqrt[4]{3})[T]$ . We only learned those tests in  $\mathbf{Q}[T]$ .)
3. a) Define the derivative on  $F[T]$  and state familiar rules from calculus which it satisfies (for all fields  $F$ ) and also rules about derivatives in calculus which need not remain true in  $F[T]$ .  
b) Let  $f(T)$  and  $g(T)$  be nonconstant polynomials in  $F[T]$ . Show they have no common root in any extension of  $F$  if and only if  $(f(T), g(T)) = 1$ .  
c) Use parts a and b to show  $f(T) \in F[T]$  has no multiple roots in a splitting field over  $F$  if and only if  $(f(T), f'(T)) = 1$ .
4. Let  $f(T)$  and  $g(T)$  be irreducible in  $F[T]$  with degrees  $m$  and  $n$ . Let  $\alpha, \beta$  satisfy  $f(\alpha) = 0$  and  $g(\beta) = 0$ .  
a) Use properties of field extensions to show  $[F(\alpha, \beta) : F] \leq mn$ .  
b) If  $(m, n) = 1$ , show  $[F(\alpha, \beta) : F] = mn$ . Make it clear how the property  $(m, n) = 1$  is used.  
c) Give an example where  $(m, n) > 1$  and  $[F(\alpha, \beta) : F] = mn$ .  
d) Give an example where  $(m, n) > 1$  and  $[F(\alpha, \beta) : F] < mn$ .
5. (Finite fields)  
a) Show any finite field has prime power order.  
b) Show  $T^3 + T + 1$  is irreducible in  $\mathbf{F}_5[T]$ .  
c) Construct a splitting field of  $T^3 + T + 1$  over  $\mathbf{F}_5$  and write down all three roots of the polynomial in that field in terms of a basis for that field over  $\mathbf{F}_5$ .  
d) Use Galois theory for finite fields to explain why the discriminant of an irreducible cubic in  $\mathbf{F}_p[T]$  must be a perfect square in  $\mathbf{F}_p$ .

6. Let  $\alpha$  and  $\beta$  in  $\mathbf{C}$  satisfy  $\alpha^2 = 1 + \sqrt{3}$  and  $\beta^2 = 1 - \sqrt{3}$ . So  $\alpha$  and  $\beta$  are both roots of  $(T^2 - 1)^2 - 3 = T^4 - 2T^2 - 2$ , which is irreducible over  $\mathbf{Q}$  with roots  $\pm\alpha$  and  $\pm\beta$ .
- Explain why  $\mathbf{Q}(\alpha, \beta)/\mathbf{Q}$  has degree 8 and is a Galois extension.
  - Explain why automorphisms  $\sigma$  and  $\tau$  in  $\text{Gal}(\mathbf{Q}(\alpha, \beta)/\mathbf{Q})$  with the indicated values on  $\alpha$  and  $\beta$  in the table below actually exist.
  - Fill in the rest of the table and then describe the Galois group in concrete terms (that is, up to isomorphism) as a familiar group of order 8.
  - Use the Galois group to determine the degree over  $\mathbf{Q}$  of  $\alpha + \beta$ .

$\varphi$	$\varphi(\alpha)$	$\varphi(\beta)$
id.	$\alpha$	$\beta$
$\sigma$	$\beta$	$-\alpha$
$\sigma^2$		
$\sigma^3$		
$\tau$	$\alpha$	$-\beta$
$\sigma\tau$		
$\sigma^2\tau$		
$\sigma^3\tau$		

7. (Examples) Give an example illustrating each of the following.
- A Galois extension with cyclic Galois group of order 6.
  - A Galois extension with abelian Galois group that is not cyclic.
  - A Galois extension with nonabelian Galois group other than the field in the previous problem.