Integral Congruences

To each \( i, j \) belonging to some set of integers, attach the integer \( a_{ij} \). For the congruences

\[
x_j - x_i \equiv a_{ij} \mod (i, j)
\]
to be solvable, we must have

\[
a_{ij} + a_{jk} \equiv a_{ik} \mod (i, j, k)
\]
for all \( i, j, k \).

**Theorem 1** This condition is sufficient.

We can generalize the question as follows. Let \( n \) be a positive integer and \((a(i_0, \ldots, i_n))_{i_0, \ldots, i_n \in I}\) a family of integers. For the congruences

\[
\sum_j (-1)^j x(i_0, \ldots, \hat{i_j}, \ldots, i_n) \equiv a(i_0, \ldots, i_n) \mod (i_0, \ldots, i_n)
\]
to be solvable, we must have

\[
\sum_j (-1)^j a(i_0, \ldots, \hat{i_j}, \ldots, i_{n+1}) \equiv 0 \mod (i_0, \ldots, i_{n+1})
\]
for all \( i_0, \ldots, i_{n+1} \in I \).

**Theorem 2** This condition is sufficient.

To push the generalization further, let \( A \) be an abelian group, \((A_i)_{i \in I}\) a family of subgroups, \( n \) a positive integer and \((a(i_0, \ldots, i_n))_{i_0, \ldots, i_n \in I}\) a family of elements of \( A \). For the congruences

\[
\sum_j (-1)^j x(i_0, \ldots, \hat{i_j}, \ldots, i_n) \equiv a(i_0, \ldots, i_n) \mod A_{i_0} + \cdots + A_{i_n}
\]
to be solvable, we must have

\[
\sum_j (-1)^j a(i_0, \ldots, \hat{i_j}, \ldots, i_{n+1}) \equiv 0 \mod A_{i_0} + \cdots + A_{i_{n+1}}
\]
for all \( i_0, \ldots, i_{n+1} \in I \).

**Theorem 3** This condition is not sufficient in general.
The above statement and its proof were suggested by Pierre Schapira and Terence Tao. Recall that a lattice is **distributive** if one of the two operations is distributive over the other, or, equivalently, if each operation is distributive over the other.

**Theorem 4** If the indexing set $I$ is finite and if the $A_i$ generate a distributive lattice, then the above condition is sufficient.

The above statement and its proof were suggested by Anton Deimtar.

1 **Refinements**

Let $A$ be an abelian group and $(A_i)_{i \in I}$ a family of subgroups. Form the cochain complex

$$C^n(I) := \prod_{i_0, \ldots, i_n \in I} \frac{A}{A_{i_0} + \cdots + A_{i_n}}, \quad d : C^{n-1}(I) \to C^n(I),$$

$$(df)(i_0, \ldots, i_n) \equiv \sum_j (-1)^j f(i_0, \ldots, \hat{i}_j, \ldots, i_n) \mod A_{i_0} + \cdots + A_{i_n}.$$  

Let $(B_j)_{j \in J}$ be another family of subgroups. A map $\tau$ from $J$ to $I$ is a **refinement map** if

$$A_{\tau j} \subset B_j \quad \forall \ j \in J,$$

and $J$ is a **refinement** of $I$ if there is such a refinement map. A refinement map $\tau$ induces a cochain map, still denoted $\tau$, from $C^n(I)$ to $C^n(J)$ defined by

$$(\tau f)(j_0, \ldots, j_n) \equiv f(\tau j_0, \ldots, \tau j_n) \mod B_{j_0} + \cdots + B_{j_n},$$

and thus a morphism $\tau^*$ from $H^n(I)$ to $H^n(J)$.

Let $\sigma$ be another refinement map from $J$ to $I$. We claim $\sigma^* = \tau^*$. Define the morphism $h$ from $C^n(I)$ to $C^{n-1}(J)$ by

$$(hf)(j_0, \ldots, j_{n-1}) := \sum_k (-1)^k f(\tau j_0, \ldots, \tau j_k, \sigma j_k, \ldots, \sigma j_{n-1}) \mod B_{j_0} + \cdots + B_{j_{n-1}}.$$  

We have
\[ dh + hd = \sigma - \tau, \]

which implies the claim.

Let \((A_i)_{i \in I}\) be as above, put

\[ J := \{ A_i \mid i \in I \}, \]

let \((B_j)_{j \in J}\) be the tautological family, let \(\pi\) be the natural surjection from \(I\) onto \(J\) and \(\iota\) a section of \(\pi\). Then \(\pi\) and \(\iota\) are refining maps, and \(C(I)\) and \(C(J)\) are homotopy equivalent.

### 2 Coefficient Systems

Recall the a **simplicial complex** is a set \(K\) equipped with a set of nonempty finite subsets, called **simplices** subject to the condition that a nonempty subset of a simplex is a simplex. A map between two simplicial complexes is **simplicial** if it maps simplices to simplices. For \(n \geq 0\) let \(\Delta_n\) be the set \(\{0, 1, \ldots, n\}\) equipped with the simplicial structure giving the status of simplex to all nonempty finite subsets, say that a a **singular** \(n\)-**simplex** of \(K\) is a simplicial map from \(\Delta_n\) to \(K\), and let \(S_n(K)\) be the set of singular \(n\)-simplices of \(K\). For \(n > 0\) and \(i \in \Delta_n\) let \(f_i\) be the increasing map from \(\Delta_{n-1}\) to \(\Delta_n\) missing the vertex \(i\).

Let \(C_n(K)\) be the free abelian group generated \(S_n(K)\) and consider the morphisms

\[ \partial_n = \partial : C_n(K) \to C_{n-1}(K), \quad \partial s := \sum_i (-1)^i s f_i \quad \forall s \in K_n \]

for \(n > 0\), and

\[ \varepsilon : C_0 \to \mathbb{Z}, \quad s \mapsto 1 \quad \forall s \in S_0(K). \]

Then \((C_*(K), \partial, \varepsilon)\) is an augmented chain complex.

**Lemma 5** Let \(s\) be in \(S_n(K)\) and \(\Phi(s)\) the subgroup of \(C_*(K)\) generated by the singular simplices of the form \(sf\) with \(f : \Delta_k \to \Delta_n\). Then \(\Phi(s)\) is an acyclic augmented subcomplex of \(C_*(K)\).

**Proof.** It is clear that \(\Phi(s)\) is a subcomplex of \(C_*(K)\), and that

\[ sf \mapsto (s0, sf0, \ldots, sf n) \]
is a homotopy from the identity of $\Phi(s)$ to 0. QED

Let $\leq$ be an ordering on $K$ and $\varphi$ be the $\mathbb{Z}$-linear endomorphism of $C_*(K)$ defined by

$$\varphi s := s \text{ if } s \text{ is noninjective},$$

$$\varphi(s_0, \ldots, s_n) := s - (-1)^{\sigma}(s_\sigma 0, \ldots, s_\sigma n) \text{ if } s \text{ is injective, } \sigma \text{ is the permutation characterized by } s_\sigma 0 < \cdots < s_\sigma n, \text{ and } (-1)^{\sigma} \text{ is the signature of } \sigma.$$

Then $\varphi$ is an endomorphism of the augmented complex $(C_*(K), \partial, \varepsilon)$.

**Lemma 6** There is a homotopy $h$ from $\varphi$ to 0 such that $hs$ is in $\Phi(s)$ for all $s \in S_n(K)$.

**Proof.** Put $C_n := C_n(K)$, let $h_0$ be the zero morphism from $C_0$ to $C_1$, and assume that we have morphisms $h_n : C_n \to C_{n+1}$ satisfying

$$\partial_{n+1} h_n = \varphi_n - h_{n-1} \partial_n$$

for $n < k$. We want to define $h_k : C_k \to C_{k+1}$ in such a way that we have

$$\partial_{k+1} h_k = \varphi_k - h_{k-1} \partial_k.$$

Observe

$$\partial_k (\varphi_k - h_{k-1} \partial_k) = \varphi_{k-1} \partial_k - \partial_k h_{k-1} \partial_k$$

$$= \varphi_{k-1} \partial_k - (\varphi_{k-1} - h_{k-2} \partial_{k-1}) \partial_k$$

$$= 0$$

and use the previous Lemma. QED

Let $A$ be a ring (commutative with 1). Define the category $K^\Delta$ as follows. The objects of $K^\Delta$ are the singular simplices of $K$. The morphisms from $s \in S_n(K)$ to $t \in S_k(K)$ are the maps $f$ from $\Delta_k$ to $\Delta_n$ such that $t = sf$, the composition being the obvious one. Say that a **coefficient system** over $K$ is a functor from $K^\Delta$ to the category of $A$-modules.

If $V$ is a coefficient system over $K$, then we denote by $V(s)$ the $A$-module attached to $s \in S_n(K)$ and by $V(s, f)$ the morphism from $V(s)$ to $V(sf)$ associated with the map $f$ from $\Delta_k$ to $\Delta_n$.

Denote by $c = (c(s))_{s \in S_n(K)} \in C^n(K, V)$ the vectors of the $A$-module
\[ C^n(K, V) := \prod_{s \in S_n(K)} V(s). \]

and consider the morphisms

\[ d_{n-1} = d : C^{n-1}(K, V) \to C^n(K, V), \quad (dc)(s) := \sum_i (-1)^i V(s, f_i) c(s) \]

for \( n > 0 \). Then \( (C^*(K, V), d) \) is a cochain complex.

Assume \( V_{s\sigma} = V_s \) whenever \( s \) is injective and \( \sigma \) is a permutation. Say that the cochain \( c \) of \( C^n(K, V) \) is \textbf{alternating} if

(a) \( c(s) = 0 \) whenever \( s \) is noninjective,

(b) \( c(s\sigma) = -c(s) \) whenever \( s \) is injective and \( \sigma \) is an odd permutation.

The alternating cochains form a subcomplex \( C^\prime*(K, V) \) of \( C^*(K, V) \).

If \( \psi \) is a \( \mathbb{Z} \)-linear map from \( C_p(K) \) to \( C_q(K) \) of the form

\[ \psi s = \sum_{f: \Delta_q \to \Delta_p} \lambda_{s,f} s f \]

with \( \lambda_{s,f} \in \mathbb{Z} \), if \( c \) is in \( C^q(K, V) \) and \( s \) in \( S_p(K) \), we put

\[ (h'c)(s) := \sum_f \lambda_{s,f} V(s, f) c(s). \]

We clearly have

**Proposition 7** In the above notation \( 1 - \varphi' \) is a projector onto \( C^\prime*(K, V) \). Moreover if \( h \) is the homotopy of the previous Lemma, then \( h' \) is a homotopy from \( 1 - \varphi' \) to the identity. In particular the inclusion of \( C^\prime*(K, V) \) into \( C^*(K, V) \) is a quasi-isomorphism.

### 3 Rings

By “ring” we mean “commutative ring with 1”. A **domain** is a nonzero ring which has no nontrivial zero divisors. An ideal of a ring is **prime** if the quotient is a domain.

**Lemma 8** The inverse image of a prime ideal under a ring morphism is prime.
Proof. Left to the reader.

A subset \( S \) of a ring \( A \) is \textbf{multiplicative} if it contains 1 and is closed under multiplication. Let \( A \) be a ring, \( S \) a multiplicative subset and \( V \) an \( A \)-module. For \((v_1, s_1), (v_2, s_2) \in V \times S\) write \((v_1, s_1) \sim (v_2, s_2)\) if there is an \( s \in S \) such that \( s(s_1v_2 - s_2v_1) = 0 \). This is an equivalence relation. Let \( S^{-1}V \) be the quotient and denote the class of \((v, s)\) by \( v/s \), by \( v_s \) or by \( s^{-1}v \). For \((v_1, s_1), (v_2, s_2) \in V \times S, a \in A, v \in V\) put

\[
\frac{v_1}{s_1} + \frac{v_2}{s_2} = \frac{s_2v_1 + s_1v_2}{s_1s_2} , \quad \frac{a}{s_1} \frac{v}{s_2} = \frac{av}{s_1s_2} .
\]

These formulas equip respectively \( S^{-1}A \) and \( S^{-1}V \) with well defined structures of ring and \((S^{-1}A)\)-module. We say that \( S^{-1}A \) and \( S^{-1}V \) are respectively the \textbf{ring of fractions of} \( A \) \textbf{with denominators in} \( S \) and the \textbf{module of fractions of} \( V \) \textbf{with denominators in} \( S \). The map

\[i_V : V \to S^{-1}V, \quad v \mapsto \frac{v}{1}\]

is called the \textbf{canonical morphism}.

\textbf{Lemma 9} The canonical morphism \( i_A \) is a ring morphism and \( i_V \) is an \( A \)-module morphism whose kernel consists of those elements of \( V \) which have an annihilator in \( S \).

\textbf{Proof.} Left to the reader.

\textbf{Lemma 10 (Universal Property)} Any ring morphism \( A \to B \) mapping \( S \) into the multiplicative group \( B^\times \) factors uniquely through \( S^{-1}A \). Under the same assumption, if \( V \) is an \( A \)-module and \( W \) a \( B \)-module, then any \( A \)-module morphism \( V \to W \) factors uniquely through \( S^{-1}V \), the induced map \( S^{-1}V \to W \) being an \((S^{-1}A)\)-module morphism.

\textbf{Proof.} Left to the reader.

\textbf{Lemma 11} The \((S^{-1}A)\)-modules \( S^{-1}V \) and \( S^{-1}A \otimes_A V \) are canonically isomorphic.

\textbf{Proof.} Left to the reader.

Recall that an \( A \)-module \( F \) is \textbf{flat} if for all \( A \)-module monomorphism \( W \hookrightarrow V \) the obvious morphism \( F \otimes_A W \to F \otimes_A V \) is injective. The Lemma below, which follows from the previous one, will be freely used.
Lemma 12 The $A$-module $S^{-1}A$ is flat.

Let $A$ be a ring, let $S$ be a multiplicative subset, let $i$ be the canonical morphism $i_A$, let $\mathcal{J}$ be the set of all ideals of $S^{-1}A$ and $\mathcal{I}$ the set of those ideals $I$ of $A$ such that the nonzero elements of $A/I$ have no annihilators in $S$.

Lemma 13 We have

1. $S^{-1}I = (S^{-1}A)i(I)$ for all ideal $I$ of $A$;
2. $S^{-1}i^{-1}(J) = J$ for all $J \in \mathcal{J}$;
3. if $I$ is an ideal of $A$, the ideal $i^{-1}(S^{-1}I)$ of $A$ is formed by those $a$ in $A$ whose image in $A/I$ has an annihilator in $S$;
4. $i^{-1}$ maps $\mathcal{J}$ bijectively onto $\mathcal{I}$ and the inverse bijection is given by $S^{-1}$:

$$\begin{array}{c}
\mathcal{I} \xrightarrow{S^{-1}i^{-1}} \mathcal{J}.
\end{array}$$

5. for $J \in \mathcal{J}$ and $I := i^{-1}(J)$, the canonical morphism from $S^{-1}A$ to $S^{-1}(A/I)$ is surjective, its kernel is $J$ and $i_{A/I}$ is injective;
6. a prime ideal of $A$ is in $\mathcal{I}$ iff it is disjoint from $S$;
7. $S^{-1}$ and $i^{-1}$ induce inverse bijections between the set of prime ideals of $A$ disjoint from $S$ and the set of prime ideals of $S^{-1}A$.

Proof. Follows from the previous Lemmas. QED

Lemma 14 An ideal of $A$ is prime iff its complement is multiplicative.

Proof. Left to the reader.

If $S \subset A$ is the complement of a prime ideal $P$ and $V$ an $A$-module, we put

$$A_P := S^{-1}A, \quad V_P := S^{-1}V.$$  \hfill (1)

Lemma 15 Let $p$ be a prime number and $(F_i)$ a family of finite abelian groups. Then the natural morphism

$$\left( \prod_i F_i \right)_{(p)} \rightarrow \prod_i (F_i)_{(p)}$$

is bijective.

Proof. We can assume either that each $F_i$ is a $p$-group, or that each $F_i$ is a $p_i$-group for some prime $p_i \neq p$. QED

7
4 The local case

Let \( p \) be a prime number. Part 7 of Lemma 13 implies that the ideals of \( \mathbb{Z}_p \) are precisely the powers of \( p \mathbb{Z}_p \). Let \( J_1, J_2, \ldots \) be a (possibly finite) decreasing sequence of ideals of \( \mathbb{Z}_p \), and form the cochain complex

\[
C^n := \prod_{i_0 < \cdots < i_n \in I} \mathbb{Z}_p / J_{i_0}, \quad d : C^{n-1} \to C^n,
\]

\[
(df)(i_0, \ldots, i_n) \equiv \sum_j (-1)^j f(i_0, \ldots, \hat{i}_j, \ldots, i_n) \bmod J_{i_0}.
\]

Proposition 16 We have \( H^n(C) = 0 \) for \( n > 0 \).

Proof. We denote by the same symbol an element of \( \mathbb{Z}_p \) and its class modulo \( J_i \). Let \( a \) be an \( n \)-cocycle of \( C \), and define the element \( x(i_1, \ldots, i_n) \) of \( \mathbb{Z}_p \) inductively on \( i_0 \) as follows. Put first

\[
x(1, i_2, \ldots, i_n) := 0.
\]

For \( i_1 > 1 \) set \( i_0 := i_1 - 1 \) and

\[
x(i_1, \ldots, i_n) := -\sum_{j=1}^{n} (-1)^j x(i_0, \ldots, \hat{i}_j, \ldots, i_n) + a(i_0, \ldots, i_n).
\]

Given \( 1 < i_1 < \cdots < i_n \) prove

\[
x(i_1, \ldots, i_n) \equiv -\sum_{j=1}^{n} (-1)^j x(i_0, \ldots, \hat{i}_j, \ldots, i_n) + a(i_0, \ldots, i_n) \bmod J_{i_0}
\]

successively for \( i_0 = i_1 - 1, i_1 - 2, \ldots, 1 \). QED

5 Proof of the Theorems

Proof of Theorem 2 Let \( C \) be the cochain complex obtained by replacing \( A \) by \( \mathbb{Z} \) and \( A_i \) by \( (i) \) in the definition of the cochain complex \( C(I) \) at the outset of Section 1. Let \( n \) be a positive integer. By Lemma 12 we have \( H^n(C) = H^n(C(p)) \). By Lemma 9 an abelian group \( A \) is trivial iff \( A_p = 0 \) for all \( p \). The triviality of \( H^n(C(p)) \) follows from Section 1, Proposition 7, Part 7 of Lemma 13, Lemma 15, and the above Proposition.
Proof of Theorem 3  Let $V$ be a three dimensional vector space; let $L_1$, $L_2$, $L_3$, $L_4$ be four lines in general position; let $C$ be the cochain complex denoted $C(I)$ in the beginning of Section 1. We claim $H^1(C) \neq 0$. By Proposition 7 we can replace the condition $i_0, \ldots, i_n \in I$ in the definition of $C$ by the condition $i_0 < \cdots < i_n \in I$; in particular we get $C^n = 0$ for $n > 1$, and we claim that the coboundary $d$ from

$$C^0 = \frac{V}{L_1} \oplus \frac{V}{L_2} \oplus \frac{V}{L_3} \oplus \frac{V}{L_4}$$

to

$$C^1 = \frac{V}{L_1 + L_2} \oplus \frac{V}{L_1 + L_3} \oplus \frac{V}{L_1 + L_4} \oplus \frac{V}{L_2 + L_3} \oplus \frac{V}{L_2 + L_4} \oplus \frac{V}{L_3 + L_4}$$

is not onto. But this follows from the fact that the kernel of $d$ contains $V$.

Proof of Theorem 4  As a general notation, write $H^n((A_i), A)$ for the $n$-cohomology of the cochain complex defined at the beginning of Section 1. Theorem 4 results from Theorem 2 and the following fact, whose proof is left to the reader.

Lemma 17  In the notation of the beginning of Section 1 assume that the lattice generated by the $A_i$ is distributive, let $B$ be one of the $A_i$, and $n$ a positive integer. Then

$$H^n((B \cap A_i), A) = 0 = H^n\left(\left(\frac{B + A_i}{B}\right), \frac{A}{B}\right) \Rightarrow H^n((A_i), A) = 0.$$