

Reading: §§8.4 and 8.6 in text.

Note: The **final exam** is scheduled for May 6 (Wednesday) 3:30-5:30 in MSB 415.

*I attempted mathematics, and even went during the summer of 1828 with a private tutor (a very dull man) to Barmouth, but I got on very slowly. The work was repugnant to me, chiefly from my not being able to see any meaning in the early steps in algebra. This impatience was very foolish, and in after years I have deeply regretted that I did not proceed far enough at least to understand something of the great leading principles of mathematics; for men thus endowed seem to have an extra sense.* Darwin

1. Fix an odd prime  $p$  and a nontrivial  $p$ -th root of unity  $\zeta_p$ . Let  $L = \mathbf{Q}(\sqrt[p]{2}, \zeta_p)$ , which is the splitting field for  $T^p - 2$  over  $\mathbf{Q}$ . (The case  $p = 3$  is  $\mathbf{Q}(\sqrt[3]{2}, \omega)$ , which was discussed in class.) The group  $\text{Gal}(L/\mathbf{Q})$  is described in Example 8.6.3. Show the Galois orbit of  $\sqrt[p]{2} + \zeta_p$  has size  $[L : \mathbf{Q}]$ , so  $L = \mathbf{Q}(\sqrt[p]{2} + \zeta_p)$ .
2. Under the natural isomorphism  $\text{Gal}(\mathbf{Q}(\zeta_{15})/\mathbf{Q}) \cong (\mathbf{Z}/15\mathbf{Z})^\times$ , determine explicitly the subfields of  $\mathbf{Q}(\zeta_{15})$  which correspond to the subgroups  $\{a \bmod 15 : a \equiv 1 \pmod 3\} = \{1, 4, 7, 13 \bmod 15\}$  and  $\{a \bmod 15 : a \equiv 1 \pmod 5\} = \{1, 11 \bmod 15\}$  and what the Galois group of each of these fields over  $\mathbf{Q}$  is (as an abstract group).
3. Determine the Galois groups of the following polynomials over the indicated field. (First verify irreducibility of the polynomial!)
  - a)  $T^3 + 2T + 1$  over  $\mathbf{Q}$ ,
  - b)  $T^3 - 12T + 8$  over  $\mathbf{Q}$ ,
  - c)  $T^4 - 3$  over  $\mathbf{Q}(i)$ ,
  - d)  $T^5 + 20T + 16$  over  $\mathbf{Q}$ . (This polynomial is irreducible mod 13 and factors mod 7 as  $(T - 4)(T - 5)(T^3 + 2T^2 + 5T + 5) \pmod 7$ .)
4. Let  $n$  be a positive integer and  $p$  be a prime.
  - a) If  $p$  does not divide  $n$  and  $\Phi_n(T) \pmod p \in \mathbf{F}_p[T]$  is irreducible, show  $(\mathbf{Z}/n\mathbf{Z})^\times = \langle p \bmod n \rangle$ . In particular, the group  $(\mathbf{Z}/n\mathbf{Z})^\times$  must be cyclic. (Hint: Use Galois theory for finite fields.)
  - b) Use part a to prove the polynomial  $\Phi_8(T) = T^4 + 1$  is reducible modulo  $p$  for *all* primes  $p$ .