SET THEORY AND MATHEMATICS
LECTURE NOTES DEPARTMENT OF LOGIC 2025

RADEK HONZIK

Contents

References

1. Yushiro Aoki, *Discontinuous homomorphsims on $C(X)$ with the negation of CH and a weak forcing axiom*, J. London Math. Soc. **110** (2024), no. 1.
2. H. G. Dales, *A discontinuous homomorphism from $C(X)$*, American Journal of Mathematics **101** (1979), 647–734.
3. H. G. Dales and H Woodin, *An introduction to independence for analysts*, London Mathematical Society Lecture Note Series, 115, Cambridge University Press, 1987.
4. Bob A. Dumas, *Discontinuous homomorphisms of $C(X)$ with $2^{\aleph_0} > \aleph_2$*, The Journal of Symbolic Logic **89** (2024), no. 2, 665–696.
5. P. C. Eklof and A. H. Mekler, *Almost free modules: Set-theoretic methods, revised edition*, North-Holland, 2002.
6. Paul C. Eklof, *Whitehead's problem is undecidable*, The American Mathematical Monthly **83** (1976), no. 10, 775–788.
7. Tomáš Jech, *Set theory*, Springer Monographs in Mathematics, Springer, Berlin, 2003.
8. R. Björn Jensen, *The fine structure of the constructible hierarchy*, Annals of Mathematical Logic **4** (1972), no. 3, 229–308.
9. Saharon Shelah, *Infinite abelian groups, Whitehead problem and some constructions*, Israel Journal of Mathematics **18** (1974), 243–256.
10. R. M. Solovay and S. Tennenbaum, *Iterated cohen extensions and souslin's problem*, Annals of Mathematics **94** (1971), no. 2, 201–245.
11. M. Y. Souslin, *Probleme 3*, Fundamenta Mathematicae **1** (1920).
12. Stevo Todorcevic, *Partition problems in topology*, Contemporary Mathematics, 84, American Mathematical Society, Providence, RI, 1989.
13. W. Hugh Woodin, *A discontinuous homomorphism from $C(X)$ without CH*, Journal of the London Mathematical Society **s2-48** (1993), no. 2, 299–315.

1. Introduction

We will discuss three famous independent mathematical problems from various areas of mathematics: from characterization of the real line, to infinite abelian group theory and functional analysis. We will briefly describe their contents, discuss their relevance, and then focus on set-theoretical reformulations which were used by set-theoretics to show their independence.

- SH denotes the statement that there are no Suslin lines.
- WC denotes the statement there exists a non-free Whitehead groups of size ω_1.
- KC denotes the statement that every homomorphism from $C(X)$ (the commutative Banach algebra of continuous real valued functions on an infinite compact space X) into any commutative Banach algebra is continuous.

SH stands for "Suslin hypothesis". Suslin asked in the 1920s, [11], whether one can replace the condition of separability in the characterization of the ordering on the reals by the weaker countable chain condition and still uniquely characterize the reals. A Suslin line is a hypothetical witness for the negative answer: it is a dense complete linear order satisfying the countable chain condition which fails to be separable. Existence of this line is equivalent to the existence of an ω_1-Suslin tree. See the appropriate sections of [7] for details.

WC stands for the "Whithead conjecture" in the infinite abelian group theory. Whitehead asked in the 1950s whether there exists a non-free abelian group G of size ω_1 such that every surjective homomorphism onto G with kernel $\mathbb{Z}$ splits (a group satisfying this property is called "Whitehead"). By a result of Stein from 1951 every countable Whitehead group is free ($\neg$WC holds in the countable case in our notation). See [6] for a clearly written summary and definitions and the book [5] for more context and generalizations.

KC stands for "Kaplansky conjecture" in Banach algebra theory. Kaplansky asked around 1947 whether every algebra homomorphism from $C(X)$, where X is any infinite compact Hausdorff space and $C(X)$ is the Banach algebra of continuous real valued functions, into any other commutative Banach algebra is continuous ("automatic continuity"). See the book [3] for more details and alternative definitions and [13, 4, 1] for more context a recent development.

Remark 1.1. Suslin, Whitehead[1] and Kaplansky apparently did not commit to a specific solution to their questions. We chose the uniform notation SH, WC, KC for easier reading: All three statements follow from PFA and all of them are refuted from $V = L$.

In all three cases, the key step for showing independence over ZFC is to identify a set-theoretic combinatorial property which is equivalent (or at least implies) the original mathematical statement. For SH, this is the non-existence of ω_1-Suslin trees, for WC the existence of uniformizations of certain colorings of ladders on stationary sets, and for KC the non-existence of strictly increasing maps from 2^{ω_1} ordered lexicographically into ω^ω ordered by eventual domination.

Let us first review additional set-theoretic assumptions which resolve these problem over ZFC. The theorem in particular implies that SH, WC, KC are independent over ZFC.

Theorem 1.2. *The following hold:*

[1] It is sometimes suggested that Whitehead conjectured that all Whitehead groups of size ω_1 are free (for instance in [1]) possibly because Stein proved in the early 1950s that all countable Whitehead groups are free. But there is no general consensus on the notation.

(i) MA_{ω_1} *implies* SH [10] *and* WC [9, 6]*, and* PFA *implies* KC [3, 12].
(ii) CH *implies* $\neg\mathsf{KC}$ [2]*,* $\diamondsuit$ *implies* $\neg\mathsf{SH}$ [8]*, and* $\diamondsuit(S)$ *for every stationary* $S \subseteq \omega_1$ *implies* $\neg\mathsf{WC}$ [9, 6].

Remark 1.3. The argument for KC in [3] goes by constructing a generic extension via a ccc iteration which yields simultaneously MA_{ω_1} and a combinatorial property which implies KC. Todorcevic noticed in [12, Theorem 8.8] that this combinatorial property already follows from PFA (see [12, p. 87] for more historical details on this point). It is open whether MA_{ω_1} is necessary for KC; see [1] which constructs a model with $\neg\mathsf{KC}$, $\neg\mathsf{CH}$ and a weak fragment of MA_{ω_1}.

2. Set-theoretic background

We will briefly review notions which appear in Theorem 1.2 to make these notes relatively self-contained.

2.1. Stationarity

We will discuss the concept of stationarity only on ω_1, but it is meaningful on any ordinal of uncountable cofinality.

Definition 2.1. A set $C \subseteq \omega_1$ is called *closed unbouded, club* if it satisfies:
(i) C is unbounded in ω_1: for every $\alpha < \omega_1$ there is $\beta \geq \alpha$ with $\beta \in C$.
(ii) C is closed: whenever $\alpha < \omega_1$ is a limit ordinal and $C \cap \alpha$ is unbounded in α, then $\alpha \in C$.

Lemma 2.2. *If C and D are clubs in ω_1, then $C \cap D$ is a club in ω_1*

Proof. We first show that $C \cap D$ is closed. This is clear: if α is a limit ordinal and $C \cap \alpha$ and $D \cap \alpha$ are both unbounded in α, then by closedness of C, D, $\alpha \in C \cap D$.

The key of the proof is to show the unboundedness. Let $\alpha < \omega_1$ be given, we wish to find some $\beta \geq \alpha$ such that $\beta \in C \cap D$. Let us construct by recursion a sequence $\langle c_i \,|\, i < \omega\rangle$ of elements of C and $\langle d_i \,|\, i < \omega\rangle$ of elements of D as follows. Choose $c_0 \in C$ and $d_0 \in D$ so that $\alpha < c_0 < d_0$. In general, in the step $n+1$, choose $c_{n+1} \in C$ and $d_{n+1} \in D$ so that $\ldots c_n < d_n < c_{n+1} < d_{n+1}$. Let us denote $c = \sup\{c_i \,|\, i < \omega\}$ and $d = \sup\{d_i \,|\, i < \omega\}$. First note that $c = d$ and that c (and d) is a limit ordinal of countable cofinality. By closedness of C and D, $c \in C \cap D$. □

Exercise. Let C be a club. Let us denote as D the set of all limit ordinals in C. Show that D is a club.

Exercise. Let C be a club and let $\mathrm{Lim}(C)$ be the set of limit points of C, where $\alpha \in C$ is a limit point of C if $C \cap \alpha$ is unbounded in α. Show that $\mathrm{Lim}(C)$ is a club (which is strictly smaller than C).

Exercise. Lemma 2.2 generalizes to countably many clubs C_i: if C_i, $i < \omega$, are clubs, so is $\bigcap_{i\in\omega} C_i$.

Lemma 2.2 allows us to define the *closed unbounded filter* generated by the club sets:

Definition 2.3. The club filter on ω_1, $\mathrm{Club}(\omega_1)$, is defined as follows:

$$\mathrm{Club}(\omega_1) = \{X \subseteq \omega_1 \,|\, \text{there is a club } C \text{ such that } C \subseteq X\}.$$

Note. Under AC, $\mathrm{Club}(\omega_1)$ is never an ultrafilter.

Definition 2.4. Let us denote by $\mathrm{NS}(\omega_1)$ the dual ideal to $\mathrm{Club}(\omega_1)$:

$$\mathrm{NS}(\omega_1) = \{X \subseteq \omega_1 \,|\, \kappa \setminus X \in \mathrm{Club}(\omega_1)\}.$$

We call the ideal $\mathrm{NS}(\omega_1)$ the *non-stationary ideal* on ω_1.

Lemma 2.5. *$X \subseteq \omega_1$ is stationary iff $X \cap C \neq \emptyset$ for every club C.*

Proof. If X is stationary iff $\kappa \setminus X$ is not in $\mathrm{Club}(\kappa)$. This means that there is no C so that $C \subseteq \kappa \setminus X$, or equivalently for any club C, $C \not\subseteq \kappa \setminus X$, which is the same as $C \cap X \neq \emptyset$. □

Exercise. Show that every stationary set S is unbounded, and hence uncountable. *Exercise.* Let us denote by $F(\omega_1)$ the Frechet filter on ω_1:

$$F(\omega_1) = \{X \subseteq \omega_1 \,|\, |\omega_1 \setminus X| < \omega_1\}.$$

Show

$$F(\omega_1) \subsetneq \mathrm{Club}(\omega_1).$$

2.2. Diamonds

Recall the definition of CH:

Definition 2.6. The *Continuum Hypothesis*, CH is defined as follows:

$$2^\omega = \omega_1.$$

Exercise. Show that the following two principles are equivalent to CH:
(i) There is a surjection from $\mathscr{P}(\omega)$ onto ω_1.
(ii) If X is an arbitrary infinite subset of the real line $\mathbb{R}$, then $|X| = \omega$ or $|X| = |\mathbb{R}|$.

The principle CH is relatively weak, the following concept is a strenghthening of CH wich much broader range of consequences in mathematics.

Definition 2.7. Let S be a stationary subset of ω_1. We say that $\diamondsuit(S)$ holds if there is sequence $\langle S_\alpha \,|\, \alpha \in S\rangle$ such that $S_\alpha \subseteq \alpha$ for every α and for every $A \subseteq \omega_1$,

$$\{\alpha \in S \,|\, S_\alpha = A \cap \alpha\} \text{ is stationary.}$$

We write $\diamondsuit$ for $\diamondsuit(\omega_1)$.

Under $V = L$,[2] $\diamondsuit(S)$ is true for every stationary S.
$\diamondsuit$ implies CH:

Theorem 2.8. *Suppose $\diamondsuit$ holds, then CH holds.*

Proof. Let $\langle S_\alpha \,|\, \alpha \in \omega_1\rangle$ be a diamond sequence. We will show that for every $X \subseteq \omega$ there is some $\alpha \in \omega_1$ such that $X = S_\alpha$. This means that there is a surjection from $\mathscr{P}(\omega)$ onto ω_1, which is equivalent to CH. Let $X \subseteq \omega$ be arbitrary. Since $\langle S_\alpha \,|\, \alpha \in \omega_1\rangle$ is a diamond sequence, the set $\{\alpha < \omega_1 \,|\, S_\alpha = X \cap \alpha\}$ is stationary and in particular unbounded. Choose any $\alpha \geq \omega$ from this set. Then $X = X \cap \alpha = S_\alpha$. □

Note that by a result of Jensen, CH plus $\neg\diamondsuit$ is consistent so the converse of Theorem 2.8 does not hold.

[2] An axiom claiming that V is equal to the the *constructible universe* or *Gödel universe*, denoted L. $L \subseteq V$ is always true. Gödel defined L to show in 1930's that CH and AC relatively consistent with ZF.

2.3. Forcing axioms

Forcing axioms are axiomatic statements which postulate existence of certain ultrafilters on a wider class of Boolean algebras, not only the powerset algebras. By extending the class of algebras, it is possible to derive from forcing axioms consequences for specific mathematical structures: roughly speaking given a mathematical problem, it is sometimes possible to associate with it a specific Boolean algebra, and the existence of an ultrafilter with certain properties implies a solution to the original problem. This is a remarkable extension of Cohen's original idea for forcing. See [7] for more details and context.

There is a conceptual similarity between compactness principles (consequences of AC) and forcing axioms: they both generalize certain ZFC-theorems, each in a different sense:

- AC implies that every filter in any powerset algebra $\mathscr{P}(X)$ can be extended into an ultrafilter.
- AC implies that given any complete Boolean algebra B and a family of countably many dense open subsets $\{D_n \mid n < \omega\}$ of B there is an ultrafilter on B which meets every D_n (this is a straightforward reformulation of the Baire category theorem).

Forcing axioms postulate the second bullet for uncountably many dense open subsets of a Boolean algebra B. B must come from some fixed class $\mathcal{B}$ of complete Boolean algebras (the larger the class $\mathcal{B}$, the stronger the associated forcing axiom).

Definition 2.9. Given a class $\mathcal{B}$ of complete Boolean algebras, we write $\mathsf{FA}_{\omega_1}(\mathcal{B})$ for the stament that for any $B \in \mathcal{B}$ and any family of dense open subsets $\{D_\alpha \mid \alpha < \omega_1\}$ of B there is an ultrafilter U on B which meets every D_α. We say that U is "partially generic".

Let us review some important classes $\mathcal{B}$. Let "ccc" denote the class of Bolean algebras satisfying the countable chain condition, "proper" the class of proper Boolean algebras, and "stat" the class of Boolean algebras preserving stationary subsets of ω_1. Note that these classes satisfy:

$$\text{ccc} \subseteq \text{proper} \subseteq \text{stat}.$$

Definition 2.10. Let us define the associated forcing axioms:

(i) Martin Axiom, also denoted MA_{ω_1}, is $\mathsf{FA}_{\omega_1}(\text{ccc})$.
(ii) Proper Forcing Axiom, also denoted PFA, is $\mathsf{FA}_{\omega_1}(\text{proper})$.
(iii) Martin Maximum, also denoted MM, is $\mathsf{FA}_{\omega_1}(\text{stat})$.

From the general perspective mentioned above, one can classify mathematical problems according to the associated Boolean algebra B and its class $\mathcal{B}$ such that the problem is decided by the existence of partially generic ultrafilters for B.

2.3.1. Some examples

Suppose $\mathbb{P} = (\mathbb{P}, \leq, 1)$ is a partially ordered set with the greatest element 1; then we say that $p, q \in \mathbb{P}$ are *compatible*, and write $p \mid\mid q$, if there is $r \in \mathbb{P}$ with $r \leq p, q$. We say that p, q are *incompatible* if there are not compatible. We say that $A \subseteq \mathbb{P}$ is an *antichain* if all $p \neq q \in A$ are incompatible. We say that $D \subseteq P$ is *dense* if for every p there is some $q \leq p$ in D and D is *open* if $p \in D$ and $q \leq p$ implies $q \in D$ (downwards closure).

Definition 2.11. We say that $\mathbb{P}$ is ccc (countable chain condition) if every antichain in $\mathbb{P}$ is at most countable.

A paradigmatic example is Cohen forcing for adding new subsets of of ω:

Definition 2.12. $\mathrm{Add}(\omega,\alpha)$, $0<\alpha$, is a set of all functions p such that $\mathrm{dom}(p)\subseteq\alpha\times\omega$, $|\mathrm{dom}(p)|<\omega$, and $\mathrm{im}(p)\subseteq\{0,1\}$. We set $p\le q$ iff $q\subseteq p$ (reverse inclusion ordering). $\mathrm{Add}(\omega,\alpha)$ is called the Cohen forcing (at ω). It adds α-many new subsets of ω.

Fact 2.13. *An application of the so called Δ-lemma shows that* $\mathrm{Add}(\omega,\alpha)$ *is ccc for every* α*. Note that for* $\alpha<\omega_1$, $\mathrm{Add}(\omega,\alpha)$ *is just countable, so it is ccc trivially.*

Let us further define that $G\subseteq\mathbb{P}$ is a filter if G contains the greatest element of $\mathbb{P}$, for every $p,q\in G$ there is some $r\in\mathbb{P}$ with $r\le p,q$, and if $p\in G$ and $p\le q$, then $q\in G$.

The following definition is equivalent to the Boolean algebra version mentioned above:

Definition 2.14 (Martin's axiom, MA_{ω_1})**.** Whenever $\mathbb{P}$ is ccc and $\mathcal{D}$ is a collection of ω_1-many dense sets in $\mathbb{P}$, then for every p there is a filter G containing p which intersects every element of $\mathcal{D}$.

Recall that if $\mathcal{D}$ has size ω, then the respective principle is provable:

Lemma 2.15 (Rasiowa-Sikorski)**.** *Suppose* $\mathbb{P}$ *is a partially ordered set and* $\mathcal{D}$ *is a countable collection of dense sets. Then for every* p *there is a filter* G *such that* $p\in G$ *and* G *meets every element of* $\mathcal{D}$*.*

Proof. Construct by induction a decreasing sequence of elements in $\mathbb{P}$, $\langle p_n\,|\,n<\omega\rangle$ with $p_0=p$ and $p_{n+1}\in D_n$. Then define

$$G=\{q\in\mathbb{P}\,|\,\exists n<\omega, p_n\le q\}.$$

□

Remark 2.16. MA_{ω_1} is not provable in ZFC, but by using a forcing argument, it holds that if ZFC is consistent, then so is $\mathsf{ZFC}+\mathsf{MA}_{\omega_1}$.

Let us show some consequences of MA_{ω_1} to illustrate its use:

Theorem 2.17. $\mathsf{ZFC}+\mathsf{MA}_{\omega_1}$ *proves* $\neg\mathsf{CH}$.

Proof. We will apply MA_{ω_1} with the partial order $\mathbb{C}=\mathrm{Add}(\omega,1)$. Suppose for contradiction that $2^\omega=\omega_1$, and let $\langle x_\alpha\,|\,\alpha<\omega_1\rangle$ enumerate all subsets of ω. Define dense sets D_α for $\alpha<\omega_1$ and D_m for $m<\omega$:

$$D_\alpha=\{p\in\mathbb{C}\,|\,\exists n<\omega, p(n)\neq x_\alpha(n)\},\ D_m=\{p\in\mathbb{C}\,|\,m\subseteq\mathrm{dom}(p)\}.$$

Let G be a filter meeting every D_α and D_m. Let x be the union of conditions in G. It is a function (because G is a filter) from ω into 2 (because G meets every D_m). It further follows $x\neq x_\alpha$ for every $\alpha<\omega_1$ because for every α there is some n the domain of x with $x(n)\neq x_\alpha(n)$ (because G meets every D_α). This contradicts the fact that $\langle x_\alpha\,|\,\alpha<\omega_1\rangle$ enumerates all subsets of ω. □

3. Whitehead conjecture

3.1. The problem

Definition 3.1. Suppose G is an abelian group and $f:G\to H$ is a surjective homomorphism. We say that f *splits* if there exists a homomorphism $f':H\to G$ such that $f\circ f'=1_H$.

Note that if $f : G \to H$ is surjective and $\ker(f)$ denotes the kernel of f, then $H \cong G/\ker(f)$ (see Theorem 3.15).

The problems is to characterize free abelian groups H via the criterion of the existence of splitting homomorphisms.

Fact 3.2 (see Theorem **??**). *H is free iff for every G and every surjective $f : G \to H$, f splits.*

It is easy to see that if H is free, then every $f : G \to H$ splits (see Theorem **??**). The converse direction is a bit more difficult to prove: it uses the fact that every abelian group H is a quotient of the free group $\mathbb{Z}^{(H)}$ generated by H, i.e. $H \cong \mathbb{Z}^{(H)}/\ker(f)$ for some surjective homomorphism $f : \mathbb{Z}^{(H)} \to H$. The existence of splitting homomorphism ensures that H has an isomorphic copy inside $\mathbb{Z}^{(H)}$, and by Dedekind's theorem (that a subroup of a free abelian group is always free), H must be free as well (see Lemma **??**).

It follows that to prove the harder direction in Fact 3.2, it suffices to require that every surjective homomorphism $f : \mathbb{Z}^{(H)} \to H$ splits. Whitehead inquired whether it is possible to weaken this criterion still further and demand that only certain f's are split.

To understand this note that if $H \cong \mathbb{Z}^{(H)}/\ker(f)$, then $\ker(f)$ is a normal subgroup of $\mathbb{Z}^{(H)}$ and again by Dedekind's theorem $\ker(f)$ itself must be a free group. All free abelian groups are up to isomorphism of the form $\mathbb{Z}^{(\kappa)}$ for some cardinal κ (finite or infinite), see Section 3.3.[3] Stein proved that if H is countable, then it suffices for the converse direction that every $f : \mathbb{Z}^{(H)} \to H$ such that $\ker(f) \cong \mathbb{Z}$ splits.[4] Whitehead asked whether one can remove the condition of countability in Stein's theorem.

Let us restate the problem now in the modern notation:

Definition 3.3. We say that an abelian group H is a *Whitehead group* or *W-group* if for every G and every surjective homomorphism $f : G \to H$, if $\ker(f) \cong \mathbb{Z}$, then f splits.

Note that by the discussion above we have the following inclusion:

$$\text{Free abelian groups} \subseteq W\text{-groups}.$$

Stein's theorem now reads that every countable H is free iff H is a W-group.

Definition 3.4. We say that *Whitehead's conjecture* holds if there is an abelian group of size ω_1 which is a W-group, but not a free group. We denote this conjecture by WC.

Remark 3.5. Whitehead apparently did not commit strongly to a particular "conjecture", he posed the question as a problem. We write WC to have all the conjectures false in $V = L$ and true under PFA, undescoring the conceptual resemblance of the three problems (Whitehead's, Kaplansky's and Suslin's) which emerged only after some hard work of generations of mathematicians. Note that the conceptual resemblance shows that Stein's theorem is specific for the countable case and should not be naively postulated for all cardinals. Compare with König's lemma which asserts that every ω-tree has a cofinal branch, and the fact that König's lemma is false for ω_1 (there exit ω_1-Aronszajn trees).

---

[3]In particular $\mathbb{Z}^{(H)} \cong \mathbb{Z}^{(|H|)}$.

[4]Since H is countable, $\mathbb{Z}^{(H)}$ is countable as well, so all the possibilities for $\ker(f)$ are $\{\mathbb{Z}^{(\kappa)} \mid 1 \leq \kappa \leq \omega\}$. Hence limiting the splitting homomorphism just to the case of $\mathbb{Z}$ is non-trivial.

3.2. Preliminaries on groups

We first review some basic concept. Recall that if G is a group (in general non-commutative) $G = (G, +_G, -_G, 0_G)$. We say that a function $f : G \to H$ between two groups is a *homomorphism* if $f(0_G) = 0_H$, $f(x +_G y) = f(x) +_H f(y)$, and $f(-_G x) = -_H f(x)$. We will omit the subscripts $_G$ and $_H$ in the subsequent text because they can be deduced from the notation.

Assume H is a subgroup, which we denote by $H \leq G$. For every $g \in G$, we call $g + H = \{g + h \mid h \in H\}$ the *left coset* (with respect to g) and $H + g = \{h + g \mid h \in H\}$ the *right coset* (with respect to g). Note that in general $g + H \neq H + g$ is possible.

As an exercise, convince yourselves that

$$H + a = H + b \leftrightarrow a - b \in H \leftrightarrow b - a \in H \\ \text{and } a + H = b + H \leftrightarrow -a + b \in H \leftrightarrow -b + a \in H. \tag{3.1}$$

Lemma 3.6. *The family of all left cosets and also of all right cosets is a partition of G. The number of elements in both partitions is the same. Also, for every g, $|g+H| = |H+g| = |H|$.*

Proof. Exercise. Hint for the second claim: define a function which maps $H + g$ to $-g + H$ and show that it is a bijection. See [H], Section 4. □

Remark 3.7. Note that we used this argument it the proof of Lagrange's theorem in Introduction to mathematics I: it implies that if G is finite and $H \leq G$, then the number of elements in H divides the number of elements in G.

It follows that the partition into left cosets defines an equivalence relation $\equiv_{H,l}$, and analogously for the right cosets, $\equiv_{H,r}$. By (3.1), a, b are equivalent if their difference is small mod H.

Recall that an equivalence $\equiv$ on G is a *congruence* if $a \equiv b$, then $-a \equiv -b$, and if $a_1 \equiv a_2$ and $b_1 \equiv b_2$, then $a_1 + b_1 \equiv a_2 + b_2$. If $\equiv$ is a congruence of G, then $G/\equiv = \{[g]_\equiv \mid g \in G\}$ can be given the group structure by postulating:

$$0 = [0]_\equiv, [a]_\equiv + [b]_\equiv = [a + b]_\equiv, -[a]_\equiv = [-a]_\equiv.$$

Congruences make it possible to define the so called *qutient structures*. In the context of groups, we get:

Lemma 3.8. *$G/\equiv$ is a group (called the* quotient group*) and $\pi : G \to G/\equiv$ is a surjective homomorphism, where $\pi(g) = [g]_\equiv$ for every $g \in G$.*

Proof. The fact that $G/\equiv$ is a group follows easily by the definition of operations in $G/\equiv$; for instance (we omit the subscript $_\equiv$): $[g] + [-g] = [g - g] = [0]$. π is clearly surjective, so it remain to show that it is a homorphism. $\pi(0) = [0]$, $\pi(-g) = [-g] = -[g]$, and $\pi(g + h) = [g + h] = [g] + [h]$. □

A natural question is whether $\equiv_{H,l}$ and $\equiv_{H,r}$ are congruences. Let us try to check it for $\equiv_{H,r}$ and for the inverse: if $a \equiv_{H,r} b$, then by (3.1) $a - b \in H$; in order to have a congruence, we would like to have $-a \equiv_{H,r} -b \leftrightarrow -a + b \in H$. But $a - b \in H$ does not necessarily imply $-a + b \in H$. However, it does if $H + a = a + H$ and $H + b = b + H$. A similar argument would work for $+$, giving a sufficient condition for being a congruence:

$$\text{if } g + H = H + g \text{ for every } g, \text{ then } \equiv_{H,r} \text{ and } \equiv_{H,l} \text{ are congruences.}$$

But this is actually the same as $\equiv_{H,r}$ being identical to $\equiv_{H,l}$.

This property is very important and can be reformuluted in many equivalent ways (where $g + N - g = \{g + n - g \mid n \in N\}$):

Lemma 3.9. *The following are equivalent for a subgroup $N \leq G$:*

(i) $\equiv_{N,r} = \equiv_{N,l}$.
(ii) $g + N = N + g$ *for all* $g \in G$.
(iii) *For all* $g \in G$, $g + N - g \subseteq N$.
(iv) *For all* $g \in G$, $g + N - g = N$.

Proof. We prove the less obvious ones.

$(ii) \to (iii)$. Let $g + n - g$ be given. $g + n \in g + N$, and since $g + N = N + g$, there is $n' \in N$ with $g + n = n' + g$. Hence $g + n - g = n' + g - g = n' \in N$.

$(iii) \to (iv)$. Suppose $n \in N$, and let us write it as $g + (-g + n + g) - g$. Since $-g + N + g \subseteq N$ by (iii), there is $n' \in N$ with $n = g + n' - g$, and so $n \in g + N - g$.

$(iv) \to (ii)$. $g + N = g - g + N + g = N + g$. □

Definition 3.10. A subgroup N which satisfies conditions in Lemma 3.9 is called *normal*, and we write $N \lhd G$.

The notions of a normal subgroup, a quotient group and a (surjective) homomorphism are deeply connected as we show next.

Definition 3.11. Suppose $f : G \to H$ is a homormophism. Then the *kernel* of f, $\ker(f)$, is defined as

$$\ker(f) = \{g \in G \mid f(g) = 0\}.$$

As it turns out every normal subgroup is kernel of some homomorphis, and kernels are always normal subgroups.

Theorem 3.12. *(i) Suppose $f : G \to H$ is homomorphism. Then* $\ker(f) \lhd G$.

(ii) Suppose $N \lhd G$. Then the function π which maps $g \in G$ to $N + g$ is a surjective homomorphism $\pi : G \to G/N$ with $\ker(\pi) = N$.

Proof. (i). First we need to check that $\ker(f)$ is a subgroup of G. Clearly $0 \in \ker(f)$ because $f(0) = 0$. If $g \in \ker(f)$, then $f(x) = 0$, and so $f(-x) = -f(x) = -0 = 0$, and so $-x \in \ker(f)$. The closure under $+$ is similar. To verify normality, it suffices to show $g + \ker(f) - g \subseteq \ker(f)$ for every $g \in G$; let fix any $n \in N$ and $g + n - g$. Since f is a homomorphism, we get $f(g + n - g) = f(g) + 0 - f(g) = 0$.

(ii). This follows from Lemma 3.8, noting that $N = [0]$. □

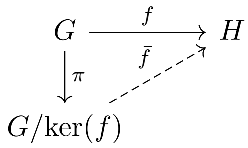
Remark 3.13. Theorem 3.12 implies that if $\equiv$ is a congruence and f is the surjective homomorphism given by $\equiv$, then $[0]_\equiv \lhd G$. Hence $\equiv_{N,r}$ (or $\equiv_{N,l}$) being a congruence is equivalent to all the conditions in Lemma 3.9.

Before we prove the first isomorphism theorem, let us state a small lemma first:

Lemma 3.14. *Suppose $f : G \to H$ is a homomorphism. Then f is injective iff* $\ker(f) = \{0\}$.

Proof. If f is injective, then clearly $\ker(f) = \{0\}$, so let us prove the converse. We notice first that if $g \neq h$ is equivalent to $g - h \neq 0$. Suppose for contradiction that $\ker(f) = \{0\}$ and for some $g \neq h$ we get $f(g) = f(h)$. Then $f(g - h) = f(g) - f(h) = 0$, and so $g - h \neq 0$ is in $\ker(f)$, a condtradiction. □

Theorem 3.15 (First isomorphism theorem for groups)**.** *If $f : G \to H$ is a group homomorphism, then there is a unique injective homomorphism $\bar{f} : G/ker f \to H$ such that $\bar{f}(g + \ker(f)) = f(g)$. It follows that $\bar{f}$ is an isomorphism between $G/ker(f)$ and $\mathrm{im}(f)$; in particular if f is surjective then $\bar{f} : G/\ker(f) \cong H$. Moreover, denoting $\pi : G \to G/\ker(f)$, the following diagram commutes:*



Proof. By Theorem 3.12, π is a surjective homomorphism. It remains to show that $\bar{f}$ is well-defined and is injective. First we check that $\bar{f}$ is well-defined: Suppose $g + \ker f = g' + \ker f$, we need to show $f(g) = f(g')$; $g + \ker(f) = g' + \ker(f)$ iff $g - g' \in \ker(f)$, and hence $f(g) - f(g') = 0$, and $f(g) = f(g')$. Next we check that $\bar{f}$ is a homomorphism: $\bar{f}(\ker(f)) = f(0) = 0$; $\bar{f}(-[g + \ker(f)]) = \bar{f}(-g + \ker(f)) = f(-g) = -f(g) = -\bar{f}(g + \ker(f))$; $\bar{f}(g + \ker(f) + g' + \ker(f)) = \bar{f}(g + g' + \ker(f)) = f(g + g') = f(g) + f(g') = \bar{f}(g + \ker(f)) + \bar{f}(g' + \ker(f))$. By Lemma 3.14, the injectivity of $\bar{f}$ follows if we show $\ker(\bar{f}) = \{\ker(f)\}$. But $\bar{f}(g + \ker(f)) = 0$ is equivalent to $f(g) = 0$ by the definition of $\bar{f}$, and hence $g + \ker(f) = \ker(f)$. □

3.3. Free abelian groups

Recall that if G is any abelian group, we write ng for $x + \cdots + x$ of length $n \in \mathbb{Z}$, and $0g$ for 0_G.[5] Clearly, $ng + mg = (n + m)g$.

Let $F(G)$ be the free abelian group generated by G. It can be represented as the direct sum $\oplus_{g \in G} \mathbb{Z}_g$ of copies of $\mathbb{Z}$ indexed by G, also written as $\mathbb{Z}^{(G)}$, where (G) indicates that only functions with finite support are allowed. That is, an element $x \in \mathbb{Z}^{(G)}$ is a function from G to $\mathbb{Z}$ such that for all but finitely many $g \in G$, $x(g) = 0$. The group operations on $F(G)$ are defined coordinate-wise:

(i) $(x + y)(g) = x(g) + y(g)$, and
(ii) $(-x)(g) = -x(g)$.
(iii) $0_{F(g)}$ is a function which is constantly 0_G.

Define a function $e : G \to F(G)$ by postulating $e(g) := e_g$ where $e_g(g) = 1$, and e_g is 0 everywhere else. The mapping e is injective, so we identify G with the image of this function.[6]

Then the basis of $\mathbb{Z}^{(G)}$ is the set $\{e_g \,|\, g \in G\}$: every $x \in F(G)$, $x \neq 0_{F(G)}$, can be written uniquely (up to permutation of its members) as

$$x = n_1 e_{g_1} + \cdots + n_k e_{g_k},$$

for some $n_i \neq 0$ and g_i, $1 \leq i \leq k$.

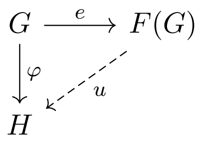
One can easily check that if $|G_1| = |G_2|$, then $F(G_1) \cong F(G_2)$.

The free group $F(G)$ has the following *universal property*:

[5] This makes every abelian group a module over $\mathbb{Z}$.

[6] However, note that e is not a homomorphism and so we cannot identify G with a subgroup of $F(G)$ by means of e: for all $g \neq h \in G$, $e_{g+h} \neq e_g + e_h$. In general, there cannot be any other embedding of G into $F(G)$ unless G is free by Dedekind's theorem. However, we can always identify e_{g+h} and $e_g + e_h$ via a congruence, obtaining that G is a quotient of $F(G)$, see Corollary 3.19. Note that by Theorem **??** a free resolution of a group H splits iff H is embeddable into $F(H)$.

Theorem 3.16 (Universal property)**.** *Whenever $\varphi : G \to H$ is a homomorphism, then there exists a unique homomorphism $u : F(G) \to H$ such that the diagram below commutes. Briefly stated: every homormophism $\varphi : G \to H$ extends uniquely to a homomorphism from $F(G)$ to H.*



Proof. Every element $x \in F(G)$ is a linear (finite) equation of the form $n_1 e_{g_1} + \cdots + n_k e_{g_k}$. Define

$$u(n_1 e_{g_1} + \cdots + n_k e_{g_k}) = n_1 \varphi(g_1) + \cdots + n_k \varphi(g_k). \tag{3.2}$$

The diagram commutes because for every $g \in G$,

$$\varphi(g) = u(e_g).$$

The mapping u is by definition a homomorphism into H, disregarding whether φ is a homomorphism or not. However, φ being a homomorphism implies that $u \circ e = \varphi$ is a homomorphism. In particular we have

$$u(e_{g+h}) = \varphi(g + h) = \varphi(g) + \varphi(h) = u(e_g) + u(e_h).$$

□

Remark 3.17. The mapping u in the previous theorem is well-defined because all the elements of the basis $\{e_g \,|\, g \in G\}$ of $F(G)$ are "independent"[7] in the sense that for any equation $n_1 g_1 + \cdots + n_k g_k$, where g_i are in G, $n_1 e_{g_1} + \cdots + n_k e_{g_k} \neq e_h$ for any $h \in G$. For instance, it always holds $e_{g+h} \neq e_g + e_h$ because they "formally different", but $u(e_{g+h}) = u(e_g) + u(e_h)$.

Corollary 3.18 (Extension of functions on basis, universal property)**.** *Suppose $F(B)$ is the free abelian group generated by basis B and let H be an abelian group. Let $u' : F = B \to H$ be any function. Then there is a unique homomorphism $u : F(B) \to H$ such that $u \restriction B = u'$.*

Proof. Define u as in the previous theorem:

$$u(n_1 b_1 + \cdots + n_k b_k) = n_1 u'(b_1) + \cdots + n_k u'(b_k), \tag{3.3}$$

where the b_i's range over the elements of the basis. □

Corollary 3.19 (Quotients of free groups)**.** *Every abelian group is a quotient of a free group.*

Proof. Apply Theorem 3.16 with $H = G$ and φ the identify function on G. Then $u : F(G) \to G$ is a surjective homomorphism because $\text{im}(\varphi) = G$ which identifies e_{g+h} with $e_g + e_h$. □

[7] The notion of *linear independence* is reserved for vector spaces, i.e. modules over a field: there one can show that every vector space has a basis (a set of linearly independent vectors), and is therefore a free object in the category of modules. This is false for abelian groups in general (not all abelian groups are free). However, a free abelian group is precisely a free module over the ring $\mathbb{Z}$ of integers.