MA553: Qual Preparation

Carlos Salinas

July 1, 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 [Hun03]. Other resources include [DF04] and (to a lesser extent) [Her75]. I may also cite Milne's *Group Theory*, *Field Theory*, and *Commutative Algebra: A Primer* notes, respectively, [Mil13], [Mil14], 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 $\operatorname{char} k$
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 $\{1, \ldots, n\}$
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
$X \simeq Y$	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

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

► **Proof**. 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

$$\begin{aligned}(a^n)^{m/(m,n)} &= a^{nm/(m,n)} \\ &= a^{mn/(m,n)} \\ &= (a^m)^{n/(m,n)} \\ &= e^{n/(m,n)} \\ &= e.\end{aligned} \tag{1}$$

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

On the other hand, by Theorem 3.4 (iv) from [Hun03, Ch. I §3.3, p. 35] 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

$$mk = (m,n)m'k = (m,n)n'\ell = n\ell \tag{2}$$

so

$$m'k = n'\ell. \tag{3}$$

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 $|ab| = mn/(m,n)$.

► **Proof**. Let ℓ denote the order of ab. Now, playing around with powers of ab, we have

$$\begin{aligned}(ab)^n &= a^n b^n \\ &= a^n \\ &\neq e\end{aligned} \tag{4}$$

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 $HK \simeq H \times K$.

► **Proof**. (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 $HK \simeq H \times K$, consider the map $\varphi\colon HK \to (HK/K) \times (HK/H)$ given by $\varphi(hk) := (\pi_K(h), \pi_H(k))$ where $\pi_H\colon HK \to HK/H$ and $\pi_K\colon HK \to HK/K$ are quotient maps. By the first (or second) isomorphism theorem, $H \simeq HK/H$ and $K \simeq HK/H$ so $HK \simeq H \times K$. ◄

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

► **Proof**. Suppose that 6 has a subgroup of order 6 say H. Then, by Cauchy's theorem, H contains an element h of order 2, 3 or 6. If the order of h is 6, H must be cyclic and hence normal in A_4. But A_4 is simple. If h has order 2, then the subgroup generated by h is normal in G which, as we previously mentioned, is impossible. Lastly, if h has order 3 then h must be a product of disjoint 3 cycles. ◄

1.1.2 Homework 2

Problem 1. 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 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.

► **Proof.** ◄

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.

► **Proof.** ◄

Problem 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 $\varphi(G) \not\subset A_n$ 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 5. Show that the only simple groups $\neq \{e\}$ of order < 60 are the groups of prime order.

► **Proof.** ◄

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.

▶ **Proof**. ◀

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

▶ **Proof**. ◀

Problem 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.

▶ **Proof**. ◀

Problem 4. Determine all groups of order 18.

▶ **Proof**. ◀

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 $G' = Z(G)$.

► **Proof**. ◄

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.

► **Proof**. ◄

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

► **Proof**. ◄

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

► **Proof**. ◄

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

► **Proof**. ◄

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

► **Proof**. ◄

1.1.5 Homework 5

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

▶ **Proof**. ◀

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

▶ **Proof**. ◀

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

▶ **Proof**. ◀

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

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

▶ **Proof**. ◀

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.

▶ **Proof**. ◀

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

▶ **Proof**. ◀

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.

▶ **Proof**. ◀

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

▶ **Proof**. ◀

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

▶ **Proof**. ◀

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).

▶ **Proof**. ◀

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

▶ **Proof**. ◀

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

▶ **Proof**. ◀

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

▶ **Proof**. ◀

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

▶ **Proof**. ◀

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 $[K : k] \mid n!$.

► **Proof.** ◄

Problem 2. Let k be a field and $n \geq 0$. Define a map $\Delta_n \colon k[X] \to k[X]$ by $\Delta_n\big(\sum a_i X^i\big) = \sum a_i \binom{i}{n} X^{i-n}$. 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 $\Delta_n(f)(a) \neq 0$.

► **Proof.** ◄

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

► **Proof.** ◄

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.

► **Proof.** ◄

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

► **Proof.** ◄

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.

► **Proof**. ◄

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 $\delta \colon k \to L$ be an embedding. Show that $k \subset K$ is purely inseparable if and only if there exists exactly one embedding $\tau \colon K \to L$ extending δ.

► **Proof**. ◄

Problem 3. 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 4. Let $f(X) \in \mathbb{F}_q[X]$ be irreducible. Show that $f(X) \mid X^{q^n} - X$ if and only if $\deg f(X) \mid n$.

► **Proof**. ◄

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

► **Proof**. ◄

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

► **Proof**. ◄

1.1.10 Homework 10

Problem 1. Let $k \subset K = k(\alpha)$ be a simple field extension, let $G = \{\delta_1, \ldots, \delta_n\}$ be a finite subgroup of $\mathrm{Aut}_k(K)$, 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 α over K^2 and that $K^G = k(a_0, \ldots, a_{n-1})$.

► **Proof**. ◄

Problem 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 $[k(X) : k(u)] = \max\{\deg f, \deg g\}$.

► **Proof**. ◄

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

► **Proof**. ◄

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

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

► **Proof**. ◄

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

► **Proof**. ◄

1.1.11 Homework 11

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

▶ **Proof**. ◀

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 $k[X]$.

▶ **Proof**. ◀

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 $G \simeq C_4$.
(iii) If neither b nor $b(a^2 - 4b)$ is a square in k, then $G \simeq D_4$.

▶ **Proof**. ◀

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 $\mathbb{Q}$.

▶ **Proof**. ◀

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 $\mathbb{Q}$?

▶ **Proof**. ◀

1.1.12 Homework 12

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

► **Proof.** ◄

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

► **Proof.** ◄

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 $-4a^3 - 27b^2$.

► **Proof.** ◄

Problem 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 $\Phi(X) = \Phi_{p_1 \cdots p_s}(X^{{p_1}^{r_1 - 1} \cdots {p_s}^{r_s - 1}})$.
(b) For a prime number p with $p \nmid n$ show that $\Phi_{pn}(X) = \Phi_n(X^p)/\Phi_n(X)$.

► **Proof.** ◄

1.1.13 Homework 13

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

▶ **Proof**. ◀

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

▶ **Proof**. ◀

Problem 3. Let $k \subset K$ be an extension of finite fields. Show that N_k^K and Tr_k^K are surjective maps from K to k.

▶ **Proof**. ◀

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 $\mathrm{Aut}_k(k(\alpha)) = \{\mathrm{id}\}$.
(c) Show that $\alpha^n \notin k$ if $n \geq 4$.

▶ **Proof**. ◀

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

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

▶ **Proof**. ◀

References

[DF04] D.S. Dummit and R.M. Foote. *Abstract Algebra*. Wiley, 2004.

[Her75] I.N. Herstein. *Topics in algebra*. Xerox College Pub., 1975.

[Hun03] T.W. Hungerford. *Algebra*. Graduate Texts in Mathematics. Springer New York, 2003.

[Mil13] James S. Milne. Group theory (v3.13), 2013. Available at www.jmilne.org/math/.

[Mil14] James S. Milne. Fields and galois theory (v4.50), 2014. Available at www.jmilne.org/math/.