

Tenth Week's Assignments

Final exam: The final examination for Math 100C will be given on Wednesday, June 13, 11:30 AM - 2:30 PM in the lecture room HSS 2321. The exam will be closed book, and will cover the entire course.

Reading in the text: Read Section 14.4, look over pp. 196 - 198 (on solvable groups), and look over Sec. 14.7. (We will discuss Galois' result on solvability of polynomials by radicals, but will not have time to work through the proof fully.)

Homework problems, due Friday, June 8:

1. Let  $F \subseteq L \subseteq K$  be fields with  $K$  Galois over  $F$ . Let  $G = \mathcal{G}(K/F)$ , and let  $H = \mathcal{G}(K/L) \subseteq G$ . We know from the Fundamental Theorem that  $L$  is Galois over  $F$  if and only if  $H$  is normal in  $G$ . This problem describes what happens when  $L$  may not be Galois over  $F$ . Let  $E = \mathcal{F}(\mathcal{G}(L/F))$ , so  $E$  is a field, with  $F \subseteq E \subseteq L$ . Let  $N = \mathcal{G}(K/E)$ , the subgroup of  $G$  corresponding to  $E$  in the Galois correspondence.

(a) Prove that  $N = N_G(H) = \{ \tau \in G \mid \tau H \tau^{-1} = H \}$ . Recall that  $N_G(H)$  is the normalizer of  $H$  in  $G$ , which is the largest subgroup of  $G$  in which  $H$  is a normal subgroup.

(b) Prove that  $\mathcal{G}(L/F) = \mathcal{G}(L/E) \cong N/H$ .

2. Let  $p$  be an odd prime number. In number theory, it is often of interest to determine whether a given integer  $n$  prime to  $p$  is a *quadratic residue mod  $p$* , i.e., whether there is an integer solution  $x$  to the congruence equation  $x^2 \equiv n \pmod{p}$ . Restated,  $n$  is a quadratic residue *mod  $p$*  just when the image  $\bar{n} = n + (p)$  of  $n$  in the multiplicative group  $(\mathbb{Z}/p\mathbb{Z})^*$  of the field  $\mathbb{Z}/p\mathbb{Z}$  lies in  $(\mathbb{Z}/p\mathbb{Z})^{*2}$ . In some sense this occurs "half the time;" for, since  $(\mathbb{Z}/p\mathbb{Z})^*$  is a cyclic group of even order  $p - 1$ , its subgroup of squares is its unique subgroup of order  $(p - 1)/2$ , so of index 2. (You can see this by noting that the squaring map  $(\mathbb{Z}/p\mathbb{Z})^* \rightarrow (\mathbb{Z}/p\mathbb{Z})^*$  is a group homomorphism with kernel the unique subgroup of order 2.) To facilitate analyzing quadratic residues, one defines the *Legendre symbol*,  $\left(\frac{n}{p}\right)$ , according to the rule (for  $n \in \mathbb{Z}$  with  $p \nmid n$ ):

$$\left(\frac{n}{p}\right) = \begin{cases} 1, & \text{if } n \text{ is a quadratic residue mod } p, \text{ i.e., } \bar{n} \in (\mathbb{Z}/p\mathbb{Z})^{*2}, \\ -1, & \text{if } n \text{ is a quadratic nonresidue mod } p, \text{ i.e., } \bar{n} \notin (\mathbb{Z}/p\mathbb{Z})^{*2}. \end{cases}$$

Note that the Legendre symbol is multiplicative in  $n$ , i.e., that if  $n, m \in \mathbb{Z}$  with each of them prime to  $p$ , then  $\left(\frac{nm}{p}\right) = \left(\frac{n}{p}\right)\left(\frac{m}{p}\right)$ . (In particular, this says that the product of two nonsquares *mod  $p$*  is a square *mod  $p$* .) This holds because the map  $n \mapsto \left(\frac{n}{p}\right)$  is the composition of the maps  $\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$ ,  $(\mathbb{Z}/p\mathbb{Z})^* \rightarrow (\mathbb{Z}/p\mathbb{Z})^*/(\mathbb{Z}/p\mathbb{Z})^{*2}$ , and  $(\mathbb{Z}/p\mathbb{Z})^*/(\mathbb{Z}/p\mathbb{Z})^{*2} \rightarrow \{1, -1\}$ , each of which is multiplicative. For example, we have  $\left(\frac{-1}{p}\right) = 1$  if  $p \equiv 1 \pmod{4}$ , while  $\left(\frac{-1}{p}\right) = -1$  if  $p \equiv 3 \pmod{4}$ . This holds because  $-1$  (the unique element of order 2 in  $(\mathbb{Z}/p\mathbb{Z})^*$ ) is a square in  $(\mathbb{Z}/p\mathbb{Z})^*$  iff this cyclic group contains an element of order 4, which occurs iff  $4 \mid |(\mathbb{Z}/p\mathbb{Z})^*| = p - 1$ . Restated,  $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$ . Because the Legendre symbol is multiplicative, to compute  $\left(\frac{n}{p}\right)$ , it suffices to know  $\left(\frac{q}{p}\right)$  for each prime number  $q$  dividing  $n$ . For this, one has the *law of quadratic reciprocity*, which is one of the really amazing facts of number theory. The law of quadratic reciprocity, discovered by Euler and first proved by Gauss, says that for odd primes  $p$  and  $q$ , we have  $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$  if  $p \equiv 1 \pmod{4}$  or  $q \equiv 1 \pmod{4}$ , while  $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$  if  $p \equiv 3 \pmod{4}$  and  $q \equiv 3 \pmod{4}$ . (Restated, in the first case  $q$  is a quadratic residue *mod  $p$*  iff  $p$  is a quadratic residue *mod  $q$* . In the second case,  $q$  is a quadratic residue *mod  $p$*  iff  $p$  is a quadratic nonresidue *mod  $q$* .) That is,

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4}.$$

It is quite a surprise that such a formula exists. (Why should the question whether  $\bar{q}$  is a square in  $\mathbb{Z}/p\mathbb{Z}$  be related at all to whether  $\bar{p}$  is a square in  $\mathbb{Z}/q\mathbb{Z}$ ?)

There are many proofs of the law of quadratic reciprocity. The next problem shows one way it can be proved, using Galois theory. For this, consider a splitting field of  $K$  of  $x^q - 1$  over  $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ , and let  $r = [K : \mathbb{F}_p]$ , so  $K = \mathbb{F}_{p^r}$ . Since  $K = \mathbb{F}_p(\omega)$ , where  $\omega$  is a primitive  $q$ -th root of unity,  $K$  must be the smallest field extension of  $\mathbb{F}_p$  which contains a primitive  $q$ -th root of unity, which is an element of order  $q$  in its multiplicative group. But for a field  $L \supseteq \mathbb{F}_p$ , if  $[L : \mathbb{F}_p] = t$ , then  $L^*$  is a cyclic group of order  $p^t - 1$ , so it contains an element of order  $q$  iff  $q \mid (p^t - 1)$ . Since  $K$  is the smallest field with this property, we must have  $[K : \mathbb{F}_p] = r$ , where  $r$  is the least positive integer such that  $q \mid (p^r - 1)$ . Note that this condition on  $r$  is equivalent to saying that  $r$  is the order of  $\bar{p} = p + (q)$  in the multiplicative group  $(\mathbb{Z}/q\mathbb{Z})^*$  of the field  $\mathbb{Z}/q\mathbb{Z}$ . Therefore, in particular,  $r \mid (q - 1)$  since  $|(\mathbb{Z}/q\mathbb{Z})^*| = q - 1$  (as the order of an element divides the order of the group). Let  $q - 1 = rs$ . (Observe that this already gives a connection between one thing concerning  $\mathbb{Z}/p\mathbb{Z}$  and another concerning  $\mathbb{Z}/q\mathbb{Z}$ .)

- Prove that  $\bar{p} \in (\mathbb{Z}/q\mathbb{Z})^{*2}$  iff the order  $r$  of  $\bar{p}$  in the (cyclic) group  $(\mathbb{Z}/q\mathbb{Z})^*$  divides  $(q - 1)/2$ , iff  $2 \mid s$ . Restated,  $\left(\frac{p}{q}\right) = (-1)^s$ . (Recall that  $(\mathbb{Z}/q\mathbb{Z})^{*2}$  is the unique subgroup of  $(\mathbb{Z}/q\mathbb{Z})^*$  of order  $(q - 1)/2$ .)
- We have  $x^q - 1 = (x - 1)\overline{\Phi}_q$ , where  $\overline{\Phi}_q$  is the image in  $\mathbb{F}_p[x]$  of the cyclotomic polynomial  $\Phi_q$ , and the roots of  $\overline{\Phi}_q$  in  $\mathbb{F}_{p^r}$  are the  $q - 1$  primitive  $q$ -th roots of unity. Prove that the irreducible factorization of  $\overline{\Phi}_q$  in  $\mathbb{F}_p[x]$  consists of  $s$  different irreducible monic factors, each of degree  $r$ .
- Let  $\tau$  be a generator of the cyclic Galois group  $\mathcal{G}(\mathbb{F}_{p^r}/\mathbb{F}_p)$  (We could take  $\tau$  to be the map  $\alpha \mapsto \alpha^p$ , but that specific description of  $\tau$  does not seem to be helpful here.) If  $\alpha_1, \dots, \alpha_q$  are the roots of  $x^q - 1$  in  $\mathbb{F}_{p^r}$ , (say with  $\alpha_1 = 1$  and  $\alpha_2, \dots, \alpha_q$  being the primitive  $q$ -th roots of unity), recall from last week's homework that we have an injective group homomorphism  $\psi: \mathcal{G}(\mathbb{F}_{p^r}/\mathbb{F}_p) \rightarrow S_q$  given by:  $\psi(\rho)$  is the permutation  $\sigma$  such that  $\rho(\alpha_i) = \alpha_{\sigma(i)}$  for  $1 \leq i \leq q$ . Prove that the disjoint cycle decomposition of  $\psi(\tau)$  in the symmetric group  $S_q$  consists of  $s$  cycles, each of length  $r$ . (Hint: For any primitive  $q$ -th root of unity  $\omega$ , note that  $\tau^j(\omega)$  is a root of  $m_{\mathbb{F}_p, \omega}$ , and show that since  $\mathbb{F}_{p^r} = \mathbb{F}_p(\omega)$  if  $\tau^j(\omega) = \omega$ , then  $\tau^j = \text{id}$ .)
- Deduce that  $\psi(\mathcal{G}(\mathbb{F}_{p^r}/\mathbb{F}_p)) \subseteq A_q$  (the alternating group in  $S_q$ ) iff  $\psi(\tau)$  is an even permutation, iff  $s$  is an even number. (Note that  $r$  and  $s$  cannot both be odd numbers since  $rs = q - 1$ .)
- Let  $D$  be the discriminant of  $x^q - 1 \in \mathbb{F}_p[x]$ , as defined in last week's problem set. Recall that  $D \in \mathbb{F}_p^{*2}$  iff  $\psi(\mathcal{G}(\mathbb{F}_{p^r}/\mathbb{F}_p)) \subseteq A_q$ . Note that the calculation of the discriminant of  $x^q - 1$  you made in last week's problem 3(b) (with  $\mathbb{Q}$  as base field) applies here also with base field  $\mathbb{F}_p$ . Deduce that  $\left(\frac{(-1)^{(q-1)/2}q}{p}\right) = (-1)^s$ .
- Deduce that  $\left(\frac{q}{p}\right) \left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4}$ .

Note: To complete the picture, we need a formula for  $\left(\frac{2}{p}\right)$  for any odd prime number  $p$ . In fact,  $\left(\frac{2}{p}\right) = 1$  if  $p \equiv 1 \pmod{8}$  or  $p \equiv 7 \pmod{8}$ , while  $\left(\frac{2}{p}\right) = -1$  if  $p \equiv 3 \pmod{8}$  or  $p \equiv 5 \pmod{8}$ . Here is a proof of this: The basic approach is to find a field containing  $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$  which contains a square root of 2, and then to analyze when that root lies in  $\mathbb{F}_p$ . We can see how to find such a field by noting that the formula for the primitive 8-th roots of unity in  $\mathbb{C}$  (they are  $\frac{\sqrt{2}}{2}(\pm 1 \pm \sqrt{-1})$ ) is also valid in an extension field of  $\mathbb{F}_p$ . Let  $K = \mathbb{F}_p(\omega)$ , where  $\omega$  is a primitive 8-th root of unity. Let  $i = \omega^2$ , which is a primitive 4-th root of unity, so  $i^2 = \omega^4 = -1$ , since  $-1$  is the unique square root of unity. Let  $\beta = \omega + \omega^{-1} \in K$ . Note that

$$\beta^2 = \omega^2 + 2 + \omega^{-2} = (\omega^4 + 1)\omega^{-2} + 2 = (-1 + 1)\omega^{-2} + 2 = 2.$$

So, the square roots of 2 in  $K$  are  $\beta$  and  $-\beta$ . Thus,  $\left(\frac{2}{p}\right) = 1$  iff  $\beta \in \mathbb{F}_p$ . This holds iff  $\beta^p = \beta$ , since  $\mathbb{F}_p = \{\alpha \in K \mid \alpha^p = \alpha\}$ . (This is the case  $d = 1$  of our description of  $\mathbb{F}_{p^d}$  as the set of roots of  $x^{p^d} - x$  for any  $d \in \mathbb{N}$ .) We have  $\beta^p = (\omega + \omega^{-1})^p = \omega^p + \omega^{-p}$ , since  $\text{char}(K) = p$ . If  $p \equiv 1 \pmod{8}$ , then  $\omega^p = \omega$ , since  $\omega^8 = 1$ ; so,  $\beta^p = \beta$ , showing  $\beta \in \mathbb{F}_p$ , hence  $\left(\frac{2}{p}\right) = 1$ . If  $p \equiv 7 \pmod{8}$ , then  $\omega^p = \omega^7 = \omega^{-1}$ , so  $\beta^p = \omega^{-1} + \omega = \beta$ , showing again that  $\beta \in \mathbb{F}_p$  and that  $\left(\frac{2}{p}\right) = 1$ . However, if  $p \equiv 3 \pmod{8}$ , then  $\omega^p = \omega^3$ ,

so  $\beta^p = \omega^3 + \omega^{-3} = \omega^4(\omega^{-1} + \omega^{-7}) = -(\omega^{-1} + \omega) = -\beta \neq \beta$ ; so  $\beta \notin \mathbb{F}_p$  and  $\left(\frac{2}{p}\right) = -1$ . Finally, if  $p \equiv 5 \pmod{8}$ , then  $\beta^p = \omega^5 + \omega^{-5} = \omega^4(\omega + \omega^{-9}) = -(\omega + \omega^{-1}) = -\beta$ ; so, again  $\beta \notin \mathbb{F}_p$  and  $\left(\frac{2}{p}\right) = -1$ .

3. Let  $G$  be group, and let  $H$  and  $N$  be subgroups of  $G$ , with  $N$  a normal subgroup of  $G$ . Suppose that  $N \cap H = (e)$ ,  $G = NH$ , and  $N$  is a cyclic group.

- Prove that every element  $a \in G$  has a unique expression in the form  $a = nh$ , where  $n \in N$  and  $h \in H$ .
- Let  $B$  be a subgroup of  $N$ . Prove that  $hBh^{-1} = B$ , for every  $h \in H$ ; deduce that  $BH$  is a subgroup of  $G$ , and that  $BH \cap N = B$ .
- Let  $A$  be any subgroup of  $G$  such that  $H \subseteq A$ . Prove that  $A = (A \cap N)H$ . (This, with part(b) shows that there is a one-to-one correspondence between the subgroups of  $G$  containing  $H$  and the subgroups of  $N$ .)

Notes: (i) If we do not want to assume that  $N$  is cyclic (but keeping the other hypotheses in problem 3), the result is that there is a one-to-one correspondence between subgroups of  $G$  containing  $H$  and subgroups  $B$  of  $N$  such that  $hBh^{-1} = B$ , for all  $h \in H$ , i.e.,  $H$  normalizes  $B$ .

(ii) Note that for the  $N$  and  $H$  of problem 3, we have that  $G/N = NH/H \cong H/(H \cap N) \cong H$ , using the Second Isomorphism Theorem. Therefore since we know from the Lattice Isomorphism Theorem that the subgroups of  $G$  containing  $N$  are in one-to-one correspondence with those of  $G/N$ , and these groups are in one-to-one correspondence with the subgroups of  $H$ . (If  $C$  is a subgroup of  $G$  containing  $N$ , then  $C = N(C \cap H)$ , and the corresponding subgroup of  $H$  is  $C \cap H$ .) However, since  $H$  need not be normal in  $G$ , we do not have the isomorphism theorems to assist us in analyzing the subgroups of  $G$  containing  $H$ . While we can see that every such subgroup has the form  $BH$  where  $B$  is a subgroup of  $N$ , one needs to check whether  $BH$  is actually a subgroup of  $G$ . This is true in the setting of problem 3 as a consequence of the further assumption on  $N$  that it is cyclic.

(iii) In the situation described in problem 3, when we have subgroups  $H$  and  $N$  of a group  $G$  such that  $N$  is normal in  $G$ ,  $G = NH$ , and  $N \cap H = (e)$ , then  $G$  is said to be a *semidirect product* of  $N$  by  $H$ . Recall that if  $H$  is also normal in  $G$ , then  $G \cong N \times H$ , a direct product. But here, we are not assuming the normality of  $H$ . Note, however, that since  $N$  is normal in  $G$ , we have a well-defined group homomorphism  $\theta: H \rightarrow \text{Aut}(N)$  (the group of automorphisms of  $N$ ) given by  $\theta(h)(n) = hnh^{-1}$ . Then, the group is completely determined by  $N$  and  $H$  and  $\theta$ . For, if we take two elements  $a, a' \in G$  and write them in the form  $a = nh$ ,  $a' = n'h'$  with  $n, n' \in N$  and  $h, h' \in H$ , then the expression for their product in this form is:  $aa' = (nh)(n'h') = n(hn'h^{-1})hh' = [n\theta(h)(n')](hh')$ .

4. Let  $F$  be a field, and let  $n \in \mathbb{N}$  with  $\text{char}(F) \nmid n$  and  $n > 1$ . Let  $f = x^n - c \in F[x]$ , and assume  $f$  is irreducible in  $F[x]$ . Let  $K$  be a splitting field of  $f$  over  $F$ . So,  $K$  is Galois over  $F$ , as the derivative test shows  $f$  has no repeated roots. Let  $G = \mathcal{G}(K/F)$ . Let  $\alpha$  be any root of  $f$ , and let  $\omega$  be a primitive  $n$ -th root of unity. Then, the roots of  $f$  are  $\alpha, \alpha\omega, \dots, \alpha\omega^{n-1}$ , so  $K = F(\alpha, \alpha\omega, \dots, \alpha\omega^{n-1}) = F(\alpha, \omega)$ . Let  $H = \mathcal{G}(K/F(\alpha)) \subseteq G$  and  $N = \mathcal{G}(K/F(\omega)) \subseteq G$ . Since  $K$  is generated by  $\omega$  over  $F(\alpha)$ , (so,  $K$  is a splitting field of  $x^n - 1$  over  $F(\alpha)$ ), we know from last week's problem 2 that  $H$  is isomorphic to a subgroup of the multiplicative group  $(\mathbb{Z}/n\mathbb{Z})^*$ . Hence,  $H$  is abelian and  $|H| \mid \varphi(n)$ . Also, since  $K$  is a splitting field of  $x^n - c$  over  $F(\omega)$ , we know from last week's problem 4 that  $N$  is isomorphic to a subgroup of the additive group of  $\mathbb{Z}/n\mathbb{Z}$ , (using the map  $N \rightarrow \mathbb{Z}/n\mathbb{Z}$  taking  $\tau \in N$  to  $i + (n)$ , where  $\tau(\alpha) = \alpha\omega^i$ ). So  $N$  is a cyclic group of order, say  $k$ , with  $k \mid n$ . We saw further in last week's problem 4 that  $k$  is the least positive integer such that  $\alpha^k \in F(\omega)$ . Also, as  $F(\omega)$  is Galois over  $F$ , the Fundamental Theorem tells us that  $N$  is normal in  $G$  and that  $G/N \cong \mathcal{G}(F(\omega)/F)$ , which is also isomorphic to a subgroup of  $(\mathbb{Z}/n\mathbb{Z})^*$ . Note further that, since the Galois correspondence is inclusion reversing and involves all the subgroups of  $G$  and all the fields  $L$  with  $F \subseteq L \subseteq K$ , the field corresponding to  $H \cap N$  must be the smallest subfield of  $K$  containing both  $F(\alpha)$  and  $F(\omega)$ , which is  $K$  itself. Hence,  $H \cap N = \mathcal{G}(K/K) = \{id\}$ . Likewise,

since  $NH$  (which is a group, as  $N$  is normal in  $G$ ) is the smallest subgroup of  $G$  containing both  $H$  and  $N$ , its corresponding field must be the largest subfield of  $K$  lying in both  $F(\alpha)$  and  $F(\omega)$ ; that is,  $\mathcal{F}(HN) = F(\alpha) \cap F(\omega)$ , and  $HN = \mathcal{G}(K/(F(\alpha) \cap F(\omega)))$ .

- (a) Prove that for each  $d \in \mathbb{N}$  with  $d \mid n$ , we have  $[F(\alpha) : F(\alpha^d)] = d$ . Likewise, if  $d \mid k$  prove that  $[F(\omega, \alpha) : F(\omega, \alpha^d)] = d$ .
- (b) Prove that  $F(\alpha) \cap F(\omega) = F(\alpha^k)$ . (Hint: Show that  $\deg(m_{F(\omega), \alpha}) \leq \deg(m_{F(\alpha) \cap F(\omega), \alpha})$ ; use this and part (a) to compare the degree of  $F(\alpha)$  over the fields of interest.) It follows from the comments above that  $\mathcal{G}(K/F(\alpha^k)) = NH$ , and that this group and its subgroups  $H$  and  $N$  satisfy the conditions of problem 3 above.
- (c) Prove that the only fields  $L$  with  $F(\alpha^k) \subseteq L \subseteq F(\alpha)$  are  $L = F(\alpha^m)$  for  $m \mid k$ . (Hint: Use problem 3 above.)
- (d) Prove that there is  $\sigma \in G$  with  $\sigma(\alpha) = \omega\alpha$ .
- (e) Prove that for the  $\sigma$  of part (d), and for any  $\tau \in H$  with  $\tau \neq id$ , we have  $\tau\sigma \neq \sigma\tau$ . (Hint: Look at what these automorphisms do to  $\alpha$ .) Clearly, this implies that  $H \cap Z(G) = \{id\}$ , where  $Z(G)$  denotes the center of  $G$ . (It follows that if  $G$  is abelian, then  $|H| = 1$ , i.e.,  $F(\omega) \subseteq F(\alpha) = K$ . However, the converse is not true, e.g., for  $F = \mathbb{Q}$ ,  $f = x^6 + 3$ ; then  $K = F(\alpha)$ ,  $n = 6$ ,  $k = 3$ , and  $|H| = 1$ , as  $\mathbb{Q}_6 = \mathbb{Q}(\sqrt{-3}) \subseteq \mathbb{Q}(\alpha)$ , but  $G \cong S_3$ .)
- (f) When  $k = n$ , then  $F(\alpha^k) = F(\alpha^n) = F$ , and part (c) gives a classification of all the fields between  $F$  and  $F(\alpha)$ . The case  $k = n$  is also of interest because then  $F(\alpha) \cap F(\omega) = F$ , so that  $NH$  is the entire Galois group  $G = \mathcal{G}(K/F)$ . Then all of  $G$  is determined by  $N$ ,  $H$ , and the conjugation action of  $H$  on  $N$ , as noted in (iii) above. Furthermore, then (and only then), we have  $H \cong \mathcal{G}(F(\omega)/F)$ . The final parts of this problem will give us many examples when we will be able to prove that  $k = n$ . At present, we only know that  $k \mid n$ . Let  $g = x^{n/k} - c \in F[x]$ , let  $\zeta$  be a primitive  $n/k$ -th root of unity, and let  $K_0 = F(\alpha^k, \zeta)$ , which is a splitting field of  $g$  over  $F$ . Prove that  $g$  is irreducible in  $F[x]$ , so the preceding parts of this problem apply, with  $n/k$  replacing  $n$ ,  $g$  replacing  $f$ ,  $\alpha^k$  replacing  $\alpha$ ,  $\zeta$  replacing  $\omega$ , and  $K_0$  replacing  $K$ . Prove that  $K_0 \subseteq F(\omega)$ , and deduce that  $\mathcal{G}(K_0/F)$  is abelian. Deduce from this (using part(e)) that  $F(\zeta) \subseteq F(\alpha^k)$ .
- (g) Suppose that  $n$  is odd and  $F = \mathbb{Q}$ . Prove that  $k = n$ . (Hint: Apply part (f) and recall that  $\varphi(\ell)$  is even for  $\ell \geq 3$ .)

Notes. (i) In the setting of problem 4(g), it is necessary to assume that  $n$  is odd. The example in part (e) is one illustration of this. For another example, let  $f = x^{10} - 5 \in \mathbb{Q}[x]$ . Then,  $\mathbb{Q}_{10} \cap \mathbb{Q}(\sqrt[10]{5}) = \mathbb{Q}(\sqrt{5})$ , so  $k = 5$  while  $n = 10$ . You can show with a little more effort that (for  $F = \mathbb{Q}$ ) if  $n$  is even, then  $n/k$  is a power of 2. For example, if  $f = x^{2^m} + 1$  (a cyclotomic polynomial) then  $n = 2^m$  and  $k = 1$ . However, if  $f = x^n - c \in \mathbb{Q}[x]$  with  $c > 0$ , you can show that  $n/k = 2$  or  $= 1$ .

(ii) The only fields between  $F(\alpha^k)$  and  $F(\alpha)$  are the “obvious” fields  $F(\alpha^m)$  for  $m \mid k$ , as you proved for part (d). However, when  $k < n$  there can be some further fields  $L$  with  $F \subseteq L \subseteq F(\alpha)$  besides  $F(\alpha^\ell)$  for  $\ell \mid n$ . This is illustrated in the example of part (e), where  $F = \mathbb{Q}$  and  $f = x^6 + 3$ , so  $K = \mathbb{Q}(\alpha)$ , where  $\alpha^6 = -3$ . Here,  $K$  contains three different fields of degree 3 over  $\mathbb{Q}$ , namely  $\mathbb{Q}(\alpha^2)$ ,  $\mathbb{Q}(\alpha^2\omega^2)$ , and  $\mathbb{Q}(\alpha^2\omega^4)$ , generated by the three different cube roots of  $-3$ . These fields are different, since none contains a primitive cube root of unity, (as  $[\mathbb{Q}(\omega^2) : \mathbb{Q}] = \varphi(3) = 2$ ).

(iii) Recall problem 3 of week 7 in which you showed that the only field  $L$  with  $\mathbb{Q} \subsetneq L \subsetneq \mathbb{Q}(\sqrt[4]{8})$  is  $\mathbb{Q}(\sqrt{8})$ . This can now be verified as a special case of problem 4 above with  $F = \mathbb{Q}$ ,  $n = 4$ , and  $a = 8$ , so  $f = x^4 - 8$ , which we know is irreducible in  $\mathbb{Q}[x]$ , and  $\alpha = \sqrt[4]{8} \subseteq \mathbb{R}$ . Since  $n = 4$ , we have  $\omega = i = \sqrt{-1} \subseteq \mathbb{C}$ . Because  $\mathbb{Q}(i) \cap \mathbb{R} = \mathbb{Q}$ , we can see that  $\alpha \notin \mathbb{Q}(i)$  and  $\alpha^2 = \sqrt{8} \notin \mathbb{Q}(i)$ . (For  $\alpha$  and  $\alpha^2$  lie in  $\mathbb{R}$  but not in  $\mathbb{Q}$ .) Hence, for our  $k$  which we know divides  $n = 4$ , we do not have  $k = 1$  or  $k = 2$ , so we must have  $k = 4 = n$ . Therefore, part (c) of problem 4 determines all the subfields of  $\mathbb{Q}(\sqrt[4]{8})$  containing  $\mathbb{Q}$ , and shows

that the only one besides  $\mathbb{Q}$  and  $\mathbb{Q}(\sqrt[4]{8})$  is  $\mathbb{Q}(\sqrt{8})$ .

(iv) Throughout problem 4, it was assumed that  $x^n - c$  was irreducible in  $F[x]$ . It can be shown that  $x^n - c$  is irreducible in  $F[x]$  iff  $c \notin F^p$  for each prime number  $p \mid n$  and (if  $4 \mid n$ )  $-4c \notin F^4$ . So, for example, if  $F = \mathbb{Q}$ , you can read off immediately from the prime factorization of  $c$  for exactly which  $n$  we have  $x^n - c$  is irreducible in  $\mathbb{Q}[x]$ .

Optional problems:

1. Let  $\alpha \in \mathbb{R}$ . Recall that  $\alpha$  is said to be a constructible number if there are fields  $\mathbb{Q} = F_0 \subseteq F_1 \subseteq \dots \subseteq F_k \subseteq \mathbb{R}$  such that  $[F_i : F_{i-1}] \leq 2$  for each  $i$ ,  $1 \leq i \leq k$ , and  $\alpha \in F_k$ . As we have seen, it follows easily from this that if  $\alpha$  is constructible, then  $\alpha$  is algebraic over  $\mathbb{Q}$  and  $[\mathbb{Q}(\alpha) : \mathbb{Q}]$  is a power of two. But, the condition on  $[\mathbb{Q}(\alpha) : \mathbb{Q}]$  is not sufficient to guarantee that  $\alpha$  is constructible. Prove that the following conditions are equivalent:

- (i)  $\alpha$  is constructible.
- (ii)  $\alpha$  is algebraic over  $\mathbb{Q}$ , and for  $K$  a splitting field of  $m_{\mathbb{Q}, \alpha}$ , we have  $[K : \mathbb{Q}]$  is a power of 2.
- (iii) There is a field  $L \supseteq \mathbb{Q}$  with  $\alpha \in L$ ,  $L$  is Galois over  $\mathbb{Q}$ , and  $[L : \mathbb{Q}]$  is a power of 2.

2. Give an example of a real number  $\alpha$  such that  $[\mathbb{Q}(\alpha) : \mathbb{Q}]$  is a power of 2, but  $\alpha$  is not a constructible number.