MA553: Spring 2016 Homework

Carlos Salinas

April 6, 2016

1 Course notes

Taken from Hungerford's *Algebra*. This first section will cover the relevant group theory part.

1.1 Group Theory

Semigroups, Monoids and Groups

If G is a nonempty subset, a *binary operation* on G is a function $G \times G \to G$. There are several commonly noted notations for the image of (a, b) under the binary operation: ab (multiplicative notation), $a + b$ (additive notation), $a{\cdot}b$, $a * b$, etc. For convenience we shall generally use multiplicative notation throughout this chapter and refer to ab as the *product* of a and b. A set may have several binary operations defined on it (for example, addition and multiplication on $\mathbf{Z}$ given by $(a, b) \mapsto a + b$ or $(a, b) \mapsto ab$ respectively).

Definition 1. A *semigroup* is a nonempty set G together with a binary operation on G which is

(a) associative: $a(bc) = (ab)c$ for all $a, b, c \in G$;

a *monoid* is a semigroup G which contains a

(b) two-sided identity element $e \in G$ such that $ae = ea = a$ for all $a \in G$.

A *group* is a monoid G such that

(c) for every $a \in G$ there exists a (two-sided) *inverse* element $a^{-1} \in G$ such that $aa^{-1} = a^{-1}a = e$.

A semigroup G is said to be *Abelian* or *commutative* if its binary operation is

(d) commutative: $ab = ba$ for all $a, b \in G$.

Our principal interests are groups, however semigroups and monoids are convenient for stating certain certain theorems in the most generality. Examples are given below. The *order* of a group G is the cardinality of the set G. G is said to be finite if $|G|$ is finite (otherwise, it is said to be infinite).

Theorem 1 (1.2). *If G is a monoid, then the identity element e is unique. If G is a group, then*

(a) *$a \in G$ and $aa = a \implies a = e$;*

(b) *for all $a, b, c \in G$, $ab = ac \implies b = c$ and $ba = ca \implies b = c$ (left and right cancellation);*

(c) *for each $a \in G$, the inverse element a^{-1} is unique;*

(d) *for each $a \in G$, $\left(a^{-1}\right)^{-1} = a$;*

(e) *for $a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$;*

(f) *for $a, b \in G$ the equation $ax = b$ and $ya = b$ have unique solutions in G: $x = a^{-1}b$ and $y = ba^{-1}$.*

Proposition 2 (1.3). *Let G be a semigroup. Then G is a group if and only if the following conditions hold:*

(i) *there exists an identity element $e \in G$ such that $ea = a$ for all $a \in G$ (left identity element);*

(ii) *for each* $a \in G$*, there exists an element* $a^{-1} \in G$ *such that* $a^{-1}a = e$ *(left inverse).*

Sketch of the proof. The direction $\Longrightarrow$ is trivial. $\Longleftarrow$: By Theorem 1.2(i) is true under the hypotheses. $G \neq \varnothing$ since $e \in G$. If $a \in G$, then (ii) $(aa^{-1})(aa^{-1}) = a(a^{-1}a)a^{-1} = aea^{-1} = aa^{-1}$ and hence $aa^{-1} = e$ by Theorem 1.2(i). Thus a^{-1} is a two-sided inverse of a. Since $ae = a(a^{-1}a) = (aa^{-1})a = ea = a$ for every $a \in G$, e is a two-sided identity. Therefore, G is a group by Definition 1.1. ∎

Proposition 3 (1.4). *Let* G *be a semigroup. Then* G *is a group if and only if for all* $a, b \in G$ *the equations* $ax = b$*,* $ya = b$ *have solutions in* G*.*

1.2 Ring Theory

1.3 Field Theory

2 Homework 1

Problem 2.1. 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. ∎

Problem 2.2. 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 $|ab| = \operatorname{lcm}(m,n)$.

Proof. ∎

Problem 2.3. 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 $HK \cong H \times K$.

Proof. ∎

Problem 2.4. Show that A_4 has no subgroup of order 6 (although $6 \mid 12 = |A_4|$).

Proof. ∎

3 Homework 2

Problem 3.1. 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 3.2. 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 3.3. 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 3.4. 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 $\phi(a)$.

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

Proof. ∎

4 Homework 3

Problem 4.1. 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 4.2. 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 4.3. 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 4.4. Determine all groups of order 18.

Proof. ∎

5 Homework 4

Problem 5.1. Let p be a prime and let G be a nonAbelian group of order p^3. Show that $G' = Z(G)$.

Proof. ∎

Problem 5.2. 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 5.3. Let p be an odd prime. Determine all groups of order p^3.

Proof. ∎

Problem 5.4. Show that $(S_n)' = A_n$.

Proof. ∎

Problem 5.5. Show that every group of order < 60 is solvable.

Proof. ∎

Problem 5.6. Show that every group of order 60 that is simple (or not solvable) is isomorphic to A_5.

Proof. ∎

6 Homework 5

Problem 6.1. Find all composition series and the composition factors of D_6.

Proof. ∎

Problem 6.2. Let T be the subgroup of $\mathrm{GL}(n, \mathbf{R})$ consisting of all upper triangular invertible matrices. Show that T is solvable.

Proof. ∎

Problem 6.3. Let $p \in \mathbf{Z}$ 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 $x \in \mathbf{Z}$.

Proof. ∎

Problem 6.4. (a) Show that the following are equivalent for an odd prime number $p \in \mathbf{Z}$:

- (i) $p \equiv 1 \mod 4$.
- (ii) $p = a^2 + b^2$ for some a, b in $\mathbf{Z}$.
- (iii) p is not prime in $\mathbf{Z}[i]$.

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

Proof. ∎

7 Homework 6

Problem 7.1. 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 elemnets and the intersection of any two principal ideals is again principal.

Proof. ∎

Problem 7.2. 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 7.3. 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 7.4. 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 7.5. Show that $x^{3^n} + 2 \in \mathbf{Q}(i)[x]$ is irreducible.

Proof. ∎

8 Homework 7

Problem 8.1. 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 8.2. 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 $\left[k(\sqrt{a}, \sqrt{b}) : k\right] = 4$.

Proof. ∎

Problem 8.3. Let R be a UFD, but not a field, and write $K = \mathrm{Quot}(R)$. Show that $[\bar{K} : k] = \infty$.

Proof. ∎

Problem 8.4. Let $k \in K$ be an algebraic field extension. Show that every k-homomorphism $\delta \colon K \to K$ is an isomorphism.

Proof. ∎

Problem 8.5. Let K be the splitting field of $x^6 - 4$ over $\mathbf{Q}$. Determine K and $[K : \mathbf{Q}]$.

Proof. ∎

9 Homework 8

Problem 9.1. 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 9.2. Let k be a field and $n \geq 0$. Define a map $\Delta_n \colon k[x] \to k[x]$ by $\Delta_n\big(\sum a_i x^i\big) \coloneqq \sum a_i \binom{i}{n} x^{i-n}$. 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 9.3. Let $k \subset K$ be a finite field extension. Show that k is perfect if and only if K is perfect.

Proof. ∎

Problem 9.4. Let K be the splitting field of $x^p - x - 1$ over $k = \mathbf{Z}/p\mathbf{Z}$. Show that $k \subset K$ is normal, separable, of degree p.

Proof. ∎

Problem 9.5. Let k be a field of characteristic $p > 0$, and $k(x, y)$ the field of rational functions in two variables.

(a) Show that $\big[k(x, y) : k(x^p, y^p)\big] = p^2$.

(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. ∎

10 Homework 9

Problem 10.1. 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 10.2. 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 10.3. 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 10.4. Let $f(x) \in \mathbf{F}_q[x]$ be irreducible. Show that $f(x) \mid x^{q^n} - x$ if and only if $\deg f(x) \mid n$.

Proof. ∎

Problem 10.5. Show that $\mathrm{Aut}_{\mathbf{F}_q}(\bar{\mathbf{F}}_q)$ is an infinite Abelian group which is torsionfree (i.e., $\delta^n = \mathrm{id}$ implies $\delta = \mathrm{id}$ or $n = 0$).

Proof. ∎

Problem 10.6. Show that in a finite field, every element can be written as a sum of two perfect squares.

Proof. ∎