Math 541

Worked Homework

Last Change: September 29, 2000

1 Home Work I

§1 Definition. A **field** is a set F equipped with two binary operations

$$F \times F \to F : (a, b) \mapsto a + b \qquad \textbf{(addition)}$$
$$F \times F \to F : (a, b) \mapsto a \cdot b \qquad \textbf{(multiplication)}$$

and two distinguished elements 0 (**zero**) and 1 (**one**) which satisfies the following laws:
Addition is associative:

$$\forall a \forall b \forall c \quad (a + b) + c = a + (b + c)$$

Addition is commutative:

$$\forall a \forall b \quad a + b = b + a$$

0 is an additive identity:

$$\forall a \quad a + 0 = a$$

Every number has an additive inverse:

$$\forall a \exists b \quad a + b = 0.$$

Multiplication is associative:

$$\forall a \forall b \forall c \quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$$

Multiplication is commutative:

$$\forall a \forall b \quad a \cdot b = b \cdot a$$

1 is an multiplicative identity:

$$\forall a \quad a \cdot 1 = 1 \cdot a = a$$

Every nonzero number has an multiplicative inverse:

$$\forall a \neq 0 \exists b \quad a \cdot b = b \cdot a = 1.$$

Multiplication is distributive over addition:

$$\forall a \forall b \forall c \quad a \cdot (b + c) = (a \cdot b) + (a \cdot c),$$

$$\forall a \forall b \forall c \quad (b + c) \cdot a = (b \cdot a) + (c \cdot a).$$

(This is the first law which involves both operations.)

§2 Lemma. $a + b_1 = 0$ and $a + b_2 = 0 \implies b_1 = b_2$

Proof: Assume $a + b_1 = 0$ and $a + b_2 = 0$. Then

$$\begin{array}{rcll} b_1 & = & b_1 + 0 & \text{(ident.)} \\ & = & b_1 + (a + b_2) & \text{(hyp.)} \\ & = & (b_1 + a) + b_2 & \text{(ass.)} \\ & = & (a + b_1) + b_2 & \text{(comm.)} \\ & = & 0 + b_2 & \text{(hyp.)} \\ & = & b_2 + 0 & \text{(comm.)} \\ & = & b_2 & \text{(ident.)} \end{array}$$

§3 Definition. Since a number a has exactly one additive inverse we can denote it by $[-a]$. Thus

$$b = [-a] \iff a + b = 0.$$

The operation of **subtraction** is defined by

$$a - b = a + [-b].$$

We use the brackets to emphasize the difference between the unary operation

$$F \to F : a \mapsto [-a]$$

and the binary operation

$$F \times F \to F : (a, b) \mapsto a - b.$$

§4 Theorem. $[-[-c]] = c$ for all $c \in F$.
Proof: Let $a = [-c]$, $b_1 = c$, $b_2 = [-[-c]]$ and use lemma 2. □

§5 Exercise. Prove the following for all $a, b, c, d \in F$:

(i) $[-(a+b)] = [-a] + [-b]$.

(ii) $(a-b) + (c-d) = (a+c) - (b+d)$.

(iii) $a - b = (a+c) - (b+c)$.

(iv) $(a-b) - (c-d) = (a-b) + (d-c)$.

Proof of (i): By the associative and commutative laws

$$(a+b) + ([-a] + [-b]) = (a + [-a]) + (b + [-b]).$$

Hence

$$(a+b) + ([-a] + [-b]) = 0 + 0 = 0$$

by the definition of the additive inverse. Hence $[-(a+b)] = ([-a] + [-b])$ by Lemma 2.

Proof of (ii):

$$\begin{array}{rcll} (a-b)+(c-d) & = & (a+[-b])+(c+[-d]) & \text{definition of } x-y \\ & = & (a+c)+([-b]+[-d]) & \text{ass. and comm.} \\ & = & (a+c)+[-(b+d)] & \text{by (i)} \\ & = & (a+c)-(b+d) & \text{definition of } x-y \end{array}$$

.

Proof of (iii): By (ii) with $c = d$ we have

$$(a-b) + (c-c) = (a+c) - (b+c).$$

But $c - c = c + [-c] = 0$ so $(a-b) + (c-c) = (a-b)$.
Proof of (iv): Read c for a, d for b, d for c, and c for d in (ii). The result is

$$(c-d) + (d-c) = (d+c) - (c+d) = 0 + 0 = 0.$$

Hence $[-(c-d)] = (d-c)$. Now add $a-b$ to both sides.

§6 Lemma. The multiplicative inverse is unique:

$$a \cdot b_1 = 1 \text{ and } a \cdot b_2 = 1 \implies b_1 = b_2$$

Proof: Like Lemma 2.

§7 Definition. We denote the multiplicative inverse by a^{-1}. Hence for $a, b \in F$

$$b = a^{-1} \iff a \cdot b = 1.$$

The operation of **division** is defined (for $a \in F$, $b \in F \setminus \{0\}$) by

$$a/b = a \cdot b^{-1}.$$

§8 Theorem. $(a^{-1})^{-1} = a$ for $a \in F \setminus \{0\}$.

Proof: Like theorem 4.

§9 Exercise. Prove the following for all $a, b, c, d \in F \setminus \{0\}$:

(i) $(a \cdot b)^{-1} = a^{-1} \cdot b^{-1}$

(ii) $\dfrac{a}{b} \cdot \dfrac{c}{d} = \dfrac{a \cdot c}{b \cdot d}$

(iii) $\dfrac{a}{b} = \dfrac{a \cdot c}{b \cdot c}$

(iv) $\dfrac{a}{b} \Big/ \dfrac{c}{d} = \dfrac{a}{b} \cdot \dfrac{d}{c}$

Proof: The proof is exactly the same as for Exercise 5. Simply replace $x+y$ by $x \cdot y$, $[-x]$ by x^{-1}, $x-y$ by x/y throughout.

§10 Theorem. $a \cdot 0 = 0$ for $a \in F$.

Proof: Choose $a \in F$. Then

$$\begin{aligned}
0 &= a - a && \text{(def, inv.)} \\
&= a \cdot 1 - a && \text{(ident.)} \\
&= a \cdot (0+1) - a && \text{(ident, comm.)} \\
&= (a \cdot 0) + (a \cdot 1)) - a && \text{(dist.)} \\
&= ((a \cdot 0) + a) - a && \text{(ident.)} \\
&= (a \cdot 0) + (a - a) && \text{(ass.)} \\
&= (a \cdot 0) + 0 && \text{(def, inv.)} \\
&= a \cdot 0 && \text{(ident.)}\square
\end{aligned}$$

§11 Exercise. Prove the following

(i) $\dfrac{a}{b}+\dfrac{c}{d}=\dfrac{(a\cdot d)+(c\cdot b)}{b\cdot d}$

(ii) $[-a]=[-1]\cdot a$

(iii) $[-a]\cdot[-b]=a\cdot b$

Proof of (i): By Lemma 9 part (iii)

$$\frac{a}{b}=\frac{a\cdot d}{b\cdot d}, \qquad \frac{c}{d}=\frac{c\cdot b}{d\cdot b}.$$

Hence by the definition of x/y

$$\frac{a}{b}=(a\cdot d)\cdot(b\cdot d)^{-1}, \qquad \frac{c}{d}=(c\cdot b)(d\cdot b).$$

Hence by $b\cdot d=d\cdot b$ and the distributive law

$$\frac{a}{b}+\frac{c}{d}=\big(a\cdot d+c\cdot b\big)\cdot(b\cdot d)^{-1}$$

so the result follows by the definition of x/y.

Proof of (ii): $a+[-1]\cdot a=1\cdot a+[-1]\cdot a=(1+[-1])\cdot a=0\cdot a=0$ by the distributive law and Theorem 10. Hence $[-1]\cdot a=[-a]$ by Lemma 2.

Proof of (iii): By part (ii) it is enough to prove this for $a=b=1$, i.e. to prove that $[-1]\cdot[-1]=1$. By Theorem 10 (and other laws) we have

$$0=\big([-1]+1\big)\cdot[-1]=[-1]\cdot[-1]+[-1].$$

Now add 1 to both sides and use the identity law $0+1=1$, the associative law

$$([-1]\cdot[-1]+[-1])+1=[-1]\cdot[-1]+([-1]+1),$$

and the inverse law $[-1]+1=0$, etc.

2 Home Work II

§12 Composition. Given mappings $f:X\to Y$ and $g:Y\to Z$ the **composition** of f and g is denoted $g\circ f$ (read " g *after* f") and defined by $g\circ f:X\to Z$ with

$$(g\circ f)(x)=g(f(x))$$

for $x \in X$. The operation of composition is associative:

$$(h \circ g) \circ f = h \circ (g \circ f).$$

For any set X the **identity map** I_X of X is the map $I_X : X \to X$ defined by $I_X(x) = x$ for $x \in X$. Note that for $f : X \to Y$ we have

$$f \circ I_X = I_Y \circ f = f.$$

§13 Maps act on sets. Suppose that $f : X \to Y$ $X_0 \subset X$ and $Y_0 \subset Y$. Define

$$f(X_0) = \{f(x) : x \in X_0\}$$

and

$$f^{-1}(Y_0) = \{x \in X : f(x) \in Y_0\}.$$

Theorem. **(i)** $I_X(X_0) = X_0$ and $g \circ f(X_0) = g(f(X_0))$. Hence **(ii)** If $f : X \to Y$ is one-one onto, then $f^{-1}(f(X_0)) = X_0$ and $f(f^{-1}(Y_0)) = Y_0$. (Warning: These last two formulas are not always true for maps which are not one-one onto.)

§14 Restriction and Extension. Suppose we are given a mapping $f : X \to Y$ and a subset $X_0 \subset X$. The **restriction of** f **to** X_0, denoted $f|X_0$, is the mapping $(f|X_0) : X_0 \to Y$ defined by

$$(f|X_0)(x) = f(x) \quad \text{for all } x \in X_0.$$

For example, if $f : \mathbb{R} \to \mathbb{R}$ is a mapping whose graph is the straight line given by $f(x) = 2x$, and if $[0, 1]$ denotes the unit interval, then $f|[0, 1]$, the restriction of f to $[0, 1]$, is a mapping whose graph is the closed line segment from the $(0, 0)$ to $(1, 2)$.

The opposite of *restricting* a mapping to a smaller source is *extending* a mapping to a larger source. Suppose $g : X \to Y$ is a mapping and $X \subset Z$. Then any mapping $h : Z \to Y$ is called an **extension of** g **to** Z if $h|X = g$, i.e., if

$$h(x) = g(x) \quad \text{for all } x \in X.$$

Thus, for example, if g is the mapping defined earlier by $g : X \to \mathbb{R} : x \mapsto \frac{1}{1-x}$ with source $X = \{x \in \mathbb{R} : x \neq 1\}$, then g has an extension $\tilde{g}$ defined by

$$\tilde{g}(x) = \begin{cases} \frac{1}{1-x} & \text{if } x \neq 1 \\ 0 & \text{if } x = 1. \end{cases}$$

The reader may recall from a calculus course that the mapping g described above is *continuous* on its source X, but *has no continuous extension* to $\mathbb{R}$. In particular, $\tilde{g} : \mathbb{R} \to \mathbb{R}$ is not continuous.

§15 Recall that for any set S the group of all permutations of S is denoted by $A(S)$; i.e.

$$f \in A(S) \iff f : S \to S, \quad \text{and } f \text{ is one-one and onto.}$$

§16 (Problem 1.4.14) Suppose $X_0 \subset X$, e.g.

$$X_0 = \{1, 2, \dots, m\}, \qquad X = \{1, 2, \dots, n\}$$

where $m \leq n$. Define $E : A(X_0) \to A(X)$ by

$$E(f)(x) = \begin{cases} f(x) & \text{for } x \in X_0, \\ x & \text{for } x \in X \setminus X_0, \end{cases}$$

for $f \in A(X_0)$. For $f, g \in A(X_0$ and $x \in X_0$ we have

$$E(f \circ g)(x) = f(g(x)) = E(f)\big(g(x)\big) = \big(E(f) \circ E(g)\big)(x)$$

(since $g(x) \in X_0$) while for $x \in X \setminus X_0$ we have

$$E(f \circ g)(x) = x = E(f)(x)\big(E(g)\big)(x) = E(f)\big(= E(f) \circ E(g)\big)(x).$$

In either case $E(f \circ g)(x) = \big(E(f) \circ E(g)\big)(x)$ so $E(f \circ g) = \big(E(f) \circ E(g)\big)$.

§17 (Problem 1.4.18) *Suppose $X_0 \subset X$ and define*

$$U(X, X_0) = \{f \in A(X) : f(X_0) = X_0\}.$$

Then $U(X, X_0)$ is a subgroup of $A(X)$, i.e.

(i) *$I_X \in U(X, X_0)$;*

(ii) *If $g \in U(X_0, X)$ and $f \in U(X, X_0)$ then $g \circ f \in U(X, X_0)$;*

(iii) *If $f \in U(X, X_0)$ then $f^{-1} \in U(X, X_0)$,*

Proof: **(i)** Since $I_X(X_0) = X_0$ we have $I_X \in U(X, X_0)$. **(ii)** If $g \in U(X, X_0)$ and $f \in U(X, X_0)$, then

$$g \circ f(X_0) = g(f(X_0)) = g(X_0) = X_0$$

so $g \circ f \in U(X, X_0)$. **(iii)** If $f \in U(X, X_0)$ then $f(X_0) = X_0$ so $X_0 = f^{-1}(X_0)$ so $f^{-1} \in U(X, X_0)$.

§18 (Problem 1.4.19) *For $f \in U(X, X_0)$ define $R(f) : X_0 \to X_0$ by*

$$R(f)(x) = f(x) \qquad \text{for } x \in X_0.$$

(Note that $f(x) \in X_0$ by the definition of $U(X, X_0)$.) Then

$$R : U(X, X_0) \to A(X_0)$$

and

$$R(g \circ f) = R(g) \circ R(f).$$

The proof is obvious. Since $R(E(g)) = g$ for $g \in A(X_0)$ it follows that R is onto.

§19 (Problem 1.4.20) Since any element of $A(X)$ is one-one onto we have

$$U(X, X_0) = U(X, X \setminus X_0).$$

Thus the set $R^{-1}(g)$ is in one-one correspondence with $A(X \setminus X_0)$. In particular, R is one-one when $X \setminus X_0$ consists of a single point.

3 Home Work III

§20 Problem 2.1.1 (b) Consider the set $\mathbb{Z}$ of integers with the operation

$$a * b = a + b + ab$$

is not a group. The one-one onto map $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(z) = z + 1$ satisfies

$$a * b = (a + 1) \cdot (b + 1) - 1 = f^{-1}(f(a) \cdot f(b))$$

for $a, b \in \mathbb{Z}$ (where $u \cdot v$ is the usual multiplication operation.) Thus $(\mathbb{Z}, *)$ satisfies the same laws as $(\mathbb{Z}, \cdot)$. In particular the associative and commutative laws hold and 0 is an identity:

$$0 * a = a * 0 = a$$

for all $a \in \mathbb{Z}$. However there is no inverse operation since

$$a * (-1) = -1$$

for all $a \in \mathbb{Z}$.

§21 2.2.3 Let $i \in \mathbb{Z}$. We say that a group G has *property* $P(i)$ iff the identity

$$(ab)^i = a^i b^i \qquad P(i)$$

holds for all $a, b \in G$.

Assume that there is an integer i for which the group G satisfies $P(i-1)$, $P(i)$, and $P(i+1)$. We show that the group G is abelian.

Step 1. If a group satisfies $P(i+1)$ and $P(i)$ then it satisfies

$$a^i b^i = b^i a^i \qquad Q(i)$$

for all $a, b \in G$. Proof: By $P(i+1)$

$$a(ba)^i b = (ab)^{i+1} = a^{i+1} b^{i+1} = a(a^i b^i) b.$$

Cancelling the a on the left and the b on the right gives

$$(ba)^i = a^i b^i.$$

Now use $P(i)$ to obtain $b^i a^i = (ba)^i = a^i b^i$.

Step 2. If a group satisfies $P(i)$ and $P(i-1)$ then it satisfies

$$a^{i-1} b^{i-1} = b^{i-1} a^{i-1} \qquad Q(i-1)$$

for all $a, b \in G$. Proof: Replace i by $i-1$ in Step 1.

Step 3. Now

$$(ab)^{i+1} = (ab)(ab)^i = (ab)a^i b^i = (ab)b^i a^i = (ab)(ba)^i$$

and

$$(ba)^i = (ba)(ba)^{i-1} = (ba)b^{i-1}a^{i-1} = (ba)a^{i-1}b^{i-1} = (ba)(ab)^{i-1}.$$

Hence

$$(ab)^{i+1} = (ab)(ba)(ab)^{i-1}.$$

Now multiply by $(ab)^{-1}$ on the left and $(ab)^{1-i}$ on the right.

§22 Remark. The problem in the book asks you to prove that *If G is a group for which $(ab)^i = a^i b^i$ for three consecutive integers i, then G is abelian.* To me the wording is ambiguous. Which is asserted?

$$[\forall i \in \mathbb{Z}\ P(i-1) \text{ and } P(i) \text{ and } P(i+1)] \implies G \text{ is abelian} \tag{1}$$

i.e.

$$\exists i \in \mathbb{Z}\ [P(i-1) \text{ and } P(i) \text{ and } P(i+1) \implies G \text{ is abelian}] \tag{1'}$$

or

$$\forall i \in \mathbb{Z}\ [P(i-1) \text{ and } P(i) \text{ and } P(i+1) \implies G \text{ is abelian}] \tag{2}$$

i.e.

$$[\exists i \in \mathbb{Z}\ P(i-1) \text{ and } P(i) \text{ and } P(i+1)] \implies G \text{ is abelian} \tag{2'}$$

However had the author intended (1) he would have said

$$[\forall i \in \mathbb{Z}\ P(i)] \implies G \text{ is abelian}$$

which is equivalent but shorter. The author must intend (2).

4 Homework IV

§23 Problem 2.4(2-3). Let S be a set and R a relation on S, i.e. $R \subset S \times S$. For $a, b \in S$ we write $a \equiv b$ instead of $(a, b) \in R$. We say that the relation R is

- **reflexive** iff $\forall a \in S\ \ a \equiv a$;
- **weakly reflexive** iff $\forall a \in S \exists b \in S\ \ a \equiv b$;
- **symmetric** iff $\forall a, b \in S\ \ a \equiv b \implies b \equiv a$;
- **transitive** iff $\forall a, b, c \in S\ \ a \equiv b,\ b \equiv c \implies a \equiv c$.

A reflexive relation is obviously weakly reflexive: take $b = a$. The relation defined in 2.4(2) is the empty relation $R = \emptyset$ on a nonempty set S. It is symmetric since for all $a, b \in S$ the implication $(a, b) \in \emptyset \implies (b, a) \in \emptyset$ is true: it has the form [false $\implies$ false]. Similarly the empty relation is transitive. The empty relation is not reflexive (or even weakly reflexive) on a nonempty set S: since $S \neq \emptyset$ there exists an $a \in S$; but for this a, we have $a \not\equiv b$, i.e. $(a,b) \notin \emptyset$ for all $b \in S$. The argument in 2.4(3) proves that a relation which is weakly reflexive, symmetric, and transitive is also reflexive.

§24 Problem 2.4(20) Recall that the transformation $T_{a,b}$ may be represented by the matrix

$$T_{a,b} = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$$

so

$$T_{a,b} \circ T_{a,b} = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} ac & ad+b \\ 0 & 1 \end{pmatrix}$$

and

$$T_{a,b}^{-1} = \begin{pmatrix} a^{-1} & -a^{-1}b \\ 0 & 1 \end{pmatrix}.$$

The conjugacy class $[T_{c,d}]$ of the element $T_{c,d}$ is the set

$$[T_{c,d}] := \left\{ T_{a,b} \circ T_{c,d} \circ T_{a,b}^{-1} \right\} : a, b \in \mathbb{R},\ a \neq 0 \right\}.$$

By matrix multiplication

$$T_{a,b} \circ T_{c,d} \circ T_{a,b}^{-1} = T_{c,g}, \qquad g = ad + b(1-c).$$

If $c \neq 1$ then every $g \in \mathbb{R}$ has the form $g = ad + b(1-c)$ with $a \neq 0$; we take $a = 1$ and $b = (g-d)/(c-1)$. If $c = 1$ and $d \neq 0$, then g has the form $g = ad + b(1-c)$ if and only if $g \neq 0$. Hence

$$\begin{aligned} [T_{c,d}] &= \left\{ T_{c,g} : g \in \mathbb{R} \right\} && \text{if } c \neq 1; \\ [T_{1,d}] &= \left\{ T_{1,g} : g \in \mathbb{R},\ g \neq 0 \right\} && \text{if } d \neq 0; \\ [T_{1,0}] &= \left\{ T_{1,0} \right\}. \end{aligned}$$

§25 Problem 2.4.(6-7) In cycle notation (see Chapter 3)

$$H = \{(), (12)\} \subset G = S_3$$

The left cosets are

$$H = \{(), (12)\}, \qquad (13)H = \{(13), (123)\}, \qquad (23)H = \{(23), (132)\}.$$

There are three left cosets and each is a two element set. The right cosets are

$$H = \{(), (12)\}, \qquad H(13) = \{(13), (132)\}, \qquad H(23) = \{(23), (123)\}.$$

There are three right cosets and each is a two element set. The right coset $H(13)$ is different from all three left cosets. In fact the only set which is both a left coset and a right coset is H itself.

5 Homework V

§26 Problem 2.5.16 *Suppose that G is a group and the $M \triangleleft G$ and $N \triangleleft G$ are normal subgroups. Let*

$$MN = \{mn : m \in M,\ n \in N\}.$$

Then $MN \triangleleft G$, i.e. MN is a normal subgroup of G.

Proof: There are four steps.

Step 1. $e \in MN$. Proof: Take $m = n = e$. Then $m \in M$ and $n \in N$ so $e = mn \in MN$.

Step 2. $x, y \in MN \implies xy \in MN$. Proof: Choose $x, y \in MN$. Then $x = m_1 n_1$ and $y = m_2 n_2$ for some $m_1, m_2 \in M$ and $n_1, n_2 \in N$. Then

$$xy = m_1 n_1 m_2 n_2 = m_1 (n_1 m_2 n_1^{-1})(n_1 n_2) = m' n'$$

where $m' = m_1(n_1 m_2 n_1^{-1}) \in M$ and $n' = n_1 n_2 \in N$. Therefore $xy \in MN$.

Step 3. $x \in MN \implies x^{-1} \in MN$. Proof: Choose $x \in MN$. Then $x = mn$ for some $m \in M$ and $n \in N$. Hence

$$x^{-1} = n^{-1} m^{-1} = (n^{-1} m^{-1} n) n^{-1} = m' n'$$

where $m' = (n^{-1} m^{-1} n) \in M$ and $n' = n^{-1} \in N$. Therefore $x^{-1} \in MN$.

Step 4. $x \in MN,\ g \in G \implies gxg^{-1} \in MN$. Choose $x \in MN$ and $g \in G$. Then $x = mn$ for some $m \in M$ and $n \in N$. Hence

$$gxg^{-1} = gmng^{-1} = (gmg^{-1})(gng^{-1}) = m' n'$$

where $m' = (gmg^{-1}) \in M$ and $n' = (gng^{-1}) \in N$. Therefore $gxg^{-1} \in MN$.

§27 Problem 2.5.21 Let S be a set having at least three elements and $A(S)$ be the group of all one-one onto maps from S to itself. For $s \in S$ define

$$H(s) = \{f \in H(S) : f(s) = s\}.$$

It is easy to see that $H(s)$ is a subgroup of $A(S)$. First, the identity map id_S is an element of $H(s)$ as $\mathrm{id}_S(x) = x$ for all $x \in S$ so in particular $\mathrm{id}_S(s) = s$, so $\mathrm{id}_S \in H(s)$. Second, if $f, g \in H(S)$ then $f(s) = s$ and $g(s) = s$ so $f \circ g(s) = f(g(s)) = f(s) = s$ so $f \circ g \in H(s)$. Third, if $f \in H(s)$, then $f(s) = s$ so $s = \mathrm{id}_S(s) = (f^{-1} \circ f) = f^{-1}(f(s)) = f^{-1}(s)$ so $f^{-1} \in H(s)$. Hence $H(s)$ is a subgroup of $A(S)$.

Now assume that the elements $s, s', s'' \in S$ are distinct. Choose $f \in A(S)$ so that $f(s') = s$ and $f(s'') = s''$. Choose $h \in A(S)$ so $h(s) = s$ and $h(s') = s''$. Then $h \in H(s)$ but $f \circ h \circ f^{-1}(s) = f(h(s')) = f(s'') = s'' \neq s$ so $f \circ h \circ f^{-1} \notin H(s)$. Hence $H(s)$ is not a normal subgroup of $A(S)$.

Remark. For $f \in A(S)$ and $s \in S$ we have

$$fH(s)f^{-1} = H(f(s)).$$

Suppose that $g \in fH(s)f^{-1}$. Then $g = f \circ h \circ f^{-1}$ where $h \in H(s)$, i.e. $h(s) = s$. Then

$$g(f(s)) = (f \circ h \circ f^{-1}) \circ f(s) = f(h(s)) = f(s)$$

so $g \in H(f(s))$. Conversely suppose that $g \in H(f(s))$, i.e. $g(f(s)) = f(s)$. Let $h = f^{-1} \circ g \circ f$. Then $h(s) = f^{-1} \circ g \circ f(s) = f^{-1}(g(f(s))) = f^{-1}(f(s)) = s$ so $h \in H(s)$. But $g = f \circ h \circ h^{-1}$ so $g \in fH(s)f^{-1}$.

6 Homework VI

§28 Problem 2.6.3-5 *Suppose that N is a normal subgroup of a groups G and that $\bar{M}$ is a subgroup of G/N. Let*

$$M = \{a \in G : aN \in \bar{M}\}.$$

Then

(2.6.3) *M is a subgroup of G and $N \subset M$.*

(2.6.4) *If $\bar{M} \lhd G/N$, then $M \lhd N$.*

(2.6.5) *If $\bar{M} \lhd G/N$, then $M/N = \bar{M}$.*

Proof: Let $\bar{G} = G/N$, and $\phi : G \to \bar{G}$ be the homomorphism defined by

$$\phi(a) = aN.$$

Then ϕ is an onto homomorphism and

$$M = \phi^{-1}(\bar{M}).$$

We prove M is a subgroup. (1) The identity e of G lies in M as $\phi(e)$ is the identity of $\bar{G}$ and henve lies in $\bar{M}$, so $e \in \phi^{-1}(\bar{M}) = M$. (2) Choose $a, b \in M$. Then $\phi(a), \phi(b) \in \bar{M}$. Hence $\phi(ab) = \phi(a)\phi(b) \in \bar{M}$. Hence $ab \in \phi^{-1}(\bar{M}) = M$. (3) Choose $a \in M$. Then $\phi(a) \in \bar{M}$. Hence $\phi(a^{-1}) = \phi(a)^{-1} \in \bar{M}$. Hence $a^{-1} \in \phi^{-1}(\bar{M}) = M$.

Assume that $\bar{M}$ is normal. Choose $a \in G$ and $m \in M$. Then $\phi(a) \in \bar{G}$ and $\phi(m) \in \bar{M}$. Hence $\phi(ama^{-1}) = \phi(a)\phi(m)\phi(a)^{-1} \in \bar{M}$. Hence $ama^{-1} \in \phi^{-1}(\bar{M}) = M$. This proves that M is normal.

The statement that $M/N = \bar{M}$ can be written as $\phi(M) = \bar{M}$, i.e. $\phi(\phi^{-1}(\bar{M})) = \bar{M}$. This latter formula is true for any onto map $\phi : G \to \bar{G}$ and any subset $\bar{M} \subset \bar{G}$.

7 Homework VII

§29 4.4-9. *Let $p > 2$ be a prime and let $U_p = \mathbb{Z}_p - \{0\}$ be the multiplicative group of the field $\mathbb{Z}_p$. Then the set*

$$S = \{x^2 : x \in U_p\}$$

of squares in U_p is a subgroup of index two.

Proof: $1 = 1^2$ so $1 \in S$. Suppose that $a, b \in S$. Then there exist $x, y \in U_p$ with $a = x^2$ and $b = y^2$. Then $ab = (xy)^2$ so $ab \in S$. Suppose $a \in S$. Then $a = x^2$ for some $x \in U_p$. Let $y \in U_p$ be the inverse of x. Then $xy = 1$. Hence $ay^2 = x^2y^2 = (xy)^2 = 1$. Hence $a^{-1} = y^2$ so $a^{-1} \in U_p$. The map

$$U_p \to S : x \mapsto x^2$$

is two-to-one onto (as $p > 2$) so $|U_p| = 2|S|$.

§30 (4.4-10) *Suppose m is a positive integer which is not a perfect square. Then the set*

$$\mathbb{Z}[\sqrt{m}] := \{a + b\sqrt{m} : a, b \in \mathbb{Z}\}$$

is a subring of $\mathbb{R}$.

Proof: (1) $\mathbb{Z}[\sqrt{m}]$ contains $0 = 0+0\sqrt{m}$. (2) $\mathbb{Z}[\sqrt{m}]$ is closed under addition and subtraction as

$$(a_1 + b_1\sqrt{m}) \pm (a_2 + b_2\sqrt{m}) = (a_1 \pm a_2) + (b_1 \pm b_2)\sqrt{m}.$$

(3) $\mathbb{Z}[\sqrt{m}]$ is closed under multiplication as

$$(a_1 + b_1\sqrt{m})(a_2 + b_2\sqrt{m}) = (a_1a_2 + mb_1b_2) + (a_1b_2 + b_1a_2)\sqrt{m}.$$

§31 (4.4-11)*Suppose m is as in 4.4-10 and that p is an odd prime. Let*

$$I_p = \{a + b\sqrt{m} \in \mathbb{Z}[\sqrt{m}] : 5|a \text{ and } 5|b\}.$$

Then I_p is an an ideal in $\mathbb{Z}[\sqrt{m}]$.

Proof: (1) I_p contains $0 = 0 + 0\sqrt{m}$ as $p|0$. (2) $\mathbb{Z}[\sqrt{m}]$ is closed under addition and subtraction. Choose $x_1, x_2 \in I_p$. Then $x_1 = a_1 + b_1\sqrt{m}$ and $x_2 = a_21 + b_2\sqrt{m}$ where $p|a_1$, $p|b_1$, $p|a_2$, $p|a_2$. Hence $p|(a_1+a_2)$ and $p|(b_1+b_2)$ so $x_1 \pm x_2 \in I_p$. (3) I_p is closed under multiplication by an element of $\mathbb{Z}[\sqrt{m}]$. Choose $x \in I_p$ and $z \in \mathbb{Z}[\sqrt{m}]$. Then $x = a + b\sqrt{m}$ where $p|a$ and $p|b$ and $z = c + d\sqrt{m}$ where $c, d \in \mathbb{Z}$. Then $p|(ac + mbd)$ and $p|(ad + bc)$ so

$$xz = (ac + mbd) + (ad + bc)\sqrt{m} \in I_p.$$

§32 (4.4-12,13) *Let p and m be as in 4.4-10 and suppose that m is not a square in U_p. Then $Z[\sqrt{m}]/I_p$ is a field of order p^2.*

Proof: The ring $\mathbb{Z}[\sqrt{m}]/I_p$ has order p^2 because every element $a + b\sqrt{m} \in \mathbb{Z}[\sqrt{m}]$ be be written uniquely in the form

$$a + b\sqrt{m} = (cp + r) + (dp + s)\sqrt{m}$$

where $c, d, r, s \in \mathbb{Z}$ and $0 \leq r < p$ and $0 \leq s < p$. (For uniqueness use the fact that If $a_1 + b_1\sqrt{m} = a_2 + b_2\sqrt{m}$ then $a_1 = a_2$ and $b_1 = b_2$ as $\sqrt{m}$

is irrational.) To show that $Z[\sqrt{m}]/I_p$ is a field we must show that every nonzero element has a multiplicative inverse. Choose $a+b\sqrt{m} \in Z[\sqrt{m}] \setminus I_p$; we must find integers u, v with

$$(a+b\sqrt{m})(u+v\sqrt{m}) \in 1 + I_p.$$

We try $u = wa$, $v = -wb$ so

$$(a+b\sqrt{m})(u+v\sqrt{m}) = w(a^2 - mb^2).$$

Since $\mathbb{Z}_p$ is a field, we can find an integer w with $w(a^2 - mb^2) \equiv 1 (\operatorname{mod} p)$ so long as $a^2 - mb^2 \not\equiv 0 (\operatorname{mod} p)$. But if $a^2 - mb^2 \equiv 0 \bmod p$ then $a^2 \equiv mb^2 \bmod p$ so $(ac)^2 \equiv m (\operatorname{mod} p)$ where $bc \equiv 1 (\operatorname{mod} p)$. (Such a c exists as $\mathbb{Z}_p$ is a field.) The equation $(ac)^2 \equiv m (\operatorname{mod} p)$ contradicts the hypothesis that m is not a square in U_p.

§33 (4.4-7) Take $m = 2$ and $p = 5$. The set of squares in U_5 is

$$S = \{1^2, 2^2, 3^2, 4^2\} = \{1, 4, 4, 1\} = \{1, 4\}.$$

Hence $2 \notin S$ so 4.4-12,13 applies and $Z[\sqrt{2}/I_5$ is a field of order $5^2 = 25$.