CHAPTER I

PRELIMINARIES

In this chapter, we shall give some notations, definitions and theorems used in this thesis. Our notations are :

$\mathbb{Z}$ is the set of all integers,

$\mathbb{Z}^+$ is the set of all positive integers,

$\mathbb{Z}_o^+ = \mathbb{Z}^+ \cup \{0\}$,

$\mathbb{Z}^-$ is the set of all negative integers,

$\mathbb{Q}$ is the set of all rational numbers,

$\mathbb{Q}^+$ is the set of all positive rational numbers,

$\mathbb{Q}_o^+ = \mathbb{Q}^+ \cup \{0\}$,

$\mathbb{R}$ is the set of all real numbers,

$\mathbb{R}^+$ is the set of all positive real numbers,

$\mathbb{R}_o^+ = \mathbb{R}^+ \cup \{0\}$.

Definition 1.1. A triple $(S,+,\cdot)$ is said to be a semiring iff

(i) $(S,+)$ and $(S,\cdot)$ are semigroups

and (ii) $x \cdot (y + z) = x \cdot y + x \cdot z$ and $(x + y) \cdot z = x \cdot z + y \cdot z$

for all $x,y,z \in S$. The operations $+$ and $\cdot$ are called the addition and multiplication of the semiring, respectively.

Example 1.2. Let S be a nonempty set. Define $x + y = y$ [$x + y = x$] and $x \cdot y = y$ [$x \cdot y = x$] for all $x,y \in S$. Then $(S,+,\cdot)$ is a semiring.

Definition 1.3. A semiring $(S,+,\cdot)$ is said to be additively [multiplicatively] commutative iff $(S,+)$ [$(S,\cdot)$] is commutative. And S is said to be commutative iff S is both additively and multiplicatively commutative.

Example 1.4.

1) Let $S = \{\begin{bmatrix} x & y \\ z & w \end{bmatrix} / x,y,z,w \in \mathbb{Z}^+\}$. Then S with the usual addition and multiplication is an additively commutative semiring.

2) Let $(S,\cdot)$ be a commutative semigroup. Define $x + y = x$ for all $x \in S$. Then $(S,+,\cdot)$ is a multiplicatively commutative semiring.

3) $\mathbb{Z}^+$ with the usual addition and multiplication is a commutative semiring.

Definition 1.5. A semiring $(D,+,\cdot)$ is said to be a skew ratio semiring iff $(D,\cdot)$ is a group.

Example 1.6. Let $(D,\cdot)$ be a group. Define $x + y = x$ [$x + y = y$] for all $x,y \in D$. Then $(D,+,\cdot)$ is a skew ratio semiring.

Definition 1.7. A semiring $(D,+,\cdot)$ is said to be a ratio semiring iff D is a commutative skew ratio semiring.

Example 1.8. $\mathbb{Q}^+$, $\mathbb{R}^+$ with the usual addition and multiplication are ratio semirings.

Definition 1.9. An element x of a semigroup $(S,\cdot)$ is said to be a left [right] zero of S iff $x \cdot y = x$ [$y \cdot x = x$] for all $y \in S$. And x is said to be a zero of S iff x is both a left and right zero of S.

Definition 1.10. An element a of a semiring $(S,+,\cdot)$ is said to be a multiplicative [additive] zero of the semiring S iff a is the zero of the semigroup $(S,\cdot)$ $[(S,+)]$.

Definition 1.11. A semiring $(K,+,\cdot)$ with a multiplicative zero 0 is said to be a skew semifield iff $(K\setminus\{0\},\cdot)$ is a group.

Example 1.12. Let $K = \{\begin{bmatrix} x & y \\ 0 & z \end{bmatrix} / x,z \in Q^+ \text{ and } y \in Q\} \cup \{\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}\}$.

Then K with the usual addition and multiplication is a skew semifield.

Definition 1.13. A semiring $(K,+,\cdot)$ with a multiplicative zero is said to be a semifield iff K is a commutative skew semifield.

Example 1.14. Q_o^+, R_o^+ with the usual additions and multiplications are semifields.

Definition 1.15. A semiring $(R,+,\cdot)$ is said to be a skew ring iff $(R,+)$ is a group. The identity of $(R,+)$ will be denoted by 0.

Example 1.16. Let $(R,+)$ be an arbitrary group with 0 as its identity. Define $x \cdot y = 0$ for all $x,y \in R$. Then $(R,+,\cdot)$ is a skew ring.

Definition 1.17. Let R be a skew ring and $x \in R\setminus\{0\}$. Then x is said to be a left [right] zero divisor iff there exists a $y \in R\setminus\{0\}$ such that $xy = 0$ $[yx = 0]$. And x is said to be a zero divisor iff x is both a left and a right zero divisor.

Example 1.18. Let R be the skew ring in Example 1.16 and $x \in R\setminus\{0\}$. Then x is a zero divisor.

Definition 1.19. A semiring $(S,+,\cdot)$ is said to be *additively cancellative* (A.C.) iff ($x + z = y + z$ implies $x = y$) and ($z + x = z + y$ implies $x = y$) for all $x,y,z \in S$, *multiplicatively cancellative* (M.C.) iff ($xz = yz$ and $z \neq 0$ imply $x = y$) and ($zx = zy$ and $z \neq 0$ imply $x = y$) for all $x,y,z \in S$ where 0 denotes the multiplicative zero of S if it exists, *cancellative* iff S is both additively cancellative and multiplicatively cancellative.

Example 1.20. $\mathbb{Z}^+$, $\mathbb{Z}_o^+$ with the usual addition and multiplication are cancellative semirings.

Proposition 1.21. Let S be an additively cancellative semiring. Then $xy + zw = zw + xy$ for all $x,y,z,w \in S$.

Proof. Let $x,y,z,w \in S$. Then

$$\begin{aligned} zy + xy + zw + xw &= (z + x)y + (z + x)w \\ &= (z + x)(y + w) \\ &= z(y + w) + x(y + w) \\ &= zy + zw + xy + xw. \end{aligned}$$

Since S is A.C., $xy + zw = zw + xy$.

#

Definition 1.22. A semiring $(S,+,\cdot)$ is said to be *strongly multiplicatively cancellative* (S.M.C.) iff ($xz + yw = xw + yz$ implies $x = y$ or $z = w$) and ($xz + yw = yz + xw$ implies $x = y$ or $z = w$) for all $x,y,z \in S$. ([2])

Example 1.23. $\mathbb{Z}^+$ with the usual addition and multiplication is a strongly multiplicatively cancellative semiring.

Proposition 1.24. Let S be a strongly multiplicatively cancellative semiring and $x \in S$. Then x is a left multiplicative zero of S iff x is a right multiplicative zero of S.

Proof. Assume that x is a left multiplicative zero of S. Let $y \in S$ and $z \in S \setminus \{x\}$ be arbitary. Since $yx + x = yx + x$, $yxz + xx = yxx + xz$. Since S is S.M.C. and $z \neq x$, $yx = x$, so x is a right multiplicative zero of S.

The proof of the converse is similar to the above. #

Proposition 1.25. If S is a strongly multiplicatively cancellative semiring then S is multiplicatively cancellative.

Proof. Assume that S is a strongly multiplicatively cancellative semiring.

Case 1 S has a multiplicative zero 0. Let $x,y,z \in S$ be such that $xy = xz$ and $x \neq 0$. Since $xy + 0z = xz + 0y$ and S is S.M.C., $y = z$. Similarly, if $yx = zx$ and $x \neq 0$ then $y = z$.

Case 2 S has no multiplicative zero. Let $x,y,z \in S$ be such that $xy = xz$. By Proposition 1.24, x is not a right multiplicative zero, so there exists a $w \in S$ such that $wx \neq x$. Since $xy + wxz = xz + wxy$ and S is S.M.C., $y = z$. Similarly, if $yx = zx$ then $y = z$.

Hence S is a multiplicatively cancellative semiring. #

Definition 1.26. A semiring S with a multiplicative identity 1 is said to be precise iff ($1 + xy = x + y$ implies $x = 1$ or $y = 1$) and

(1 + xy = y + x implies x = 1 or y = 1) for all $x,y \in S$. ([2])

<u>Example 1.27.</u> $\mathbb{Z}^+$ with the usual addition and multiplication is a precise semiring.

<u>Definition 1.28.</u> A semigroup $(S,\cdot)$ is said to satisfy the <u>right</u> [left] <u>Ore condition</u> iff for all $a,b \in S\setminus\{0\}$ there exist $x,y \in S\setminus\{0\}$ such that $ax = by$ [$xa = yb$] where 0 denotes the zero of S if it exists. ([3])

Note that every commutative semigroup satisfies the left and right Ore conditions but the converse is not true.

<u>Example 1.29.</u> $S = \{\begin{bmatrix} x & y \\ 0 & z \end{bmatrix} / x,z \in \mathbb{Z}^+ \text{ and } y \in \mathbb{Z}\}$ with the usual multiplication is a semigroup. Let $A = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$, $B = \begin{bmatrix} d & e \\ 0 & f \end{bmatrix} \in S$. Let $X = \begin{bmatrix} ad & d + ec - bf \\ 0 & af \end{bmatrix}$ and $Y = \begin{bmatrix} a^2 & a \\ 0 & ac \end{bmatrix}$. Then $X,Y \in S$ and $AX = \begin{bmatrix} a^2d & ad + aec \\ 0 & caf \end{bmatrix} = \begin{bmatrix} da^2 & da + eac \\ 0 & fac \end{bmatrix} = BY$. Hence $(S,\cdot)$ satisfies the right Ore condition and $(S,\cdot)$ is noncommutative.

<u>Definition 1.30.</u> Let S be a semiring without a multiplicative zero and $\leqslant$ a partial order on S. Then $(S,\leqslant)$ is said to be a <u>partially ordered semiring</u> iff $x \leqslant y$ implies $(x + z) \leqslant (y + z)$, $(z + x) \leqslant (z + y)$, $(xz) \leqslant (yz)$ and $(zx) \leqslant (zy)$ for all $x,y,z \in S$.

Let S be a semiring with a multiplicative zero 0 and $\leqslant$ a partial order on S. Then $(S,\leqslant)$ is said to be a <u>partially ordered semiring</u> iff for all $x,y,z \in S$

(i) $x \leqslant y$ implies $(x + z) \leqslant (y + z)$ and $(z + x) \leqslant (z + y)$

and (ii) $x \leqslant y$ and $0 \leqslant z$ imply $xz \leqslant yz$ and $zx \leqslant zy$.

Definition 1.31. A partial order $\leqslant$ on a semiring S with a multiplicative zero 0 is said to be multiplicatively regular (M.R.) iff ($xz \leqslant yz$ and $0 < z$ imply $x \leqslant y$) and ($zx \leqslant zy$ and $0 < z$ imply $x \leqslant y$) for all $x,y,z \in S$.

A partial order $\leqslant$ on a semiring S without a multiplicative zero is said to be multiplicatively regular (M.R.) iff ($xz \leqslant yz$ implies $x \leqslant y$) and ($zx \leqslant zy$ implies $x \leqslant y$) for all $x,y,z \in S$.

A partial order $\leqslant$ on a semiring S is said to be additively regular (A.R.) iff ($(x + z) \leqslant (y + z)$ implies $x \leqslant y$) and($(z + x) \leqslant (z + y)$ implies $x \leqslant y$) for all $x,y,z \in S$.

Definition 1.32. Let $(L,\leqslant)$ and $(M,\overset{*}{\leqslant})$ be partially ordered sets. A function $f : L \to M$ is said to be an order isomorphism iff

(i) f is a bijection,

(ii) $x \leqslant y$ implies $f(x) \overset{*}{\leqslant} f(y)$ for all $x,y \in L$

and (iii) $z \overset{*}{\leqslant} w$ implies $f^{-1}(z) \leqslant f^{-1}(w)$ for all $z,w \in M$.

A function $g : L \to M$ is said to be an increasing map iff ($x < y$ iff $g(x) \overset{*}{<} g(y)$ for all $x,y \in L$).

Definition 1.33. Let $(P,\leqslant)$ be a partially ordered set and $x,y \in X$.

An element z of P is said to be a least upper bound of $\{x,y\}$, denoted by $x \vee y$, iff 1) $x \leqslant z$, 2) $y \leqslant z$ and 3) $x \leqslant w$ and $y \leqslant w$ imply $z \leqslant w$ for all $w \in P$. A greatest lower bound of $\{x,y\}$, denoted by $x \wedge y$, is defined dually.

P is said to be an upper [lower] semilattice iff $x \vee y[x \wedge y]$ exists for all $x,y \in P$. P is said to be a lattice iff P is both an upper and a lower semilattice.

<u>Proposition 1.34.</u> Let X be a set and P the set of all partial orders on X. Then $(P,\subseteq)$ is a lower semilattice.

<u>Proof.</u> The proof is obvious. #

<u>Example 1.35.</u> Let X be a set of order > 1 and P the set of all partial orders on X. There exist $x,y \in X$ such that $x \neq y$. Define a relation $\leqslant$ on X by $x \leqslant y$ and $z \leqslant z$ for all $z \in X$ and define a relation $\leqslant^*$ on X by $y \leqslant^* x$ and $z \leqslant^* z$ for all $z \in X$. Then $\leqslant, \leqslant^* \in P$. Suppose that $\leqslant \vee \leqslant^*$ exists. Let $\leqslant^{**} = \leqslant \vee \leqslant^*$. Then $x \leqslant^{**} y$ and $y \leqslant^{**} x$ but $x \neq y$, so we have a contradiction. Hence $(P,\subseteq)$ is not an upper semilattice.

<u>Definition 1.36.</u> An equivalence relation ρ on a semiring S is said to be a <u>congruence on S</u> iff $x \rho y$ implies $(x + z) \rho (y + z)$, $(z + x) \rho (z + y)$, $xz \rho yz$ and $zx \rho zy$ for all $x,y,z \in S$.

<u>Definition 1.37.</u> A congruence ρ on S is said to be <u>multiplicatively regular</u> (M.R.) iff ($xz \rho yz$ and $z \neq 0$ imply $x \rho y$) and ($zx \rho zy$ and $z \neq 0$ imply $x \rho y$) for all $x,y,z \in S$ where 0 denotes the multiplicative zero of S if it exists, <u>additively regular</u> (A.R.) iff ($(x + z) \rho (y + z)$ implies $x \rho y$) and ($(z + x) \rho (z + y)$ implies $x \rho y$) for all $x,y,z \in S$.

<u>Proposition 1.38.</u> Let C be the set of all congruences on a semiring S. Then $(C,\subseteq)$ is a lattice.

<u>Proof.</u> Let $\rho, \rho^* \in C$. Then $\rho \wedge \rho^* = \rho \cap \rho^*$. Let $\mathcal{T} = \{\sigma \in C \mid \rho \cup \rho^* \subseteq \sigma\}$. Since $S \times S \in \mathcal{T}, \mathcal{T} \neq \emptyset$. Then $\rho \vee \rho^* = \bigcap_{\sigma \in \mathcal{T}} \sigma$. #

Definition 1.39. Let S be a commutative semiring with a multiplicative zero 0 such that $|S| > 1$. Then a semifield K is said to be a semifield of quotients of S iff there exists a monomorphism $i : S \to K$ such that for all $x \in K$ there exist $a \in S, b \in S\setminus\{0\}$ such that $x = i(a)i(b)^{-1}$. A monomorphism i satisfying the above property is called a quotient embedding of S into K. It follows from the definition that $i(0) = 0$ because K has only two multiplicative idempotents and $|S| > 1$. If K is a field then we shall call K a field of quotients of S.

Example 1.40. $\mathbb{Q}_0^+$, $\mathbb{Q}$ with the usual addition and multiplication are a semifield of quotients of $\mathbb{Z}_0^+$ and a field of quotients of $\mathbb{Z}$, respectively.

Theorem 1.41. Let S be a commutative semiring with a multiplicative zero 0 such that $|S| > 1$. Then a semifield of quotients of S exists iff S is multiplicatively cancellative.

We shall now give the construction of a semifield of quotients of S which appears in [1] p. 27 - 28.

Assume that S is multiplicatively cancellative. Define a relation $\sim$ on $S \times (S\setminus\{0\})$ by $(x,y) \sim (z,w)$ iff $xw = zy$ for all $(x,y),(z,w) \in S \times (S\setminus\{0\})$. It is easily shown that $\sim$ is an equivalence relation.

Let $\alpha,\beta \in \frac{S \times (S\setminus\{0\})}{\sim}$. Define + and $\cdot$ on $\frac{S \times (S\setminus\{0\})}{\sim}$ in the following way : Choose $(a,b) \in \alpha$ and $(c,d) \in \beta$. Define $\alpha + \beta = [(ad + bc,bd)]$ and $\alpha \cdot \beta = [(ac,bd)]$. In [1] it was shown that $(\frac{S \times (S\setminus\{0\})}{\sim}, +,\cdot)$ is a semifield of quotients of S.

Remark 1.42. In the proof of Theorem 1.41, P. Sinutoke used the commutativity of the addition of S only one time, to make $\frac{S \times (S \setminus \{0\})}{\sim}$ commutative with respect to addition. If the addition in the definition of semifield is not assumed to be commutative and S is multiplicatively commutative, then we can still use the construction in Theorem 1.41 and the "semifield of quotients" so constructed will not necessarily have commutative addition.

Example 1.43. Define $x + y = x[x + y = y]$ for all $x, y \in \mathbb{Z}_0^+$. $\mathbb{Z}_0^+$ with this addition and the usual multiplication is multiplicatively commutative semiring which is multiplicatively cancellative. Then $\mathbb{Q}_0^+$ with the addition already defined and the usual multiplication is a "semifield of quotients" of $\mathbb{Z}_0^+$.

Corollary 1.44. Let S be a semiring having K as a semifield of quotients, $i : S \to K$ a quotient embedding, L a semifield and $f : S \to L$ a homomorphism such that $f(x) = 0$ iff $x = 0$. Then there exists a unique homomorphism $g : K \to L$ such that $g \circ i = f$. Furthermore, if f is a monomorphism then g is a monomorphism.

Proof. Define $g : K \to L$ in the following way : Let $x \in K$. Then there exist $a \in S$, $b \in S \setminus \{0\}$ such that $x = i(a)i(b)^{-1}$. Define $g(x) = f(a)f(b)^{-1}$. It is easily shown that g is well-defined and satisfies all properties of the corollary.

#

Corollary 1.45. If L is a semifield and L contains an isomorphic copy of S then L contains an isomorphic copy of K.

Corollary 1.46. If S is a semiring having K and K' as semifields of quotients then $K \cong K'$.

Corollary 1.47. Let R be a ring of order > 1. Then a field of quotients of R exists iff R is commutative and has no zero divisors.

Remark 1.48. If R is a ring having a multiplicative identity $1 \neq 0$, then a field of quotients of R exists iff R is an integral domain.

Corollary 1.49. Let R be a ring having K as a field of quotients, $i : R \to K$ a quotient embedding, L a field and $f : R \to L$ a monomorphism. Then there exists a unique monomorphism $g : K \to L$ such that $g \circ i = f$.

Corollary 1.50. If L is a field and L contains an isomorphic copy of R then L contains an isomorphic copy of K.

Corollary 1.51. If R is a ring having K and K' as fields of quotients then $K \cong K'$.

Definition 1.52. Let S be a commutative semiring without a multiplicative zero. Then a ratio semiring D is said to be a ratio semiring of quotients of S iff there exists a monomorphism $i : S \to D$ such that for all $x \in D$ there exist $a, b \in S$ such that $x = i(a)i(b)^{-1}$. A monomorphism i satisfying the above property is called a quotient embedding of S into D.

Example 1.53. Q^+ with the usual addition and multiplication is a ratio semiring of quotients of $\mathbb{Z}^+$.

Theorem 1.54. Let S be a commutative semiring without a multiplicative zero. Then a ratio semiring of quotients of S exists iff S is multiplicatively cancellative.

The construction of a ratio semiring of quotients is the same as the construction of a semifield of quotients and all of the remarks and corollarys about semifields of quotients already given are true for ratio semirings of quotients.

Definition 1.55. Let S be a commutative semiring. A ring R is said to be a ring of differences of S iff there exists a monomorphism $i : S \to R$ such that for all $x \in R$ there exist $a,b \in S$ such that $x = i(a) - i(b)$. A monomorphism i satisfying the above property is called a difference embedding of S into R.

Example 1.56. $\mathbb{Z}$ with the usual addition and multiplication is a ring of differences of $\mathbb{Z}^+$.

Theorem 1.57. Let S be a commutative semiring. Then a ring of differences of S exists iff S is additively cancellative.

We shall now give the construction of a ring of differences of S which appears in [1] p. 37 - 39.

Assume that S is additively cancellative. Define a relation $\sim$ on $S \times S$ by $(x,y) \sim (z,w)$ iff $x + w = z + y$ for all $x,y,z,w \in S$. It is easily shown that $\sim$ is an equivalence relation.

Let $\alpha,\beta \in \frac{S \times S}{\sim}$. Define + and $\cdot$ on $\frac{S \times S}{\sim}$ in the following way : Choose $(a,b) \in \alpha$ and $(c,d) \in \beta$. Define $\alpha + \beta = [(a + c,b + d)]$ and $\alpha \cdot \beta = [(ac + bd,ad + bc)]$. In [1] it was shown that $(\frac{S \times S}{\sim},+,\cdot)$

is a ring of differences of S. #

Remark 1.58. In the proof of Theorem 1.57, P. Sinutoke defined $\theta : S \to \frac{S \times S}{\sim}$ by $\theta(a) = [(a + x,x)]$ for fixed $x \in S$ and for all $a \in S$ and she used the commutativity of multiplication of S to show that θ is a homomorphism. This is not necessary as we shall show now. Define $i : S \to \frac{S \times S}{\sim}$ by $i(x) = [(x + x,x)]$ for all $x \in S$. Let $a,b \in S$.

Then

$$\begin{aligned} i(ab) &= [(ab + ab,ab)] \\ &= [(ab + ab + ab + ab + ab,ab + ab + ab + ab)] \\ &= [((a + a)(b + b) + ab,(a + a)b + a(b + b)] \\ &= [(a + a,a)][(b + b,b)] \\ &= i(a)i(b), \end{aligned}$$

and

$$\begin{aligned} i(a + b) &= [(a + b + a + b,a + b)] \\ &= [(a + a + b + b,a + b)] \\ &= [(a + a,a)] + [(b + b,b)] \\ &= i(a) + i(b). \end{aligned}$$

Suppose that $i(a) = i(b)$. Thus $[(a + a,a)] = [(b + b,b)]$, so $a + a + b = b + b + a = b + a + b$, hence $a = b$. Therefore i is a monomorphism. Let $\alpha \in \frac{S \times S}{\sim}$. Choose $(a,b) \in \alpha$. Then

$$\begin{aligned} \alpha &= [(a,b)] \\ &= [(a + a + b,a + b + b)] \\ &= [(a + a,a)] + [(b,b + b)] \\ &= [(a + a,a)] - [(b + b,b)] \\ &= i(a) - i(b). \end{aligned}$$

Hence i is a difference embedding of S into $\frac{S \times S}{\sim}$. Hence $(\frac{S \times S}{\sim},+,\cdot)$ is a ring of differences of S. Therefore, we still have Theorem 1.57 if S is additively commutative but not multiplicatively commutative. In this case, the ring of differences will not be multiplicatively commutative.

Example 1.59. Let $S = \{\begin{bmatrix} x & y \\ z & w \end{bmatrix} / x,y,z,w \in \mathbb{Z}^+\}$ and

$R = \{\begin{bmatrix} x & y \\ z & w \end{bmatrix} / x,y,z,w \in \mathbb{Z}\}$ Then S and R with the usual addition and multiplication are additively commutative semirings, S is additively cancellative and R is its ring of differences.

Corollary 1.60. Let S be an additively commutative semiring having R as a ring of differences, $i : S \to R$ a difference embedding, T a ring and $f : S \to T$ a homomorphism. Then there exists a unique homomorphism $g : R \to T$ such that $g \circ i = f$. Furthermore, if f is a monomorphism then g is a monomorphism.

Proof. The proof of this corollary is similar to the proof of Corollary 1.44.

#

Corollary 1.61. If T is a ring and T contains an isomorphic copy of S, then T contains an isomorphic copy of R.

Corollary 1.62. If S is an additively commutative semiring having R and R' as rings of differences, then $R \cong R'$.

Proposition 1.63. Let G be a group and H,K normal subgroups of G such that $H \cap K = \{1\}$. Then $hk = kh$ for all $h \in H$, $k \in K$.

Proof. Let $h \in H$ and $k \in K$. Since $k^{-1}hk \in H$, $k^{-1}hkh^{-1} \in H$. Similarly, $k^{-1}hkh^{-1} \in K$. Thus $k^{-1}hkh^{-1} \in H \cap K = \{1\}$, so $k^{-1}hkh^{-1} = 1$, hence $hk = kh$.

#