MA553: Qual Preparation

Carlos Salinas

August 9, 2016

Contents

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 $1, 2, \ldots$
k	is used to denote the base field with characteristic ch 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 $\{1, \ldots, n\}$
A_n	is the alternating group on $\{1, \ldots, n\}$
D_n	is the dihedral group of order n
$A \smallsetminus B$	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

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

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

Solution. ▸ Let ℓ denote the order of a^n. Then ℓ 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 $m' = m/(n,m)$ 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, $\ell = m/(m,n)$. ◂

Exercise 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 $\operatorname{ord}(ab) = mn/(m,n)$.

Solution. ▸ Let ℓ 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, $\operatorname{ord}(a^n) = m/(m,n)$ so $\operatorname{ord}(ab) = mn/(m,n)$. ◂

Exercise 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 $H \subseteq G$, $h \in G$ 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 $\varphi\colon HK \to (HK/K) \times (HK/H)$ given by $\varphi(hk) = (\pi_K(h), \pi_H(k))$ where $\pi_H : HK \to HK/H$ and $\pi_K : HK \to HK/K$ are quotient maps. By the first (or second) isomorphism theorem, $H \cong HK/H$ and $K \cong HK/H$ so $HK \cong H \times K$. ◂

Exercise 4. Show that A_4 has no subgroup of order 6 (although $6 \mid 12 = \operatorname{card} A_4$.

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 σ^2 where $\sigma \in A$.

> *Proof of claim.* Since $\operatorname{card} H = 6$, $(A_4 : H) = 2$ 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 $\operatorname{card}(G/H) = 2$ 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

$$
\begin{aligned}
(1)^2 &= (1) & (1\,2\,3)^2 &= (1\,3\,2)\\
(1\,3\,2)^2 &= (1\,2\,3) & (1\,2\,4)^2 &= (1\,4\,2)\\
(1\,4\,2)^2 &= (1\,2\,4) & (1\,3\,4)^2 &= (1\,4\,3)\\
(1\,4\,3)^2 &= (1\,3\,4) & (2\,3\,4)^2 &= (2\,3\,4)\\
(2\,4\,3)^2 &= (2\,4\,3) & ((1\,2)(3\,4))^2 &= (1)\\
((1\,3)(2\,4))^2 &= (1) & ((1\,4)(2\,3))^2 &= (1)
\end{aligned}
$$

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

Exercise 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 $\operatorname{card} G = 2^n \cdot 3$. By Sylow's theorem, G contains a 2-Sylow subgroup P of order $\operatorname{card} P = 2^n$. If P is the unique 2-Sylow subgroup in G, $P \trianglelefteq G$.

Otherwise, Sylow's theorem implies that $\operatorname{card}(\mathrm{Syl}_2(G))$ must divide 3 and, since 3 is prime, must in fact equal 3. Then, each $Q \in \mathrm{Syl}_2(G)$ is conjugate to P. Enumerate the set $\mathrm{Syl}_2(G) = \{P, P', P''\}$ and let G act on $\mathrm{Syl}_2(G)$ by conjugation. This action gives rise to a homomorphism $\varphi\colon G \to S_3$ given by the permutation representation of the action. This action is nontrivial since there exists elements $g_1, g_2 \in G$ such that $P' = g_1 P g_1{}^{-1}$ and $P'' = g_2 P g_2{}^{-1}$ (which correspond to the permutations $(1\,2)$ and $(1\,3)$). By the first isomorphism theorem, $\operatorname{Ker}\varphi \trianglelefteq G$ and $(G : \operatorname{Ker}\varphi) \mid \operatorname{card} S_3 = 6$. But we observed that the image of G in S_3 contains at least 3 permutations: $(1\,2)$, $(1\,3)$ and $(1\,2)(1\,3) = (1\,3\,2)$. Thus, $(G : \operatorname{Ker}\varphi) = 3$ or 6. In either case, $\operatorname{Ker}\varphi$ is a 2-subgroup of G. ◂

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

Solution. ▸ Suppose $\operatorname{card} G = p^2 q$. Assuming $p < q$ there are 1 or p^2 q-Sylow subgroups. If there is 1 q-Sylow subgroup Q then $Q \trianglelefteq G$. Otherwise, there are p^2 q-Sylow subgroups in G and, counting the total number of elements of order q, there are $p^2(q-1) = p^2q - p^2$ remaining elements in G which leaves just enough room for 1 p-Sylow subgroup P which implies that $P \trianglelefteq G$. Otherwise, $p > q$ and we must be one 1 p-Sylow subgroup P in G which implies $P \trianglelefteq G$. In each case, we either have a normal p-Sylow subgroup or a normal q-Sylow subgroup. ◂

Exercise 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. ▸ By Sylow's theorem, we have 1 or pq r-Sylow subgroup in G. In the former case, there is a unique r-Sylow subgroup R which implies $R \trianglelefteq G$. In the latter case, there are pq r-Sylow subgroups in G and that implies that we have $pq(r-1) = pqr - pq$ elements of order r. That leaves room for exactly pq elements that do not have order r. Now we ask, what are the possible number of p- and q-Sylow subgroups? At minimum, we have 1 p- and 1 q-Sylow subgroups. This yields a total of

$$\begin{aligned}(p-1) + (q-1) + 1 &= p + q - 1 \\ &< pq\end{aligned}$$

which flows under the total number of elements to complete the size of the group. What is the next smallest possible number of p- and q-Sylow subgroups is r. In this case, we have

$$\begin{aligned}r(p-1) + r(q-1) + 1 &= rp - r + rq - r + 1 \\ &= r(p + q - 2) + 1 \\ &> pq\end{aligned}$$

since $r > p$ and $p + q - 2 > 2p - 2 > p$. Thus, we cannot have pq r-Sylow subgroups in G. It follows that there is only 1 r-Sylow subgroup R in G and so $R \trianglelefteq G$. ◂

Exercise 4. Let G be a group of order n and let $\varphi\colon G \to S_n$ 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 $\varphi(G) \nsubseteq A_n$ 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. ▸ For (a), let $\{g_0 = e, g_1, \ldots, g_{n-1}\}$ be an enumeration of G. Fix $a = g_k$ in G for some $0 \le k \le n-1$. Then the action of G on itself by translation gives a homomorphism $\varphi\colon G \to S_n$ which sends $\{g_0, g_1, \ldots, g_n\}$ to the set $\{ag_0, ag_1, \ldots, ag_n\}$. If a is nontrivial, the latter set equals G so has no fixed point. This implies that every nontrivial a in G corresponds to an n-cycle in S_n. I don't know what he's talking about so I am just moving on.

For (b), ◂

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

Solution. ▸ First, let us list all of the possible orders of groups with order less than 60, these orders are

$$\begin{array}{ccccc} 4 & 6 & 8 & 9 & 10 \\ 12 & 14 & 15 & 16 & 18 \\ 20 & 21 & 22 & 24 & 25 \\ 26 & 27 & 28 & 30 & 32 \\ 33 & 34 & 35 & 36 & 38 \\ 39 & 40 & 42 & 44 & 45 \\ 46 & 48 & 49 & 50 & 51 \\ 52 & 54 & 55 & 56 & 58 \end{array}.$$

These integers fall into one of the following categories $n = p^2, pq, p^3, p^2q, pqr, p^4, p^3q, p^2q^2, p^5, p^4q$; here they are by type

p^2	pq	p^3	p^2q	pqr	p^4	p^3q	p^2q^2	p^5	p^4q
4	6	8	12	30	16	24	36	32	48
9	10	27	18	42		40			
25	14		20			56			
49	15		28						
	21		44						
	22		45						
	26		50						
	33		52						
	34								
	35								
	38								
	39								
	46								
	51								
	54								
	55								
	58								

.

All p-groups have a nontrivial center, so groups of orders corresponding to the the p^2, p^3, p^4 and p^5 columns are not simple. Similarly, groups of order pq are not simple and we have just shown that groups of order p^2q and pqr are not simple.

Now we cover the following cases:

Claim.

(a) *If* $\operatorname{card} G = p^n q$ *for* $n \geq 2$, *G contains a nontrivial normal subgroup.*

(b) *If* $\operatorname{card} G = p^2 q^2$, *G contains a nontrivial normal subgroup.*

Proof of claim. For (a), consider the p-Sylow subgroup P of G. ■

◂

1.1.3 Homework 3

Exercise 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. ▸ ◂

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

Solution. ▸ ◂

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

Solution. ▸ ◂

Exercise 4. Determine all groups of order 18.

Solution. ▸ ◂

1.1.4 Homework 4

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

Solution. ► ◄

Exercise 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. ► ◄

Exercise 3. Let p be an odd prime. Determine all groups of order p^3.

Solution. ► ◄

Exercise 4. Show that $(S_n)' = A_n$.

Solution. ► ◄

Exercise 5. Show that every group of order < 60 is solvable.

Solution. ► ◄

Exercise 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

Exercise 1. Find all composition series and the composition factors of D_6.

Solution. ► ◄

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

Solution. ► ◄

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

(a) $(p-1)! \equiv -1 \mod p$.

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

Solution. ► ◄

Exercise 4.

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

  (i) $p \equiv 1 \mod 4$.

  (ii) $p = a^2 + b^2$ for some a, b in $\mathbb{Z}$.

  (iii) p is not prime in $\mathbb{Z}[\mathrm{i}]$.

(b) Determine all prime ideals of $\mathbb{Z}[\mathrm{i}]$.

Solution. ► ◄

1.1.6 Homework 6

Exercise 1. Let R be a domain. Show that R is a u.f.d. 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. ▸ ◂

Exercise 2. Let R be a p.i.d. 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. ▸ ◂

Exercise 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. ▸ ◂

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

Solution. ▸ ◂

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

Solution. ▸ ◂

1.1.7 Homework 7

Exercise 1. Let $k \subseteq K$ and $k \subseteq L$ 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. ▸ ◂

Exercise 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 $\left[k\left(\sqrt{a}, \sqrt{b}\right) : k\right] = 4$.

Solution. ▸ ◂

Exercise 3. Let R be a u.f.d, but not a field, and write $K = \mathrm{Quot}(R)$. Show that $[\bar{K} : k] = \infty$.

Solution. ▸ ◂

Exercise 4. Let $k \in K$ be an algebraic field extension. Show that every k-homomorphism $\delta \colon K \to K$ is an isomorphism.

Solution. ▸ ◂

Exercise 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

Exercise 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. ▸ ◂

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

(a) Δ_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. ▸ ◂

Exercise 3. Let $k \subseteq K$ be a finite filed extension. Show that k is perfect if and only if K is perfect.

Solution. ▸ ◂

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

Solution. ▸ ◂

Exercise 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 $\left[k(X, Y) : k(X^p, Y^p)\right] = p^2$.

(b) Show that the extension $k(X^p, Y^p) \subseteq k(X, Y)$ is not simple.

(c) Find infinitely many distinct fields L with $k(X^p, Y^p) \subseteq L \subseteq k(X, Y)$.

Solution. ▸ ◂

1.1.9 Homework 9

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

Solution. ► ◄

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

Solution. ► ◄

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

Solution. ► ◄

Exercise 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. ► ◄

Exercise 5. Show that $\mathrm{Aut}_{\mathbb{F}_q}(\bar{\mathbb{F}}_q)$ is an infinite Abelian group which is torsionfree (i.e., $\delta^n = \mathrm{id}$ implies $\delta = \mathrm{id}$ or $n = 0$.

Solution. ► ◄

Exercise 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

Exercise 1. Let $k \subset K = k(\alpha)$ be a simple field extension, let $G = \{\delta_1, \ldots, \delta_n\}$ be a finite subgroup of $\operatorname{Aut}_k(K)$, and write $f(X) = \prod_{i=1}^{n}\big(X - \delta_i(\alpha)\big) = \sum_{i=0}^{n} a_i X^i$. Show that $f(X)$ is the minimal polynomial of α over K^2 and that $K^G = k(a_0, \ldots, a_{n-1})$.

Solution. ► ◄

Exercise 2. Let k be a field, $k(X)$ the field of rational functions, and $u \in k(X) \smallsetminus k$. 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. ► ◄

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

Solution. ► ◄

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

(a) Assume $\delta(X) = 1/(1 - X)$. Show that $|G| = 3$ and determine K^G.

(b) Assume $\operatorname{ch} k = 0$ and $\delta(X) = X + 1$. Show that G is infinite and determine K^G.

Solution. ► ◄

Exercise 5. Let $k \subset K$ be a finite Galois extension with $G = \operatorname{Gal}(K/k)$, let L be a subfield of K containing k with $H = \operatorname{Gal}(K/L)$, 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) $\operatorname{Gal}(K/L') = \bigcap_{\delta \in G} \delta H \delta^{-1}$.

Solution. ► ◄

1.1.11 Homework 11

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

Solution. ► ◄

Exercise 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. ► ◄

Exercise 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. ► ◄

Exercise 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. ► ◄

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

Solution. ► ◄

1.1.12 Homework 12

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

Solution. ▸ ◂

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

Solution. ▸ ◂

Exercise 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. ▸ ◂

Exercise 4. Let $\Phi_n(X)$ be the nth 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 $\Phi(X) = \Phi_{p_1 \cdots p_s}\left(X^{{p_1}^{r_1-1} \cdots {p_s}^{r_s-1}}\right)$.

(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

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

Solution. ▸ ◂

Exercise 2. Let ρ be a primitive nth root of unity over $\mathbb{Q}$. Determine all n so that $\mathbb{Q} \subseteq \mathbb{Q}(\rho)$ is cyclic.

Solution. ▸ ◂

Exercise 3. Let $k \subseteq K$ be an extension of finite fields. Show that norm_k^K and tr_k^K are surjective maps from K to k.

Solution. ▸ ◂

Exercise 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 $\mathrm{Aut}_k(k(\alpha)) = \{\mathrm{id}\}$.

(c) Show that $\alpha^n \notin k$ if $n \geq 4$.

Solution. ▸ ◂

Exercise 5. Let $k \subseteq K$ be a Galois extension.

(a) For $k \subseteq L \subseteq K$ show that $\mathrm{Gal}(K/L)$ is solvable if $\mathrm{Gal}(K/k)$ is solvable.

(b) For $k \subseteq L \subseteq K$ with $k \subseteq L$ normal show that $\mathrm{Gal}(L/k)$ and $\mathrm{Gal}(K/L)$ are solvable if and only if $\mathrm{Gal}(K/k)$ is solvable.

(c) For $k \subseteq L$ with K and L in a common field show that $\mathrm{Gal}(KL/L)$ is solvable if $\mathrm{Gal}(K/k)$ is solvable.

Solution. ▸ ◂

2 Ulrich

2.1 Ulrich: Winter 2002

Exercise 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 $N \subseteq H$.

Solution. ▸ Suppose $N < G$ with $n = [G : N] < \infty$. Let G act on H by translation. This action gives a homomorphism $\varphi \colon G \to S_n$. Then, by the first isomorphism theorem $[G : \operatorname{Ker}\varphi] \mid \operatorname{card} S_n = n!$. Thus, $\operatorname{Ker}\varphi$ is a normal subgroup of G with finite index. ◂

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

Solution. ▸ Suppose $\operatorname{card} G = 992 = 32 \cdot 31 = 2^5 \cdot 31$. By Sylow's theorem, G has 1 or 32 31-Sylow subgroups. In the former case, this implies that there is a unique 31-Sylow subgroup P and therefore $P \trianglelefteq G$. Moreover, since $\operatorname{card}(G/P) = 2^3$, G/P is solvable since it is a p-group. Thus, both G/P and P are solvable (the latter since it is Abelian), which implies that G is solvable.

On the other hand, if G contains 32 31-Sylow subgroups, then there are exactly $32 \cdot 31 - 32 \cdot 30 = 32$ elements not of order 31. This implies that there is exactly one 2-Sylow subgroup Q in G. Again, since $\operatorname{card} G/Q = 31$, G/Q is solvable and Q is solvable since it is a p-group. Thus, G is solvable.

In every case, G we see that is solvable. ◂

Exercise 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 $G \simeq P \times Q$ or $Q \simeq \mathbb{Z}/(2) \times \mathbb{Z}/(2) \times \mathbb{Z}/(2)$. [*Hint*: P acts on $Q \setminus \{e\}$ via conjugation. Show that this action is either trivial or transitive.]

Solution. ▸ Suppose G is a group of order $56 = 2^3 \cdot 7$ with a normal 2-Sylow subgroup Q and let $P \in \operatorname{Syl}_7(G)$. Taking the hint, let P act on Q by conjugation. This action gives a homomorphism $\varphi \colon P \to \operatorname{Aut} Q$. The kernel of this action is exactly the centralizer Q in P, $\operatorname{Ker}\varphi = \mathrm{C}_P(Q)$. Considering the Cardinality of P, either $\operatorname{Ker}\varphi = P$ or $\operatorname{Ker}\varphi = \{e\}$. In the former case, this implies that $pq = qp$ for every $p \in P$, $q \in Q$. In particular, Q is in the normalizer of P and since $\operatorname{card} P \mid \mathrm{N}_G(P)$, we must have $\mathrm{N}_G(P) = G$. Thus, since $P, Q \trianglelefteq G$, $P \cap Q = \{e\}$ and $PQ = G$, we have $G \simeq P \times Q$.

On the other hand, if $\operatorname{Ker}\varphi = \{e\}$ then P acts transitively on Q. Since conjugation is an order preserving action, and Q contains at least one element of order 2 (by Cauchy's theorem), every element $q \in Q$ is of order 2. Now, if $a, b \in Q$ are distinct nontrivial elements, $a = a^{-1}$, $b = b^{-1}$ and $(ab)^2 = e$ implies $ab = b^{-1}a^{-1} = ba$. Thus, Q must be Abelian. It follows that $Q \simeq Z_2 \times Z_2 \times Z_2$ (since this is the only group of order 8, up to isomorphism, such that every nontrivial element has order 2). ◂

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

(a) Let $a \in R$. Show that $a \in \operatorname{Rad}(R)$ 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 $\operatorname{Rad}(R[X]) = 0$.

Solution. ▸ For part (a), $\implies$ seeking a contradiction, suppose that $1 + ab$ is not a unit. By Krull's theorem, there exists a maximal ideal $\mathfrak{m}$ containing $1 + ab$. However, since $a \in \mathfrak{m}$ for every maximal ideal $\mathfrak{m}$ in R, $a \in \mathfrak{m}$. This implies that $ab \in \mathfrak{m}$ so $1 + ab - ab = 1 \in \mathfrak{m}$. This contradicts the assumption that $\mathfrak{m}$ is a maximal ideal. Thus, $1 + ab$ must have been a unit.

$\impliedby$ On the other hand, suppose $1 + ab$ is a unit for every $b \in R$. If $a \notin \operatorname{Rad} R$, then $a \notin \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$. By maximality, $(a) + \mathfrak{m} = R$, i.e., there exists $x \in R$ and $m \in \mathfrak{m}$ such that $ax + m = 1$. Thus, $m = 1 - ax = 1 + a(-x)$, but $1 + ab$ is a unit for every $b \in R$. This contradicts the fact that $\mathfrak{m}$ is a maximal ideal.

For part (b), by part (a), $f \in \operatorname{Rad}(R[X])$ if and only if $1 + fg$ is a unit for every $g \in R[X]$. Since the only units in $R[X]$ are in R, this implies that $1 + fg \in R$ for every $g \in R[X]$. This is true if and only if $f = 0$ for otherwise $1 + fX$ is a polynomial contained in R, but $R \cap (x) = \{0\}$. Thus, $\operatorname{Rad} R = \{0\}$. ◂

Exercise 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. ▸ For part (a), pick $f \in \mathfrak{p}$ of degree n. Then

$$f(X) = a_n X^n + \cdots + a_1 X + a_0.$$

Since R is a u.f.d., we can take the $a = \gcd\{a_n, \ldots, a_1, a_0\}$ and $b_i \in R$ such that $a_i = ab_i$. Then,

$$g(X) = b_n X^n + \cdots + b_1 X + b_0$$

is a primitive polynomial since, by construction $\gcd\{b_n, \ldots, b_1, b_0\} = 1$.

For part (b), it is clear that $(g) \subseteq \mathfrak{p}$. Let $f \in \mathfrak{p}$ and $F = \operatorname{Frac} R$. To see the reverse containment note that g is irreducible in R since, by Gauß's lemma, if $g = pq$ for some nontrivial ($\deg > 0$) polynomials $p, q \in F[X]$, then there exists $a, b \in F[x]$ such that $p' = ap, q' = bq \in R[X]$ and $g = p'q'$. By primality of $\mathfrak{p}$, this implies either $p' \in \mathfrak{p}$ or $q' \in \mathfrak{p}$. But this is an impossibility since g is of minimal degree in $\mathfrak{p}$. Now, let $f \in \mathfrak{p}$. Then, embedding R in its field of fractions F, by the Euclidean algorithm there exists $p, r \in F[X]$ with $\deg r < \deg g$ or $r = 0$ such that $f = pg + r$. Clearing denominators if necessary, r (or some multiple of it) is in $\mathfrak{p}$. Thus, $r = 0$ for otherwise, we contradict the minimality of $\deg g$ in $\mathfrak{p}$. Thus, $(g) = \mathfrak{p}$ as was to be shown. ◂

Exercise 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. ▸ We show that every polynomial $f \in k[X]$ has a root in k. Let K be the splitting field of f. Then $[K : k] = 2^\alpha m$ for some odd positive integer m. Let $G = \operatorname{Gal}(K/k)$ and let P be a 2-Sylow subgroup of G. By the Galois correspondence, K^P is a subfield of K of index $[G : P] = m$ over k. Since every extension over a field of characteristic 0 is separable, by the primitive element theorem, $K^P = K(\alpha)$ where α is the root of some irreducible polynomial f of degree m (namely, its minimal polynomial). But by assumption, f has a root in α. Thus, $k(\alpha) \subseteq k$. Thus, the degree of the splitting field must be $[K : k] = 2^\alpha$. Thus, $\operatorname{card} G = 2^\alpha$ so G is has a normal subgroup of order p^k for every $0 \leq k \leq \alpha$. Take N of index $[G : N] = 2$. Then, by the primitive element theorem $K^N = k(\beta)$ for β the root of polynomial g of degree 2. Thus, $k(\beta) \subseteq k$. Repeat this method recursively until $\alpha = 0$. Thus, k is algebraically closed. ◂

Exercise 7. Let $k \subseteq K$ be a finite Galois extension with Galois group $\mathrm{Gal}(K/k)$, let L be a field with $k \subseteq L \subseteq K$, and set $H = \left\{ \sigma \in \mathrm{Gal}(K/k) : \sigma(L) = L \right\}$.

(a) Show that H is the normalizer of $\mathrm{Gal}(K/L)$ in $\mathrm{Gal}(K/k)$.

(b) Describe the group $H/\mathrm{Gal}(K/L)$ as an automorphism group.

Solution. ▸ For part (a), let N denote the normalizer of $\mathrm{Gal}(K/L)$ in $\mathrm{Gal}(K/k)$. Then for any $\sigma \in H$, $\tau \in \mathrm{Gal}(K/L)$ and $x \in L$ we have

$$\begin{aligned} \sigma^{-1} \circ \tau\sigma(x) &= \sigma^{-1}(\tau(\sigma(x))) \\ &= \sigma^{-1}(\sigma(x)) \\ &= x. \end{aligned}$$

Thus, $\sigma \circ \tau\sigma^{-1}$ fixes L so $\sigma \circ \tau\sigma^{-1} \in \mathrm{Gal}(K/L)$ so $H \subseteq N$. On the other hand, if $\sigma \in N$ then we claim $\sigma(L) = L$. Otherwise there exists $x \in L$ such that $\sigma(x) \notin L$. Since K is Galois over k, it is Galois over L. Thus, there is an element $\tau \in \mathrm{Gal}(K/L)$ such that $\tau \circ \sigma(x) \neq \sigma(x)$. Thus, $\sigma^{-1} \circ \tau\sigma(x) \neq x$ so $\sigma^{-1} \circ \tau\sigma \notin \mathrm{Gal}(K/L)$. This is a contradiction. Thus, we conclude that $H = N$.

For part (b), we say that $H/\mathrm{Gal}(K/L)$ is precisely the automorphisms on L which do not leave L. ◂

2.2 Ulrich: Summer 2006

Exercise 1. Let G be a group of order $2n$, where n is odd. Show that G as a subgroup of index 2. (*Hint*: embed G into S_{2n}).

Solution. ▸

◂

Exercise 2. Let G be a group of odd order and let H be a normal subgroup of order 5. Show that H is in the center of G.

Solution. ▸ ◂

Exercise 3. Show that up to isomorphism, there are at most two groups of order 147 having an element of order 49.

Solution. ▸ ◂

Exercise 4. Let R be a principal ideal domain and $\mathfrak{m}$ a maximal ideal of the polynomial ring $R[X]$ with $\mathfrak{m} \cap R \neq \{0\}$. Show that $\mathfrak{m} = (p, f)$ for some prime element p of R and some monic irreducible polynomial f in $R[X]$.

Solution. ▸ ◂

Exercise 5. Let $k \subseteq K$ be a normal extension of fields of characteristic $p > 0$ with $G = \mathrm{Aut}_k(K)$. Show that the extension $k \subseteq K^G$ is purely inseparable.

Solution. ▸ Take $\alpha \in K^G$. Then, since $\alpha \in K$ and K is a normal extension, α is the root of some polynomial $f \in k[X]$. Then f factors completely over K and G acts transitively on the roots of f. But σ fixes every element in K^G so a is the only root of f. Thus, $f = (X - \alpha)^n$ for some $n \in \mathbb{N}$ and we have K^G is purely inseparable. ◂

Exercise 6. Let $k \subseteq K_1$ and $k \subseteq K_2$ be finite a Galois extension contained in a common field, and write $K = K_1K_2$.

(a) Show that the extension $k \subseteq K$ is finite Galois.

(b) Show that the Galois group $\mathrm{Gal}(K/k)$ is isomorphic to the subgroup $H = \left\{ (\sigma, \tau) : \sigma\restriction_{K_1 \cap K_2} = \tau\restriction_{K_1 \cap K_2} \right\}$ of $\mathrm{Gal}(K_1/k) \times \mathrm{Gal}(K_2/k)$.

Solution. ▸ ◂

Exercise 7. Let p be a prime number, $\zeta \in \mathbb{C}$ a primitive pth root of unity and $K = \mathbb{Q}(\zeta)$. Determine those p for which K has a unique maximal power subfield $k \subsetneq K$.

Solution. ► ◄

2.3 Ulrich: Summer 2009

Exercise 1. Let G be a group such that $G/Z(G)$ is Abelian, and let $H \neq \{e\}$ be a normal subgroup of G. Show that $H \cap Z(G)$. (*Hint*: Consider the commutator subgroup G' of G).

Solution. ▸ ◂

Exercise 2. Let G be a group of order 150. Show that G has a normal subgroup of order 25. (*Hint*: You may want to show that G has a normal subgroup of order 5 or 25.)

Solution. ▸ ◂

Exercise 3. Show that up to isomorphism, there are at most three non-Abelian groups of order 70.

Solution. ▸ ◂

Exercise 4. Let R be a unique factorization domain with quotient field K, let $K \subseteq L$ be a field extension, and let α be an element of L that is algebraic over K. Consider the subgring $R[\alpha]$ of L. Find an ideal I of the polynomial ring $R[X]$ so that $R[\alpha] \cong R[X]/I$ (*Hint*: Consider the minimal polynomial of α over K.)

Solution. ▸ ◂

Exercise 5. Let k be a field of characteristic $p > 0$, and let $k \subseteq K$ be an algebraic field extension of finite inseparable degree.

(a) Show that there exists $e \in \mathbb{N}$ such that $kK^{p^n} = kK^{p^e}$ for every $n \geq e$.

(b) Show that the inseparable degree of $k \subseteq K$ in $\left[K : kK^{p^e}\right]$ for e as in (a).

Solution. ▸ ◂

Exercise 6. Let k be a field, let $f[X] \in k[X]$ be a separable polynomial of degree n whose Galois group is isomorphic to S_n, and let α be a root of $f(X)$ in some algebraic closure $\bar{k}$.

(a) Show that $f(X)$ is irreducible.

(b) Show that $\mathrm{Aut}_k\left(k(\alpha)\right) = \{\mathrm{id}_k\}$ if $n \geq 3$.

(c) Show that $\alpha^n \notin k$ if $n \geq 4$.

Solution. ▸ ◂

Exercise 7. Determine the Galois group (up to isomorphism) of the polynomial $f = X^4 - 4X^2 + 2$ over $\mathbb{Q}$. Find all intermediate fields between $\mathbb{Q}$ and the splitting field of f over $\mathbb{Q}$.

Solution. ▸ ◂

References

[1] D.S. Dummit and R.M. Foote. *Abstract Algebra*. Wiley, 2004.

[2] I.N. Herstein. *Topics in algebra*. Xerox College Pub., 1975.

[3] T.W. Hungerford. *Algebra*. Graduate Texts in Mathematics. Springer New York, 2003.

[4] James S. Milne. Group theory (v3.13), 2013. Available at `www.jmilne.org/math/`.

[5] James S. Milne. Fields and galois theory (v4.50), 2014. Available at `www.jmilne.org/math/`.