

# MA553: Qual Preparation

Carlos Salinas

July 22, 2016

## Contents

|          |                                                             |           |
|----------|-------------------------------------------------------------|-----------|
| <b>1</b> | <b>MA 553 Spring 2016</b>                                   | <b>2</b>  |
| 1.1      | Homework . . . . .                                          | 2         |
| 1.1.1    | Homework 1 . . . . .                                        | 3         |
| 1.1.2    | Homework 2 . . . . .                                        | 5         |
| 1.1.3    | Homework 3 . . . . .                                        | 6         |
| 1.1.4    | Homework 4 . . . . .                                        | 7         |
| 1.1.5    | Homework 5 . . . . .                                        | 8         |
| 1.1.6    | Homework 6 . . . . .                                        | 9         |
| 1.1.7    | Homework 7 . . . . .                                        | 10        |
| 1.1.8    | Homework 8 . . . . .                                        | 11        |
| 1.1.9    | Homework 9 . . . . .                                        | 12        |
| 1.1.10   | Homework 10 . . . . .                                       | 13        |
| 1.1.11   | Homework 11 . . . . .                                       | 14        |
| 1.1.12   | Homework 12 . . . . .                                       | 15        |
| 1.1.13   | Homework 13 . . . . .                                       | 16        |
| <b>2</b> | <b>Ulrich</b>                                               | <b>17</b> |
| 2.1      | Ulrich: Winter 2002 . . . . .                               | 17        |
| <b>3</b> | <b>Field Theory and Galois Theory</b>                       | <b>20</b> |
| 3.1      | Roots and irreducibles . . . . .                            | 20        |
| 3.1.1    | Roots in larger fields . . . . .                            | 20        |
| 3.1.2    | Divisibility and roots in $KX$ . . . . .                    | 21        |
| 3.2      | Raising to the $p$ th power in characteristic $p$ . . . . . | 22        |
| 3.3      | Roots of irreducibles in $F_pX$ . . . . .                   | 23        |

# 1 MA 553 Spring 2016

This is material from the course MA 533 as it was taught in the spring of 2016.

## 1.1 Homework

Most of the homework is Ulrich original (or as original as elementary exercises in abstract algebra can be). However, an excellent resource and one that I will often quote on these solutions is [3]. Other resources include [1] and (to a lesser extent) [2]. I may also cite Milne's *Group Theory*, *Field Theory*, and *Commutative Algebra: A Primer* notes, respectively, [4], [5], and (no reference for the last). Unless otherwise stated, whenever we quote a result, e.g., Theorem 1.1, it is understood to come from Hungerford's *Algebra*.

Throughout these notes

|                 |                                                                                                     |
|-----------------|-----------------------------------------------------------------------------------------------------|
| $\mathbb{R}$    | is the set of real numbers                                                                          |
| $\mathbb{C}$    | is the set of complex numbers                                                                       |
| $\mathbb{Q}$    | is the set of rational numbers                                                                      |
| $\mathbb{F}_q$  | is the finite field of order $q = p^n$ for some prime $p$                                           |
| $\mathbb{Z}$    | is the set of the integers                                                                          |
| $\mathbb{N}$    | is the set of the natural numbers $1, 2, \dots$                                                     |
| $k$             | is used to denote the base field with characteristic $\text{char } k$                               |
| $K, E, L$       | is used to denote field extensions over the base field $k$                                          |
| $Z_n$           | is the cyclic group of order $n$ not necessarily equal (but isomorphic) to $\mathbb{Z}/p\mathbb{Z}$ |
| $S_n$           | is the symmetric group on $\{1, \dots, n\}$                                                         |
| $A_n$           | is the alternating group on $\{1, \dots, n\}$                                                       |
| $D_n$           | is the dihedral group of order $n$                                                                  |
| $A \setminus B$ | is the set difference of $A$ and $B$ , that is, the complement of $A \cap B$ in $A$                 |
| $X \cong Y$     | means $X$ and $Y$ are isomorphic as groups, rings, $R$ -modules, or fields                          |

### 1.1.1 Homework 1

**Problem 1.** Let  $G$  be a group,  $a \in G$  an element of finite order  $m$ , and  $n$  a positive integer. Prove that

$$|a^n| = \frac{m}{(m, n)}.$$

**Solution.** ► Let  $\ell$  denote the order of  $a^n$ . Then  $\ell$  is the minimal power of  $a^n$  such that  $(a^n)^\ell = e$ . Now, observe that

$$\begin{aligned} (a^n)^{m/(m, n)} &= a^{nm/(m, n)} \\ &= a^{mn/(m, n)} \\ &= (a^m)^{n/(m, n)} \\ &= e^{n/(m, n)} \\ &= e. \end{aligned}$$

Thus  $\ell \leq m/(m, n)$ .

On the other hand, by Theorem 3.4 (iv) since  $(a^n)^\ell = a^{n\ell} = e$  and the order of  $a$  is  $m$ ,  $m \mid n\ell$  or, equivalently,  $mk = n\ell$  for some  $k \in \mathbb{Z}^+$ . Now, since  $(m, n) \mid m$  and  $(m, n) \mid n$ , we can represent  $m$  and  $n$  as the products  $(m, n)m'$  and  $(m, n)n'$ , respectively. Now, note that  $m' = m/(m, n)$  so we must show that  $m' \leq \ell$ . Putting all of this together, we have  $mk$

$$mk = (m, n)m'k = (m, n)n'\ell = n\ell$$

so

$$m'k = n'\ell.$$

Thus  $m' \mid n'\ell$  so either  $m' \mid n'$  or  $m' \mid \ell$ . But since we factored the  $(m, n)$  from  $m$  and  $n$ , it follows that  $(m', n') = 1$  so  $m' \mid \ell$ . Therefore  $m' \leq \ell$  and equality holds, that is,  $\ell = m/(m, n)$ . ◀

**Problem 2.** Let  $G$  be a group, and let  $a, b$  be elements of finite order  $m, n$  respectively. Show that if  $ba = ab$  and  $\langle a \rangle \cap \langle b \rangle = \{e\}$ , then  $|ab| = mn/(m, n)$ .

**Solution.** ► Let  $\ell$  denote the order of  $ab$ . Now, playing around with powers of  $ab$ , we have

$$\begin{aligned} (ab)^n &= a^n b^n \\ &= a^n \\ &\neq e \end{aligned}$$

since the order of  $a$  is  $m$  and  $n < m$ . Thus, by Problem 1,  $|a^n| = m/(m, n)$  so  $|ab| = mn/(m, n)$ . ◀

**Problem 3.** Let  $G$  be a group and  $H, K$  normal subgroups with  $H \cap K = \{e\}$ . Show that

- (a)  $hk = kh$  for every  $h \in H, k \in K$ .
- (b)  $HK$  is a subgroup of  $G$  with  $HK \cong H \times K$ .

**Solution.** ► (a) Suppose that  $H$  and  $K$  are normal in  $G$ . Then, for every  $g \in G$ ,  $gh = hg$  and  $gk = kg$  for any  $h \in H, k \in K$ . In particular, since  $H \subset G, h \in G$  so  $hk = kh$ .

(b) Consider the subset  $HK$  of  $G$  consisting of all products  $hk$  where  $h \in H, k \in K$ . First, we show that  $HK$  is closed under multiplication: Pick  $h_1k_1, h_2k_2 \in HK$  then  $h_1k_1h_2k_2 = h_1(k_1k_2)h_2 = h_1h_2(k_1k_2)$  is in  $HK$  since  $h_1h_2 \in H, k_1k_2 \in K$ . Moreover, since  $e \in H$  and  $e \in K, ee = e \in HK$ . Lastly, given  $hk \in HK, hkh^{-1}k^{-1} = (hkh^{-1})k^{-1} = kk^{-1} = e$  so  $HK$  is closed under taking inverses. Thus,  $HK$  is a subgroup of  $G$ .

To see that  $HK \cong H \times K$ , consider the map  $\varphi: HK \rightarrow (HK/K) \times (HK/H)$  given by  $\varphi(hk) = (\pi_K(h), \pi_H(k))$  where  $\pi_H: HK \rightarrow HK/H$  and  $\pi_K: HK \rightarrow HK/K$  are quotient maps. By the first (or second) isomorphism theorem,  $H \cong HK/H$  and  $K \cong HK/K$  so  $HK \cong H \times K$ . ◀

**Problem 4.** Show that  $A_4$  has no subgroup of order 6 (although  $6 \mid 12 = |A_4|$ ).

**Solution.** ► We proceed by contradiction. Suppose that  $A_4$  has a subgroup of order 6, call it  $H$ . Then, we claim that  $H$  must contain all elements  $\sigma^2$  where  $\sigma \in A$ .

*Proof of claim.* Since  $|H| = 6, [A_4 : H] = 2$  which implies that  $H$  is must be a normal subgroup of  $A_4$ . Now, consider the collection of  $G/H$  of right-cosets of  $H$  in  $G$ . By Theorem 5.4,  $G/H$  is a group with order  $|G/H| = 2$  so either  $\bar{\sigma} = \bar{e}$  or  $\bar{\sigma}^2 = \bar{e}$ . Thus,  $\sigma^2 \in H$ . ■

Thus,  $H$  must contain all of the squares in  $A_4$ . However, counting all of the elements in  $A_4$  and squaring them

$$\begin{array}{ll} (1)^2 = (1) & (123)^2 = (132) \\ (132)^2 = (123) & (124)^2 = (142) \\ (142)^2 = (124) & (134)^2 = (143) \\ (143)^2 = (134) & (234)^2 = (234) \\ (243)^2 = (243) & ((12)(34))^2 = (1) \\ ((13)(24))^2 = (1) & ((14)(23))^2 = (1) \end{array}$$

we see that there are a total of 9 squares (8 nontrivial ones) which exceeds the order of  $H$ . This is a contradiction therefore,  $G$  has no subgroup of order 6. ◀

### 1.1.2 Homework 2

**Problem 1.** Let  $G$  be the group of order  $2^n \cdot 3$ ,  $n \geq 2$ . Show that  $G$  has a normal 2-subgroup  $\neq \{e\}$ .

**Solution.** ► Suppose that  $|G| = 2^n \cdot 3$ . By the first Sylow theorem,  $G$  contains a 2-Sylow subgroup, i.e., a subgroup  $P$  of order  $|P| = 2^3$ ; this is, by Corollary 5.3, a 2-subgroup. Now, by Corollary 5.8 (iii), it suffices to show that  $P$  is the only 2-Sylow subgroup. By The third Sylow theorem, the number of 2-Sylow subgroups  $n_2$  is  $n_2 \equiv 1 \pmod{2}$  so either  $n_2 = 1$  or  $n_2 = 3$ .

Suppose that  $n_2 = 3$ . Then

◄

**Problem 2.** Let  $G$  be a group of order  $p^2q$ ,  $p$  and  $q$  primes. Show that the Sylow  $p$ -Sylow subgroup or the  $q$ -Sylow subgroup of  $G$  is normal in  $G$ .

**Solution.** ►

◄

**Problem 3.** Let  $G$  be a subgroup of order  $pqr$ ,  $p < q < r$  primes. Show that the  $r$ -Sylow subgroup of  $G$  is normal in  $G$ .

**Solution.** ►

◄

**Problem 4.** Let  $G$  be a group of order  $n$  and let  $\varphi: G \rightarrow S_n$  be given by the action of  $G$  on  $G$  via translation.

- (a) For  $a \in G$  determine the number and the lengths of the disjoint cycles of the permutation  $\varphi(a)$ .
- (b) Show that  $\varphi(G) \not\subset A_n$  if and only if  $n$  is even and  $G$  has a cyclic 2-Sylow subgroup.
- (c) If  $n = 2m$ ,  $m$  odd, show that  $G$  has a subgroup of index 2.

**Solution.** ►

◄

**Problem 5.** Show that the only simple groups  $\neq \{e\}$  of order  $< 60$  are the groups of prime order.

**Solution.** ►

◄

### 1.1.3 Homework 3

**Problem 1.** Let  $G$  be a finite group,  $p$  a prime number,  $N$  the intersubsection of all  $p$ -Sylow subgroups of  $G$ . Show that  $N$  is a normal  $p$ -subgroup of  $G$  and that every normal  $p$ -subgroup of  $G$  is contained in  $N$ .

**Solution.** ►

◄

**Problem 2.** Let  $G$  be a group of order 231 and let  $H$  be an 11-Sylow subgroup of  $G$ . Show that  $H \subset Z(G)$ .

**Solution.** ►

◄

**Problem 3.** Let  $G = \{e, a_1, a_2, a_3\}$  be a non-cyclic group of order 4 and define  $\varphi: S_3 \rightarrow \text{Aut}(G)$  by  $\varphi(\sigma)(e) = e$  and  $\varphi(\sigma)(a_1) = a_{\sigma(i)}$ . Show that  $\varphi$  is well-defined and an isomorphism of groups.

**Solution.** ►

◄

**Problem 4.** Determine all groups of order 18.

**Solution.** ►

◄

#### 1.1.4 Homework 4

**Problem 1.** Let  $p$  be a prime and let  $G$  be a nonAbelian group of order  $p^3$ . Show that  $G' = Z(G)$ .

**Solution.** ►

◄

**Problem 2.** Let  $p$  be an odd prime and let  $G$  be a nonAbelian group of order  $p^3$  having an element of order  $p^2$ . Show that there exists an element  $b \notin \langle a \rangle$  of order  $p$ .

**Solution.** ►

◄

**Problem 3.** Let  $p$  be an odd prime. Determine all groups of order  $p^3$ .

**Solution.** ►

◄

**Problem 4.** Show that  $(S_n)' = A_n$ .

**Solution.** ►

◄

**Problem 5.** Show that every group of order  $< 60$  is solvable.

**Solution.** ►

◄

**Problem 6.** Show that every group of order 60 that is simple (or not solvable) is isomorphic to  $A_5$ .

**Solution.** ►

◄

### 1.1.5 Homework 5

**Problem 1.** Find all composition series and the composition factors of  $D_6$ .

**Solution.** ►

◀

**Problem 2.** Let  $T$  be the subgroup of  $\text{GL}(n, \mathbb{R})$  consisting of all upper triangular invertible matrices. Show that  $T$  is solvable.

**Solution.** ►

◀

**Problem 3.** Let  $p \in \mathbb{Z}$  be a prime number. Show:

- (a)  $(p-1)! \equiv -1 \pmod{p}$ .
- (b) If  $p \equiv 1 \pmod{4}$  then  $x^2 \equiv -1 \pmod{p}$  for some  $x \in \mathbb{Z}$ .

**Solution.** ►

◀

**Problem 4.** (a) Show that the following are equivalent for an odd prime number  $p \in \mathbb{Z}$ :

- (i)  $p \equiv 1 \pmod{4}$ .
  - (ii)  $p = a^2 + b^2$  for some  $a, b$  in  $\mathbb{Z}$ .
  - (iii)  $p$  is not prime in  $\mathbb{Z}[i]$ .
- (b) Determine all prime ideals of  $\mathbb{Z}[i]$ .

**Solution.** ►

◀



### 1.1.6 Homework 6

**Problem 1.** Let  $R$  be a domain. Show that  $R$  is a UFD if and only if every nonzero nonunit in  $R$  is a product of irreducible elements and the intersection of any two principal ideals is again principal.

**Solution.** ►

◀

**Problem 2.** Let  $R$  be a PID and  $\mathfrak{p}$  a prime ideal of  $R[X]$ . Show that  $\mathfrak{p}$  is principal or  $\mathfrak{p} = (a, f)$  for some  $a \in R$  and some monic polynomial  $f \in R[X]$ .

**Solution.** ►

◀

**Problem 3.** Let  $k$  be a field and  $n \geq 1$ . Show that  $Z^n + Y^3 + X^2 \in k(X, Y)[Z]$  is irreducible.

**Solution.** ►

◀

**Problem 4.** Let  $k$  be a field of characteristic zero and  $n \geq 1$ ,  $m \geq 2$ . Show that  $X_1^n + \cdots + X_m^n - 1 \in k[X_1, \dots, X_m]$  is irreducible.

**Solution.** ►

◀

**Problem 5.** Show that  $X^{3^n} + 2 \in \mathbb{Q}(i)[X]$  is irreducible.

**Solution.** ►

◀

### 1.1.7 Homework 7

**Problem 1.** Let  $k \subset K$  and  $k \subset L$  be finite field extensions contained in some field. Show that:

- (a)  $[KL : L] \leq [K : k]$ .
- (b)  $[KL : k] \leq [K : k][L : k]$ .
- (c)  $K \cap L = k$  if equality holds in (b).

**Solution.** ►

◀

**Problem 2.** Let  $k$  be a field of characteristic  $\neq 2$  and  $a, b$  elements of  $k$  so that  $a, b, ab$  are not squares in  $k$ . Show that  $[k(\sqrt{a}, \sqrt{b}) : k] = 4$ .

**Solution.** ►

◀

**Problem 3.** Let  $R$  be a UFD, but not a field, and write  $K = \text{Quot}(R)$ . Show that  $[\bar{K} : k] = \infty$ .

**Solution.** ►

◀

**Problem 4.** Let  $k \in K$  be an algebraic field extension. Show that every  $k$ -homomorphism  $\delta : K \rightarrow K$  is an isomorphism.

**Solution.** ►

◀

**Problem 5.** Let  $K$  be the splitting field of  $X^6 - 4$  over  $\mathbb{Q}$ . Determine  $K$  and  $[K : \mathbb{Q}]$ .

**Solution.** ►

◀

### 1.1.8 Homework 8

**Problem 1.** Let  $k$  be a field,  $f \in k[X]$  is a polynomial of degree  $n \geq 1$ , and  $K$  the splitting field of  $f$  over  $k$ . Show that  $[K : k] \mid n!$ .

**Solution.** ►

◀

**Problem 2.** Let  $k$  be a field and  $n \geq 0$ . Define a map  $\Delta_n : k[X] \rightarrow k[X]$  by  $\Delta_n(\sum a_i X^i) = \sum a_i \binom{i}{n} X^{i-n}$ . Show:

- (a)  $\Delta_n$  is  $k$ -linear, and for  $f, g$  in  $k[X]$ ,  $\Delta_n(fg) = \sum_{j=0}^n \Delta_j(f) \Delta_{n-j}(g)$ ;
- (b)  $f^{(n)} = n! \Delta_n(f)$ ;
- (c)  $f(X+a) = \sum \Delta_n(f)(a) X^n$ , where  $a \in k$ ;
- (d)  $a \in k$  is a root of  $f$  of multiplicity  $n$  if and only if  $\Delta_i(f)(a) = 0$  for  $0 \leq i \leq n-1$  and  $\Delta_n(f)(a) \neq 0$ .

**Solution.** ►

◀

**Problem 3.** Let  $k \subset K$  be a finite field extension. Show that  $k$  is perfect if and only if  $K$  is perfect.

**Solution.** ►

◀

**Problem 4.** Let  $K$  be the splitting field of  $X^p - X - 1$  over  $k = \mathbb{Z}/p\mathbb{Z}$ . Show that  $k \subset K$  is normal, separable, of degree  $p$ .

**Solution.** ►

◀

**Problem 5.** Let  $k$  be a field of characteristic  $p > 0$ , and  $k(X, Y)$  the field of rational functions in two variables.

- (a) Show that  $[k(X, Y) : k(X^p, Y^p)] = p^2$ .
- (b) Show that the extension  $k(X^p, Y^p) \subset k(X, Y)$  is not simple.
- (c) Find infinitely many distinct fields  $L$  with  $k(X^p, Y^p) \subset L \subset k(X, Y)$ .

**Solution.** ►

◀

### 1.1.9 Homework 9

**Problem 1.** Let  $k \subset K$  be a finite extension of fields of characteristic  $p > 0$ . Show that if  $p \nmid [K : k]$ , then  $k \subset K$  is separable.

**Solution.** ►

◀

**Problem 2.** Let  $k \subset K$  be an algebraic extension of fields of characteristic  $p > 0$ , let  $L$  be an algebraically closed field containing  $K$ , and let  $\delta: k \rightarrow L$  be an embedding. Show that  $k \subset K$  is purely inseparable if and only if there exists exactly one embedding  $\tau: K \rightarrow L$  extending  $\delta$ .

**Solution.** ►

◀

**Problem 3.** Let  $k \subset K = k(\alpha, \beta)$  be an algebraic extension of fields of characteristic  $p > 0$ , where  $\alpha$  is separable over  $k$  and  $\beta$  is purely inseparable over  $k$ . Show that  $K = k(\alpha + \beta)$ .

**Solution.** ►

◀

**Problem 4.** Let  $f(X) \in \mathbb{F}_q[X]$  be irreducible. Show that  $f(X) \mid X^{q^n} - X$  if and only if  $\deg f(X) \mid n$ .

**Solution.** ►

◀

**Problem 5.** Show that  $\text{Aut}_{\mathbb{F}_q}(\bar{\mathbb{F}}_q)$  is an infinite Abelian group which is torsion-free (i.e.,  $\delta^n = \text{id}$  implies  $\delta = \text{id}$  or  $n = 0$ ).

**Solution.** ►

◀

**Problem 6.** Show that in a finite field, every element can be written as a sum of two perfect squares.

**Solution.** ►

◀

### 1.1.10 Homework 10

**Problem 1.** Let  $k \subset K = k(\alpha)$  be a simple field extension, let  $G = \{\delta_1, \dots, \delta_n\}$  be a finite subgroup of  $\text{Aut}_k(K)$ , and write  $f(X) = \prod_{i=1}^n (X - \delta_i(\alpha)) = \sum_{i=0}^n a_i X^i$ . Show that  $f(X)$  is the minimal polynomial of  $\alpha$  over  $K^G$  and that  $K^G = k(a_0, \dots, a_{n-1})$ .

**Solution.** ►

◀

**Problem 2.** Let  $k$  be a field,  $k(X)$  the field of rational functions, and  $u \in k(X) \setminus k$ . Write  $u = f/g$  with  $f$  and  $g$  relatively prime in  $k[X]$ . Show that  $[k(X) : k(u)] = \max\{\deg f, \deg g\}$ .

**Solution.** ►

◀

**Problem 3.** Let  $k$  be a field and  $K = k(X)$  the field of rational functions. Show that for every  $\delta \in \text{Aut}_k(K)$ ,  $\delta(X) = (aX + b)/(cX + d)$  for some  $a, b, c, d$  in  $k$  with  $ad - bc \neq 0$ , and that conversely, every such rational functions uniquely determines an automorphism  $\delta \in \text{Aut}_k(K)$ .

**Solution.** ►

◀

**Problem 4.** With the notion of the previous problem let  $\delta \in \text{Aut}_k(K)$  and  $G = \langle \delta \rangle$ .

- (a) Assume  $\delta(X) = 1/(1 - X)$ . Show that  $|G| = 3$  and determine  $K^G$ .
- (b) Assume  $\text{char } k = 0$  and  $\delta(X) = X + 1$ . Show that  $G$  is infinite and determine  $K^G$ .

**Solution.** ►

◀

**Problem 5.** Let  $k \subset K$  be a finite Galois extension with  $G = \text{Gal}(K/k)$ , let  $L$  be a subfield of  $K$  containing  $k$  with  $H = \text{Gal}(K/L)$ , and let  $L'$  be the compositum in  $K$  of the fields  $\delta(L)$ ,  $\delta \in G$ . Show that:

- (a)  $L'$  is the unique smallest subfield of  $K$  that contains  $L$  and is Galois over  $k$ .
- (b)  $\text{Gal}(K/L') = \bigcap_{\delta \in G} \delta H \delta^{-1}$ .

**Solution.** ►

◀

### 1.1.11 Homework 11

**Problem 1.** Show that every algebraic extension of a finite field is Galois and Abelian.

**Solution.** ►

◀

**Problem 2.** Let  $k$  be a field of characteristic  $\neq 2$  and  $f(X) \in k[X]$  a cubic whose discriminant is a square. Show that  $f$  is either irreducible or a product of linear polynomials in  $k[X]$ .

**Solution.** ►

◀

**Problem 3.** Let  $k$  be a field of characteristic  $\neq 2$ , and let  $f(X) = X^4 + aX^2 + b \in k[X]$  be irreducible with Galois group  $G$ . Show:

- (i) If  $b$  is a square in  $k$ , then  $G = H$ .
- (ii) If  $b$  is not a square in  $k$ , but  $b(a^2 - 4b)$  is, then  $G \cong C_4$ .
- (iii) If neither  $b$  nor  $b(a^2 - 4b)$  is a square in  $k$ , then  $G \cong D_4$ .

**Solution.** ►

◀

**Problem 4.** Determine the Galois group of:

- (a)  $X^4 - 5$  over  $\mathbb{Q}$ , over  $\mathbb{Q}(\sqrt{5})$ , over  $\mathbb{Q}(\sqrt{-5})$ ;
- (b)  $X^3 - 10$  over  $\mathbb{Q}$ ;
- (c)  $X^4 - 4X^2 + 5$  over  $\mathbb{Q}$ ;
- (d)  $X^4 + 3X^3 + 3X - 2$  over  $\mathbb{Q}$ ;
- (e)  $X^4 + 2X^2 + X + 3$  over  $\mathbb{Q}$ .

**Solution.** ►

◀

**Problem 5.** Let  $K$  be the splitting field of  $X^4 - X^2 - 1$  over  $\mathbb{Q}$ . Determine all intermediate fields  $L$ ,  $\mathbb{Q} \subset L \subset K$ . Which of these are Galois over  $\mathbb{Q}$ ?

**Solution.** ►

◀

### 1.1.12 Homework 12

**Problem 1.** Prove that the resolvent cubic  $X^4 + aX^2 + bX + c$  is given by  $X^3 - aX^2 - 4cX + 4ac - b^2$ .

**Solution.** ►

◀

**Problem 2.** Show that the general polynomial  $g(Y) = Y^n + u_1Y^{n-1} + \cdots + u_n$  is irreducible in  $k(u_1, \dots, u_n)[Y]$ .

**Solution.** ►

◀

**Problem 3.** Let  $k$  be a field.

- (a) compute the discriminant  $Y^3 - Y \in k[Y]$  and  $Y^3 - 1 \in k[Y]$ .
- (b) Show that the discriminant of the polynomial  $(Y - X_1)(Y - X_2)(Y - X_3)$  over  $k(X_1, X_2, X_3)$  is of the form

$$\lambda_1 s_1^4 + \lambda_2 s_1^4 s_2 + \lambda_3 s_1^3 s_3 + \lambda_4 s_1^2 s_2^2 + \lambda_5 s_1 s_2 s_3 + \lambda_6 s_2^3 + \lambda_7 s_3^2$$

with  $\lambda_i \in k$ .

- (c) From (b) and (a) conclude that the discriminant  $Y^3 + aY + b \in k[Y]$  is  $-4a^3 - 27b^2$ .

**Solution.** ►

◀

**Problem 4.** Let  $\Phi_n(X)$  be the  $n$ th cyclotomic polynomial over  $\mathbb{Q}$ .

- (a) Let  $n = p_1^{r_1} \cdots p_s^{r_s}$  with  $p_i$  distinct prime numbers and  $r_i > 0$ . Show that  $\Phi(X) = \Phi_{p_1 \cdots p_s}(X^{p_1^{r_1-1} \cdots p_s^{r_s-1}})$ .
- (b) For a prime number  $p$  with  $p \nmid n$  show that  $\Phi_{pn}(X) = \Phi_n(X^p)/\Phi_n(X)$ .

**Solution.** ►

◀

### 1.1.13 Homework 13

**Problem 1.** Let  $n \geq 3$  and  $\rho$  a primitive  $n$ th root of unity over  $\mathbb{Q}$ . Show that  $[\mathbb{Q}(\rho + \rho^{-1}) : \mathbb{Q}] = \varphi(n)/2$ .

**Solution.** ►

◀

**Problem 2.** Let  $\rho$  be a primitive  $n$ th root of unity over  $\mathbb{Q}$ . Determine all  $n$  so that  $\mathbb{Q} \subset \mathbb{Q}(\rho)$  is cyclic.

**Solution.** ►

◀

**Problem 3.** Let  $k \subset K$  be an extension of finite fields. Show that  $\text{Norm}_k^K$  and  $\text{Tr}_k^K$  are surjective maps from  $K$  to  $k$ .

**Solution.** ►

◀

**Problem 4.** Let  $f(X) \in k[X]$  be a separable polynomial of degree  $n \geq 3$  with Galois group isomorphic to  $S_n$ , and let  $\alpha \in \bar{k}$  be a root of  $f(X)$ .

- (a) Show that  $f(X)$  is irreducible.
- (b) Show that  $\text{Aut}_k(k(\alpha)) = \{\text{id}\}$ .
- (c) Show that  $\alpha^n \notin k$  if  $n \geq 4$ .

**Solution.** ►

◀

**Problem 5.** Let  $k \subset K$  be a Galois extension.

- (a) For  $k \subset L \subset K$  show that  $\text{Gal}(K/L)$  is solvable if  $\text{Gal}(K/k)$  is solvable.
- (b) For  $k \subset L \subset K$  with  $k \subset L$  normal show that  $\text{Gal}(L/k)$  and  $\text{Gal}(K/L)$  are solvable if and only if  $\text{Gal}(K/k)$  is solvable.
- (c) For  $k \subset L$  with  $K$  and  $L$  in a common field show that  $\text{Gal}(KL/L)$  is solvable if  $\text{Gal}(K/k)$  is solvable.

**Solution.** ►

◀



## 2 Ulrich

### 2.1 Ulrich: Winter 2002

**Problem 1.** Let  $G$  be a group and  $H$  a subgroup of finite index. Show that there exists a normal subgroup  $N$  of  $G$  of finite index with  $N \subset H$ .

**Solution.** ► Let  $n = [G : H]$  and  $X = \{H, g_1H, \dots, g_{n-1}H\}$  the set of left-cosets of  $H$  in  $G$  with representatives  $g_0 = e, g_1, \dots, g_{n-1}$ . Let  $G$  act on  $X$  by left multiplication, i.e.,  $g \mapsto gg_iH$ ; this is indeed an action since  $e(g_iH) = eg_iH = g_iH$  for all  $g_iH \in X$  and for  $k_1, k_2 \in G$   $k_2(k_1g_iH) = k_2k_1g_iH = (k_2k_1)g_iH$ . By Cayley's theorem, this induces a homomorphism  $\varphi: G \rightarrow S_n$ . Note that the action is not necessarily faithful. However, by the first isomorphism theorem, the kernel of  $\varphi$ ,  $N = \text{Ker } \varphi$ , is a normal subgroup of  $G$  with index  $[G : N] \leq |S_n| = n!$  and  $N \subset H$  since  $g \in N$  if and only if  $gg_iH = g_iH$  which, in particular, implies that  $gH = H$ . Thus,  $N \subset H$  and  $[G : N] < \infty$ . ◀

**Problem 2.** Show that every group of order 992 ( $= 32 \cdot 31$ ) is solvable.

**Solution.** ► Suppose  $G$  is a group with order  $|G| = 992 = 2^5 \cdot 31$ . By Sylow's theorem, the number of 2-Sylow subgroups in  $G$  is either 1 or 31. If the number of 2-Sylow subgroups is 1, then  $P \triangleleft G$  and the quotient  $G/P$  has order  $[G : P] = 31$ , hence, is cyclic. Moreover, since  $P$  is a  $p$ -group, it is solvable. Since  $P$  and  $G/P$  are solvable,  $G$  is solvable.

Now, suppose the number of 2-Sylow subgroups is 31. Let  $\text{Syl}_2(G) = \{P, P_1, P_2\}$ . Then, by Sylow's theorem, the three 2-Sylow subgroups are conjugate, i.e., there exists  $g_1, g_2 \in G$  such that  $P_1 = g_1Pg_1^{-1}$  and  $P_2 = g_2Pg_2^{-1}$ . Thus,  $G$  acts on the set  $\text{Syl}_2(G)$  by conjugation. This action defines a (not necessarily injective) homomorphism  $\varphi: G \rightarrow S_3$ . Now, we ask: What is the kernel of this homomorphism? By the first isomorphism theorem, we know that the index of the kernel in  $G$  divides the order of  $S_3$ , i.e.,  $[G : \text{Ker } \varphi] \mid 6$ . Since  $|G| < \infty$  implies that the order of the kernel is one of the following values

$$|\text{Ker } \varphi| = 2^4, 2^4 \cdot 31, 2^5, 2^5 \cdot 31.$$

Now,  $|\text{Ker } \varphi| \neq 2^5 \cdot 31$  since we know at least one automorphism, namely conjugation by  $g_1$ , which sends  $P \mapsto P_1$ . Thus, the order of the kernel is either  $2^4$ ,  $2^4 \cdot 31$  or  $2^5$ . If the  $|\text{Ker } \varphi| = 2^4$  or  $2^5$ , we are done for similar reasons to the argument we gave in the previous paragraph, namely, that  $\text{Ker } \varphi \triangleleft G$  and  $G/\text{Ker } \varphi$  is solvable (for  $|\text{Ker } \varphi| = 2^4$ , the quotient  $G/\text{Ker } \varphi$  has order 6 so is isomorphic to one of two groups,  $S_3$  or  $Z_6$ , both of which are solvable).

Suppose  $\text{Ker } \varphi$  has order  $2^4 \cdot 31$ . Then the number of 3-Sylow subgroups is either 1, 4 or 16. If this number is 1, we are done as  $Q \in \text{Syl}_3(\text{Ker } \varphi)$  is a normal subgroup and the quotient is a  $p$ -group. Suppose the number of 3-Sylow subgroups is 16. Then there are  $16 \cdot 2 = 32$  elements of order 3 in  $\text{Ker } \varphi$ . ◀

**Problem 3.** Let  $G$  be a group of order 56 with a normal 2-Sylow subgroup  $Q$ , and let  $P$  be a 7-Sylow subgroup of  $G$ . Show that either  $G \cong P \times Q$  or  $Q \cong \mathbf{Z}/(2) \times \mathbf{Z}/(2) \times \mathbf{Z}/(2)$ .

[Hint:  $P$  acts on  $Q \setminus \{e\}$  via conjugation. Show that this action is either trivial or transitive.]

**Solution.** ► First, note that, by the fundamental theorem of arithmetic, the order of  $G$  can be broken down into  $56 = 2^3 \cdot 7$ . Suppose  $G$  has a normal 2-Sylow subgroup  $Q$  and let  $P \in \text{Syl}_3(G)$ . Then  $|\text{Syl}_3(G)| = 1, 4$ . If  $|\text{Syl}_3(G)| = 1$ , then  $P$  is the unique 3-Sylow subgroup of  $G$ , hence it is normal. Thus,  $|P||Q| = |G|$  and  $PQ = G$  since, if  $g \in Q \cap P$ , then  $|g| = 3$ , but  $2 \mid |g|$  so  $g = e$ . Thus,  $G \cong P \times Q$ .

Now, suppose  $|\text{Syl}_3(G)| = 4$ . Then  $G$  contains 4 3-Sylow subgroups which, by Sylow's theorem, are conjugate, i.e., there exists  $g_1, g_2, g_3 \in G$  such that  $\text{Syl}_p(G) = \{P, g_1Pg_1^{-1}, g_2Pg_2^{-1}, g_3Pg_3^{-1}\}$ . Let  $P$  act on  $Q$  by conjugation. Then ◀

**Problem 4.** Let  $R$  be a commutative ring and  $\text{Rad}(R)$  the intersection of all maximal ideals of  $R$ .

- (a) Let  $a \in R$ . Show that  $a \in \text{Rad}(R)$  if and only if  $1 + ab$  is a unit for every  $b \in R$ .
- (b) Let  $R$  be a domain and  $R[X]$  the polynomial ring over  $R$ . Deduce that  $\text{Rad}(R[X]) = 0$ .

**Solution.** ► ◀

**Problem 5.** Let  $R$  be a unique factorization domain and  $\mathfrak{p}$  a prime ideal of  $R[X]$  with  $\mathfrak{p} \cap R = 0$ .

- (a) Let  $n$  be the smallest possible degree of a nonzero polynomial in  $\mathfrak{p}$ . Show that  $\mathfrak{p}$  contains a primitive polynomial  $f$  of degree  $n$ .
- (b) Show that  $\mathfrak{p}$  is the principal ideal generated by  $f$ .

**Solution.** ► ◀

**Problem 6.** Let  $k$  be a field of characteristic zero. assume that every polynomial in  $k[X]$  of odd degree and every polynomial in  $k[X]$  of degree two has a root in  $k$ . Show that  $k$  is algebraically closed.

**Solution.** ► ◀

**Problem 7.** Let  $k \subset K$  be a finite Galois extension with Galois group  $\text{Gal}(K/k)$ , let  $L$  be a field with  $k \subset L \subset K$ , and set  $H = \{\sigma \in \text{Gal}(K/k) : \sigma(L) = L\}$ .

- (a) Show that  $H$  is the normalizer of  $\text{Gal}(K/L)$  in  $\text{Gal}(K/k)$ .
- (b) Describe the group  $H/\text{Gal}(K/L)$  as an automorphism group.

**Solution.** ►



### 3 Field Theory and Galois Theory

Notes taken from Keith Conrad's blurbs.

#### 3.1 Roots and irreducibles

This handout discusses relationships between roots of irreducible polynomials and field extensions.

##### 3.1.1 Roots in larger fields

For most fields  $K$ , there are polynomials in  $K[X]$  without a root in  $K$ . Consider  $X^2 + 1$  in  $\mathbf{R}[X]$  or  $X^3 - 2$  in  $\mathbf{F}_7[X]$ . If we are willing to enlarge the field. The following is due to Kronecker.

**Theorem 1.** *Let  $K$  be a field and  $f(X)$  be a nonconstant polynomial in  $K[X]$ . There exists a field extension of  $K$  containing a root of  $f(X)$ .*

*Proof.* It suffices to prove the theorem when  $f(X) = \pi(X)$  is irreducible.

Set  $F = K[t]/(\pi(t))$  where  $t$  is an indeterminate. Since  $\pi(t)$  is irreducible in  $K[t]$ ,  $F$  is a field. Inside of  $F$  we have  $K$  as a subfield: the congruence classes represented by constants. There is also a root of  $\pi(X)$  in  $F$ , namely the class of  $t$ . Indeed, writing  $\bar{t}$  for the congruence class of  $t$  in  $F$ , the congruence  $\pi(t) \equiv 0 \pmod{\pi(t)}$  becomes the equation  $\pi(\bar{t}) = 0$  in  $F$ . ■

**Corollary 2.** *Let  $K$  be a field and  $f(X) = c_m X^m + \cdots + c_0$  a polynomial in  $K[X]$  with degree  $m \geq 1$ . There is a field  $L \supset K$  such that in  $L[X]$*

$$f(X) = c_m(X - \alpha_1) \cdots (X - \alpha_m).$$

*Proof.* We induct on the degree  $m$ . The case  $m = 1$  is clear, using  $L = K$ . By Theorem 2.1, there is a field  $F \supset K$  such that that  $f(X)$  has a root in  $F$ , say  $\alpha$ . Then in  $F[X]$ ,

$$f(X) = (X - \alpha_1)g(X),$$

where  $\deg g(X) = m - 1$ . The leading coefficient of  $g(X)$  is also  $c_m$ .

Since  $g(X)$  has smaller degree than  $f(X)$ , by induction on the degree there is a field  $L \supset F$  (so  $L \supset K$ ) such that  $g(X)$  decomposes into linear factors in  $L[X]$ , so we get the desired factorization of  $f(X)$  in  $L[X]$ . ■

**Corollary 3.** *Let  $f(X)$  and  $g(X)$  be nonconstant in  $K[X]$ . They are relatively prime in  $K[X]$  if and only if they do not have a common root in any extension field of  $K$ .*

*Proof.* Assume  $f(X)$  and  $g(X)$  are relatively prime in  $K[X]$ . Then we can write

$$f(X)u(X) + g(X)v(X) = 1$$

for some  $u(X)$  and  $v(X)$  in  $K[X]$ . If there were an  $\alpha$  in a field extension of  $K$  which is a common root of  $f(X)$  and  $g(X)$ , then substituting  $\alpha$  for  $X$  in the

above polynomial identity makes the left side 0 while the right side is 1. This is a contradiction, so  $f(X)$  and  $g(X)$  have no common root in any field extension of  $K$ .

Now assume  $f(X)$  and  $g(X)$  are not relatively prime in  $K[X]$ . Say,  $h(X) \in K[X]$  is a (nonconstant) common factor. There is a field extension of  $K$  in which  $h(X)$  has a root and this root will be a common root of  $f(X)$  and  $g(X)$ . ■

### 3.1.2 Divisibility and roots in $K[X]$

There is an important connection between roots of a polynomial and divisibility by linear polynomials. For  $f(X) \in K[X]$  and  $\alpha \in K$ ,  $f(\alpha) = 0 \iff (X - \alpha) \mid f(X)$ . The next result is an analogue for divisibility by higher degree polynomials in  $K[X]$ , provided they are irreducible. (All linear polynomials are irreducible.)

**Theorem 4.** *Let  $\pi(X)$  be an irreducible in  $K[X]$  and let  $\alpha$  be a root of  $\pi(X)$  in some larger field. For  $h(X)$  in  $K[X]$ ,  $h(\alpha) = 0 \iff \pi(X) \mid h(X)$  in  $K[X]$ .*

*Proof.* If  $h(X) = \pi(X)g(X)$ , then  $h(\alpha) = \pi(\alpha)g(\alpha) = 0$ .

Now assume  $h(\alpha) = 0$ . Then  $h(X)$  and  $\pi(X)$  have a common root, so by Corollary 2.4 they have a common factor in  $K[X]$ . Since  $\pi(X)$  is irreducible, this means  $\pi(X) \mid h(X)$  in  $K[X]$ . To see this argument more directly, suppose  $h(\alpha) = 0$  and  $\pi(X)$  does not divide  $h(X)$ . Then (because  $\pi$  is irreducible) the polynomials  $\pi(X)$  and  $h(X)$  are relatively prime in  $K[X]$  so we can write

$$\pi(X)u(X) + h(X)v(X) = 1$$

for some  $u(X), v(X) \in K[X]$ . Substitute  $\alpha$  for  $X$  and the left side vanishes. The right side is 1 so we have a contradiction. ■

**Theorem 5.** *Let  $K$  be a field and  $L$  be a larger field. For  $f(X)$  and  $g(X)$  in  $K[X]$ ,  $f(X) \mid g(X)$  in  $K[X]$  if and only if  $f(X) \mid g(X)$  in  $L[X]$ .*

*Proof.* It is clear that divisibility in  $K[X]$  implies divisibility in larger  $L[X]$ . Conversely suppose  $f(X) \mid g(X)$  in  $L[X]$ . Then

$$g(X) = f(X)h(X)$$

for some  $h(X) \in L[X]$ . By the division algorithm in  $K[X]$ ,

$$g(X) = f(X)q(X) + r(X)$$

where  $q(X)$  and  $r(X)$  are in  $K[X]$  and  $r(X) = 0$  or  $\deg r < \deg f$ . Comparing these two formulas for  $g(X)$ , the uniqueness of the division algorithm in  $L[X]$  implies  $q(X) = h(X)$  and  $r(X) = 0$ . Therefore  $g(X) = f(X)q(X)$ , so  $f(X) \mid g(X)$  in  $L[X]$ . ■

### 3.2 Raising to the $p$ th power in characteristic $p$

**Lemma 6.** *Let  $A$  be a commutative ring with prime characteristic. Pick any  $a$  and  $b$  in  $A$ .*

(a)  $(a + b)^p = a^p + b^p$ .

(b) *When  $A$  is a domain,  $a^p = b^p \implies a = b$ .*

*Proof.* (a) By the binomial theorem,

$$(a + b)^p = a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^{p-k} b^k + b^p.$$

For  $1 \leq k \leq p-1$ , the integer  $\binom{p}{k}$  is a multiple of  $p$ , so the intermediate terms are 0 in  $A$ .

(b) Now assume  $A$  is a domain and  $a^p = b^p$ . Then  $0 = a^p - b^p = (a - b)^p$ . (Note  $(-1)^p = -1$  for  $p \neq 2$ , and also for  $p = 2$  since  $2 = 0 \implies -1 = 1$  in  $A$ .) Since  $A$  is a domain,  $a - b = 0$  so  $a = b$ . ■

**Lemma 7.** *Let  $F$  be a field containing  $\mathbf{F}_p$ . For  $c \in F$ ,  $c \in \mathbf{F}_p \iff c^p = c$ .*

*Proof.* Every element  $c$  of  $\mathbf{F}_p$  satisfies the equation  $c^p = c$ . Conversely, solutions to this equation are the roots of  $X^p - X$ , which has at most  $p$  roots. The elements of  $\mathbf{F}_p$  already fulfill this upper bound, so there are no further roots in characteristic  $p$ . ■

**Theorem 8.** *For any  $f(X) \in \mathbf{F}_p[X]$ ,  $f(X)^p = f(X^{p^r}) = f(X^{p^r})$  for  $r \geq 0$ . If  $F$  is a field of characteristic  $p$  other than  $\mathbf{F}_p$ , this is not always true in  $F[X]$ .*

*Proof.* Writing

$$f(X) = c_m X^m + c_{m-1} X^{m-1} + \cdots + c_1 X + c_0,$$

Lemma 4.1a with  $A = \mathbf{F}_p[X]$  gives

$$\begin{aligned} f(X)^p &= (c_m X^m + c_{m-1} X^{m-1} + \cdots + c_1 X + c_0)^p \\ &= c_m^p X^{mp} + c_{m-1}^p X^{p(m-1)} + \cdots + c_1^p X^p + c_0^p \\ &= c_m (X^p)^m + c_{m-1} (X^p)^{m-1} + \cdots + c_1 X^p + c_0, \end{aligned}$$

since  $c^p = c$  for any  $c \in \mathbf{F}_p$ . The last expression is  $f(X^p)$ . Applying this result  $r$  times, we find  $f(X)^{p^r} = f(X^{p^r})$ . ■

Let  $f(X) \in \mathbf{F}_p[X]$  be nonconstant, with degree  $m$ . Let  $L \supset \mathbf{F}_p$  be a field over which  $f(X)$  decomposes into linear factors, i.e., (2.1) holds. It is possible to that some roots of  $f(X)$  are multiple roots. As long as that does not happen, the following corollary says something about the  $p$ th powers of the roots.

**Corollary 9.** *When  $f(X) \in \mathbf{F}_p[X]$  has distinct roots, raising all roots of  $f(X)$  to the  $p$ th power permutes the roots*

$$\{\alpha_1^p, \dots, \alpha_m^p\} = \{\alpha_1, \dots, \alpha_m\}.$$

*Proof.* Let  $S = \{\alpha_1, \dots, \alpha_m\}$ . Since  $f(X)^p = f(X^p)$  by Theorem 4.3, the  $p$ th power of each root of  $f(X)$  is again a root of  $f(X)$ . Therefore raising to the  $p$ th power defines a function  $\varphi: S \rightarrow S$ . By Lemma 4.1b,  $\varphi$  takes different values on different elements of  $S$ . Since  $S$  is a finite set,  $\varphi$  must assume each element of  $S$  as a value (in the language of set theory, a one-to-one function from a finite set to itself is onto), so  $\varphi$  is a permutation of  $S$ . ■

### 3.3 Roots of irreducibles in $\mathbf{F}_p[X]$

**Lemma 10.** *For  $h(X)$  in  $\mathbf{F}_p[X]$  with degree  $m$ ,  $\mathbf{F}_p[X]/(h(X))$  has size  $p^m$ .*

*Proof.* By the division algorithm in  $\mathbf{F}_p[X]$ , every congruence class modulo ■

## References

- [1] DUMMIT, D., AND FOOTE, R. *Abstract Algebra*. Wiley, 2004.
- [2] HERSTEIN, I. *Topics in algebra*. Xerox College Pub., 1975.
- [3] HUNGERFORD, T. *Algebra*. Graduate Texts in Mathematics. Springer New York, 2003.
- [4] MILNE, J. S. Group theory (v3.13), 2013. Available at [www.jmilne.org/math/](http://www.jmilne.org/math/).
- [5] MILNE, J. S. Fields and galois theory (v4.50), 2014. Available at [www.jmilne.org/math/](http://www.jmilne.org/math/).