

MA553: Qual Preparation

Carlos Salinas

May 1, 2016

Contents

Contents	1
1 MA 553 Spring 2016	2
1.1 Homework	2
Bibliography	12

MA 553 Spring 2016

This is material from the course MA 533 as 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].

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

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

Proof. Without loss of generality, we may assume $n < m$; otherwise, by the fundamental theorem of arithmetic, there exist q and r with $r < m$ such that $n = qm + r$ so $a^n = a^{qm+r} = a^{qm}a^r = a^r$. ■

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 $|ab| = \text{lcm}(m, n)$.

Proof. ■

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 $HK \simeq H \times K$.

Proof. ■

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

Proof.



Homework 2

Problem 5. Let G be the group of order $2^3 \cdot 3$, $n \geq 2$. Show that G has a normal 2-subgroup $\neq \{e\}$.

Proof. ■

Problem 6. 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 .

Proof. ■

Problem 7. Let G be a subgroup of order pqr , $p < q < r$ primes. Show that the r -Sylow subgroup of G is normal in G .

Proof. ■

Problem 8. 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.

Proof. ■

Problem 9. Show that the only simple groups $\neq \{e\}$ of order < 60 are the groups of prime order.

Proof. ■

Homework 3

Problem 10. Let G be a finite group, p a prime number, N the intersection 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 .

Proof. ■

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

Proof. ■

Problem 12. 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 $\varphi(\sigma)(a_i) = a_{\sigma(i)}$. Show that φ is well-defined and an isomorphism of groups.

Proof. ■

Problem 13. Determine all groups of order 18.

Proof. ■

Homework 4

Problem 14. Let p be a prime and let G be a nonAbelian group of order p^3 . Show that $G' = Z(G)$.

Proof. ■

Problem 15. 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 .

Proof. ■

Problem 16. Let p be an odd prime. Determine all groups of order p^3 .

Proof. ■

Problem 17. Show that $(S_n)' = A_n$.

Proof. ■

Problem 18. Show that every group of order < 60 is solvable.

Proof. ■

Problem 19. Show that every group of order 60 that is simple (or not solvable) is isomorphic to A_5 .

Proof. ■

Homework 5

Problem 20. Find all composition series and the composition factors of D_6 .

Proof. ■

Problem 21. Let T be the subgroup of $\text{GL}(n, \mathbb{R})$ consisting of all upper triangular invertible matrices. Show that T is solvable.

Proof. ■

Problem 22. 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 $x \in \mathbb{Z}$.

Proof. ■

Problem 23. (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 $\mathbb{Z}[i]$.

Proof. ■

Homework 6

Problem 24. 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.

Proof. ■

Problem 25. Let R be a PID and p a prime ideal of $R[X]$. Show that p is principal or $p = (a, f)$ for some $a \in R$ and some monic $f \in R[X]$.

Proof. ■

Problem 26. Let k be a field and $n \geq 1$. Show that $Z^n + Y^3 + X^2 \in k(X, Y)[Z]$ is irreducible.

Proof. ■

Problem 27. 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.

Proof. ■

Problem 28. Show that $X^{3^n} + 2 \in \mathbb{Q}(i)[X]$ is irreducible.

Proof. ■

Homework 7

Problem 29. 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).

Proof. ■

Problem 30. 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 $[k(\sqrt{a}, \sqrt{b}) : k] = 4$.

Proof. ■

Problem 31. Let R be a UFD, but not a field, and write $K := \text{Quot}(R)$. Show that $[\bar{K} : k] = \infty$.

Proof. ■

Problem 32. Let $k \in K$ be an algebraic field extension. Show that every k -homomorphism $\delta : K \rightarrow K$ is an isomorphism.

Proof. ■

Problem 33. Let K be the splitting field of $X^6 - 4$ over \mathbb{Q} . Determine K and $[K : \mathbb{Q}]$.

Proof. ■

Homework 8

Problem 34. Let k be a field, $f \in k[X]$ a polynomial of degree $n \geq 1$, and K the splitting field of f over k . Show that $[K : k] \mid n!$.

Proof. ■

Problem 35. 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 that

- (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) $f(x+a) = \sum \Delta_n(f)(a) X^n$.
- (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 $\Delta_n(f)(a) \neq 0$.

Proof. ■

Problem 36. Let $k \subset K$ be a finite field extension. Show that k is perfect if and only if K is perfect.

Proof. ■

Problem 37. 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 .

Proof. ■

Problem 38. 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 $k(X^p, Y^p) \subset L \subset k(X, Y)$.

Proof. ■

Homework 9

Problem 39. 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.

Proof. ■

Problem 40. 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 δ .

Proof. ■

Problem 41. Let $k \subset K = k(\alpha, \beta)$ 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 $K = k(\alpha + \beta)$.

Proof. ■

Problem 42. Let $f(x) \in \mathbb{F}_q[X]$ be irreducible. Show that $f(X) \mid X^{q^n} - X$ if and only if $\deg f(X) \mid n$.

Proof. ■

Problem 43. Show that $\text{Aut}_{\mathbb{F}_q}(\bar{\mathbb{F}}_q)$ is an infinite Abelian group which is torsionfree (i.e., $\delta^n = \text{id}$ implies $\delta = \text{id}$ or $n = 0$).

Proof. ■

Problem 44. Show that in a finite field, every element can be written as a sum of two perfect squares.

Proof. ■

Bibliography

- [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.