

### HOMEWORK 3-4. DUE FRIDAY APRIL 25

HAND IN: 7.3.9, 7.3.11, 7.3.13, 7.4.1, 7.4.3.

AND

1. For the following polynomials in  $\mathbb{Z}_2[x]$ , prove:  
 $x^5 + x + 1$  is reducible. (Use trial and error.)  
 $x^5 + x^2 + 1$  is irreducible. (Use trial and error.)
2. Compute the number of all monic irreducible polynomials of degree 3 over  $\mathbb{Z}_p$  (Hint: use the factorization of  $F_3 = x^{p^3} - x$ ).
3. Find the minimal polynomials of  $\sqrt{1 + \sqrt{5}}$  and of  $i\sqrt{5} - \sqrt{3}$  over  $\mathbb{Q}$ .
4. (i) Prove:  $\mathbb{Q}(\sqrt{2}) \not\cong \mathbb{Q}(\sqrt{3})$ .  
(ii) Find a basis of  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  over  $\mathbb{Q}$ . Prove that it's a basis.
5. Prove  $\mathbb{Q}(\sqrt{p}, \sqrt{q}) = \mathbb{Q}(\sqrt{p} + \sqrt{q})$  for any distinct primes  $p$  and  $q$ .
- 6\* (**Bonus problem**). Let  $K \subset L$  be a field extension.  
(i) Assume that  $a, b \in L$  are algebraic over  $K$ , and that their minimal polynomials  $f$  and  $g$  over  $K$  have degrees  $m$  and  $n$ , respectively. Prove: IF  $m$  and  $n$  are relatively prime then  $\dim_K K(a, b) = mn$ .  
(ii) Give an example to show that this is false if  $m$  and  $n$  are not relatively prime.  
(iii) In (i) prove that  $f$  is irreducible over  $K(b)$ .

DO NOT HAND IN: 7.3.8, 7.3.10, 7.3.12, 7.4.2

AND

7. Prove: for any integers  $n_1, \dots, n_k$ ,  $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{n_1}, \dots, \sqrt{n_k}) \leq 2^k$ .
8. Let  $u \in \mathbb{C}$  be an algebraic number whose minimal polynomial has odd degree. Prove:  $\mathbb{Q}(u^2) = \mathbb{Q}(u)$ .
9. Let  $\mathbb{Q} \subset K \subset \mathbb{C}$  for a field  $K$  such that  $\dim_{\mathbb{Q}}(K) = 2$ . Prove:  $K = \mathbb{Q}(\sqrt{d})$  where  $d$  is a square-free integer (i.e., if a prime  $p$  divides  $d$  then  $p^2$  does not divide  $d$ ).
10. (i) Prove: the intersection of any collection of subfields is a subfield.

DEFINITION: If  $K \subseteq L$  are fields and  $S$  is any nonempty subset of  $L$ , then  $K(S)$ , the *subfield generated by  $S$* , is defined to be the intersection of all subfields of  $L$  containing  $S$ . Here  $K(S)$  is also called the subfield of  $L$  obtained by *adjoining* the members of  $S$ .

Abbreviation:  $K(\alpha_1, \dots, \alpha_n) = K(\{\alpha_1, \dots, \alpha_n\})$ .

(ii) Prove:  $(K(S))(T) = K(S \cup T)$  for any subsets  $S$  and  $T$  of  $L$ . (Here  $K(S)$  is a field, to which we adjoin a set  $T$  of elements.)

(iii) Deduce:  $K(\alpha_1, \dots, \alpha_n) = (K(\alpha_1, \dots, \alpha_{n-1}))(\alpha_n)$ , showing how *successive adjunctions* of elements fit together.

(iv) Prove:  $K(S)$  is isomorphic to the field of fractions of the **subring** of  $L$  generated by  $S$ . (For example, take  $L = K(x)$  and  $S = \{x\}$ .)