

MATH113 PROBLEMS: HOMEWORK 8 (“DUE” TUESDAY, AUG. 14)

- (1) Suppose we have a tower of field extensions  $L \subset K \subset F$ , and suppose that  $F$  is algebraic over  $K$ , and  $K$  is algebraic over  $L$ . Prove that  $F$  is algebraic over  $L$ .
- (2) §6.2 #4 Construct a field  $K$  with nine elements, and find a cyclic generator of  $K^\times$ .
- (3) §6.2 #6 Determine all the finite subgroups of  $\mathbb{C}^\times$ .
- (4) Let  $F$  be a field, and let  $\alpha$  and  $\beta$  have minimal polynomials  $p_\alpha$  and  $p_\beta$ , in  $F[x]$ , respectively. It is **NOT TRUE** that  $F(\alpha) \simeq F(\beta)$  if and only if  $p_\alpha = p_\beta$ .
  - (a) Show that over  $\mathbb{Q}$ , the algebraic numbers  $\sqrt{3}$  and  $\sqrt{3} + 1$  have different minimal polynomials, but generate the same extension of  $\mathbb{Q}$ .
  - (b) Show that  $f = x^3 + x^2 + 1$  and  $g = x^3 + x + 1$  are irreducible over  $\mathbb{F}_2$ . If  $\alpha$  is a root of  $f$ , and  $\beta$  is a root of  $g$ , show that  $\mathbb{F}_2(\alpha) \simeq \mathbb{F}_2(\beta)$ , even though  $\alpha$  and  $\beta$  have different minimal polynomials.
  - (c) Here’s a **correct statement**: Let  $F$  be a field. Let  $\alpha$  and  $\beta$  be algebraic over  $F$  with minimal polynomials  $p_\alpha$  and  $p_\beta$ . Show that  $p_\alpha = p_\beta$  if and only if there is an isomorphism  $\phi : F(\alpha) \rightarrow F(\beta)$  with  $\phi(\alpha) = \beta$  and  $\phi(a) = a$  for all  $a \in F$ .
- (5) Let  $q = p^n$  with  $p$  prime and  $n \geq 1$ . In this problem we find the subfields of  $\mathbb{F}_q$ .
  - (a) Show that if  $a|b$  then  $x^a - 1 | x^b - 1$  in  $\mathbb{Z}[x]$
  - (b) Let  $q' = p^m$  with  $m|n$ . Show that  $q' - 1 | q - 1$ .
  - (c) Show  $x^{q'} - x$  divides  $x^q - x$ , and conclude that  $\mathbb{F}_q$  contains  $\mathbb{F}_{q'}$  as a subfield.
  - (d) By considering degrees over  $\mathbb{F}_p$ , show that the subfields  $\mathbb{F}_{q'}$  from part (c) are the only subfields of  $\mathbb{F}_q$ .