Abstract Algebra, Lecture 6

Congruences, cosets, and normal subgroups

Jan Snellman[1]

[1]Matematiska Institutionen
Linköpings Universitet

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

Linköping, fall 2019

Lecture notes availabe at course homepage
http://courses.mai.liu.se/GU/TATA55/

Summary

Summary

Summary

Summary

Definition

An equivalence relation $\sim$ on a semigroup S is a

1. *left congruence* if $s \sim t$ implies $as \sim at$ for all $a, s, t \in S$
2. *right congruence* if $s \sim t$ implies $sa \sim ta$ for all $a, s, t \in S$
3. *congruence* if $s \sim t$ and $a \sim b$ implies $sa \sim tb$ for all $a, b, s, t \in S$

Example

Let $\mathbb{P}$ denote the positive integers under multiplication; this is a semigroup (even a monoid). Let $2\mathbb{P}$ denote the subset of even positive integers. Define an equivalence relation $\sim$ by partitioning $\mathbb{P}$ into $2\mathbb{P}$, together with singleton partitions for the odd positive integers. Then $\sim$ is a left congruence, a right congruence, and a congruence.

Lemma

An equivalence relation $\sim$ on a semigroup S is a congruence if and only if it is both a left and a right congruence.

Proof.

- Suppose $\sim$ congruence. Take $a, s, t \in S$ with $s \sim t$. Since $a \sim a$, we have $as \sim at$. Similarly for right.
- Suppose $\sim$ left and right congruence. Take $a, b, s, t \in S$ with $s \sim t$, $a \sim b$. Then

$$s \sim t \implies as \sim at$$

and

$$a \sim b \implies at \sim bt$$

so by transitivity

$$as \sim bt,$$

as desired.

$\square$

Assume: G group, $\sim$ congruence, $N = [1_G]$.

Definition

We say that a subgroup $H \leq G$ is normal in G, written $H \triangleleft G$, if $ghg^{-1} \in H$ for each $h \in H$, $g \in G$. Thus H is closed under conjugation with elements in G.

Theorem

$N \triangleleft G$.

Proof.

$$N \ni h \implies h \sim 1 \implies gh \sim g \implies ghg^{-1} \sim gg^{-1} = 1 \implies ghg^{-1} \in N$$

$\square$

Definition

If $A, B \subseteq G$, then

$$AB = \{\, ab \,|\, a \in A, b \in B \,\}.$$

We use aB for $\{a\}\, B$, an so on and so forth.

Example

For abelian groups written additively, we write $A + B$ instead. For instance, $1 + 4\mathbb{Z}$ are all integers congruent to 1 modulo 4.

Theorem

- *For* $g \in G$, $[g]_\sim = gN = Ng$
- *For* $x, y \in G$, $x \sim y$ *iff* $xy^{-1} \in N$ *iff* $x^{-1}y \in N$.

Proof.

- $x \in [g]_\sim \iff x \sim g \iff xg^{-1} \sim 1 \iff xg^{-1} \in N \iff xg^{-1} = n \iff x = ng \iff x \in Ng$
- $x \sim y \iff xy^{-1} \sim 1 \iff xy^{-1} \in N$

$\square$

So, a group congruence is completely determined by the equivalence class $[1]_\sim$. This is not so for semigroups.

Now let $H \leq G$ be a *not necessarily normal* subgroup of G.

Definition

For $x, y \in G$, define $x \sim_L y$ iff $y^{-1}x \in H$, and define $x \sim_R y$ iff $xy^{-1} \in H$.

Theorem

- $x \sim_L y$ *iff* $x \in yH$
- $x \sim_H y$ *iff* $x \in Hy$
- $\sim_L$ *is a left congruence*
- $\sim_R$ *is a right congruence*

Proof.

$x \sim_L y \iff y^{-1}x \in H \iff x \in yH \implies tx \in tyH \iff tx \sim_L ty.$ $\square$

Definition

The equivalence class $[x]_{\sim_L} = xH$ is called the *left coset* of H containing x. The right coset is $[x]_{\sim_R} = Hx$

Theorem (Lagrange)

The left cosets (and the right cosets) are all equipotent with H. Thus, if G is finite, then $|G| = |H|m$, where m is the number of distinct left cosets, also called the index of H in G, denoted $[G : H]$.

Proof.

Let $g \in G$. Then $H \ni h \mapsto gh \in gH$ is surjective by definition, and injective since $gh_1 = gh_2 \implies g^{-1}gh_1 = g^{-1}gh_2$. $\square$

Example

- In our example $\mathbb{P} = 2\mathbb{P} \cup_{k \in \mathbb{P}} \{2k-1\}$ one equivalence is infinite, and the rest singletons — this could never happen in a group!
- If $G = S_3$, $H = \langle (1,2) \rangle$, then the left cosets are

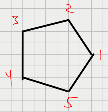
  $$()H = \{(), (1,2)\}, (1,3)H = \{(1,3), (1,2,3)\}, (2,3)H = \{(2,3), (1,3,2)\},$$

  whereas the right cosets are

  $$H() = \{(), (1,2)\}, H(1,3) = \{(1,3), (1,3,2)\}, H(2,3) = \{(2,3), (1,2,3)\}.$$

  So the left and right cosets, while equally many and equally big, are different. Of course, $\sim_L \neq \sim_R$. Furthermore, H is not normal.

D_5



$r = (1,2,3,4,5)$

$s = (2,5)(3,4)$

$sr = (1,5)(2\,4)(3)$

$sr^2 = (1,4)(2,3)(5)$

$\boxed{sr^3 = (1,3)(2)(4,5)}$

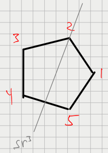
$sr^4 = sr^{-1} = rs = (1\;2)(3,5)(4)$

$r^5 = 1$

$s^2 = 1$

$rsrs = 1$

$rs = sr^{-1}$



$H = \{e, sr^3\}$

$rH = \{r, rsr^3 = sr^{-1}r^3 = sr^2\}$, $Hr = \{r, sr^4\}$

$sH = \{s, r^3\}$, $Hs = \{s, sr^3s\}$

$srr\underline{rs} = sr\underline{rs}r^{-1} = sr\underline{s}r^{-1}r^{-1}$

$= ssr^{-1}r^{-1}r^{-1} = r^{-3} = r^2$

In fact:

Lemma

The following are equivalent:

1. $H \triangleleft G$,
2. $\sim_L = \sim_R$,
3. $gH = Hg$ *for all* $g \in G$.

When this holds, $\sim_L$ *and* $\sim_R$ *are congruences.*

Corollary

Let G be a finite group with n elements. Let H be a subgroup of G, and $g \in G$.

- *The size of H divides n,*
- *$o(g)$ divides n.*

Proof.

$o(g) = |\langle g \rangle|$. □

Example

There is no element in S_6 of order 7. Nor is there a subgroup of size 25.

Example

The full symmetry group of a cube has 48 elements, so *a priori*, the possible orders of elements are

$$1, 2, 3, 4, 6, 8, 12, 16, 24, 32$$

Actually occuring orders are

$$1, 2, 3, 4$$

Recall that for a positive integer n, $U_n = \{\, [k]_n | \gcd(k,n) = 1 \,\}$ is a group under multiplication.

Definition

Euler's totient ϕ is defined by $\phi(n) = |U_n|$.

Lemma

1. *If p is a prime number, then $\phi(p^r) = p^r - p^{r-1}$,*
2. *If $\gcd(m,n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$*
3. *If n has prime factorization $n = \prod_j p_j^{a_j}$, then* $\phi(n) = \prod_j \phi(p_j^{a_j}) = \prod_j (p_j^{a_j} - p_j^{a_j - 1})$.

Proof.

Elementary, CRT, immediate consequence. □

Recall that if $o(g) = n$, then $g^k = 1$ iff $n|k$.

Theorem (Euler)

If $n \not| a$ then

$$a^{\phi(n)} \equiv 1 \mod n$$

Proof.

By Lagrange, since $\phi(n) = |U_n|$, and since

$$[a]_n^k = [1]_n \in U_n \quad \iff \quad a^k \equiv 1 \mod n$$

$\square$

Historically, the special case of prime modulus was proved first, using elementary means:

Theorem (Fermat)

If p prime, and $p \not| a$ then,

$$a^{p-1} \equiv 1 \mod p$$

Example

$$20^{258} \equiv 3^{258} \equiv 3^{16*16+2} \equiv (3^{16})^{16} * 3^2 \equiv 1^{16} * 9 \equiv 9 \mod 17$$

Example

$$x = 7^{123} \equiv 7^{12*10+3} \equiv (7^{12})^{10} * 7^3 \equiv 7^3 \equiv 49 * 7 \equiv 9 * 7 \equiv 3 \mod 20$$

since $\phi(20) = \phi(4 * 5) = \phi(4) * \phi(5) = 3 * 4 = 12$.
Alternatively,

$$x \equiv 3^{123} \equiv 3^{2*61+1} \equiv 3 \mod 4$$

and

$$x \equiv 5^{123} \equiv 3^{4*30+1} \equiv 3 \mod 5$$

so by CRT, $x \equiv 3 \mod 20$.

Definition

If S, T are semigroups, then a semigroup homomorphism is a function $f : S \to T$ such that $f(xy) = f(x)f(y)$ for all $x, y \in S$. If S, T are both monoids, we demand in addition that $f(1) = 1$. If S, T are both groups, then it follows that a monoid homomorphism will also preserve inverses.

We have previously defined group isomorphisms, which are bijective group homomorphisms.

Lemma

The inverse of a group isomorphism is a group isomorphism.

Definition

Let G, H be semigroups, and let $\phi : G \to H$ be a semigroup homomorphism, i.e., $\phi(g_1 g_1) = \phi(g_1)\phi(g_2)$ for all $g_1, g_2 \in G$. We define

- $\mathrm{Im}(\phi) = \phi(G) = \{\, \phi(g) | g \in G \,\}$,
- $\ker(\phi) = \{\, (g_1, g_2) \in G | \phi(g_1) = \phi(g_2) \,\}$.

Lemma

$\mathrm{Im}(\phi)$ *is a subsemigroup of* H *and* $\ker(\phi)$ *is a congruence on* G*.*

Proof.

If $h_1, h_2 \in \mathrm{Im}(\phi)$ then $h_1 = \phi(g_1)$, $h_2 = \phi(g_2)$, so
$h_1 h_2 = \phi(g_1)\phi(g_2) = \phi(g_1 g_2) \in \mathrm{Im}(\phi)$.
If $(g_1, g_2), (k_1, k_2) \in \ker(\phi)$ then $\phi(g_1) = \phi(g_2)$ and $\phi(k_1) = \phi(k_2)$.
Hence $\phi(g_1 k_1) = \phi(g_1)\phi(k_1) = \phi(g_2)\phi(k_2) = \phi(g_2 k_2)$, so
$(g_1 k_1, g_2, k_2) \in \ker(\phi)$. $\square$

Lemma

If $\phi : G \to H$ is a group homomorphism, then

1. $\mathrm{Im}(\phi)$ *is a subgroup of* H,
2. $\phi^{-1}(\{1_H\})$ *is a normal subgroup of* G. *It coincides with the class* $N = [1_G]$ *of the identity element of* G, *under the kernel congruence.*
3. *More explicitly,* $\phi(x) = \phi(y)$ *iff* $(x, y) \in \ker \phi$ *iff* $xy^{-1} \in N$ *iff* $x^{-1}y \in N$

Definition

By abuse of notation, when ϕ is a group homomorphism, we call N the kernel of ϕ, and denote it by $\ker(\phi)$.

The kernel congruence is determined by N, in that all other classes are translates of N.

Lemma

Let $\phi : G \to H$ be a group homomorphism. Then ϕ is injective iff $\ker(\phi) = \{1_G\}$.

Proof.

By definition of group homomorphism, we have that $\phi(1_G) = 1_H$. If ϕ is injective, no other element of G maps to 1_H.

Conversely, suppose that $\ker(\phi) = \{1_G\}$, and that $\phi(x) = \phi(y)$. Then $\phi(x)\phi(y)^{-1} = 1_H$, so $\phi(xy^{-1}) = 1H$, so $xy^{-1} \in \ker(\phi)$. By assumption, $xy^{-1} = 1_G$, and so $x = y$. □

Definition

Let $\sim$ be a congruence on the semigroup S. Then the set of equivalence classes is denoted by $S/\sim$.

Example

In our example with a congruence on $\mathbb{P}$, the quotient $\mathbb{P}/\sim$ contains one element for each odd positive number, and one element representing the even positive numbers.

Theorem

1. *$S/\sim$ becomes a semigroup under the (well-defined) operation*

$$[x]_\sim * [y]_\sim = [xy]_\sim$$

2. *The canonical surjection*

$$\begin{aligned} S &\to S/\sim \\ x &\mapsto [x]_\sim \end{aligned}$$

is a semigroup homomorphism, i.e., $x * y$ is mapped to $[x]_\sim * [y]_\sim$

3. *Conversely, for any surjective semigroup homomorphism $f : S \to T$, the kernel*

$$\ker f = \left\{ (x, y) \in S^2 \middle| f(x) = f(y) \right\}$$

is a congruence.

4. *Finally, if $\sim$ is a congruence on S, the kernel congruence of the canonical surjection above is simply $\sim$.*

The group version is as follows:

Theorem

Let $\phi : G \to H$ be a surjective group homomorphism, with kernel N, and associated congruence $\sim$. Then the quotient $S/\sim = S/N$ is the set of left (or right) cosets of N. It becomes a group with the operation

$$[x]_\sim [y]_\sim = [xy]_\sim,$$

or equivalently,

$$xN * yN = (xy)N$$

Conversely, if $N \triangleleft G$ then the canonical surjection $\pi : G \to G/N$ defined by $\pi(g) = gN$ has kernel N.

Epimorphisms, normal subgroups, congruences

$$
\begin{tikzcd}
 & \text{epimorphism } \phi \arrow[dl, bend right, "N=\mathtt{ker}(\phi)"'] \arrow[dr, bend left, "\phi(x)=\phi(y)"] & \\
\text{normal subgroup } N \arrow[ur, bend right, "G\to G/N"] \arrow[rr, bend right, "xN=yN"'] & & \text{congruence } \sim \arrow[ul, bend left, "G\to G/\sim"'] \arrow[ll, "N=[1]"]
\end{tikzcd}
$$

Theorem (First isomorphism thm)

If $\phi : G \to H$ is a group homomorphism with kernel N, then $G/N \simeq \mathrm{Im}(\phi)$.

Proof.

The map $gN \mapsto \phi(g)$ is well-defined, and has image $\mathrm{Im}(\phi)$. Furthermore, $g_1Ng_2N = (g_1g_2)N \mapsto \phi(g_1g_2) = \phi(g_1)\phi(g_2)$, so it is a homomorphism. If $gN \mapsto 1_H$ then $\phi(g) = 1_H$, thus $g \in N$, thus $gN = N$. So the assignment is injective, as well. □

The semigroup version is similar.

One often makes use of the following version:

Theorem

Suppose that $\phi : G \to H$ is a group homomorphism, and let M be a normal subgroup of G contained in $\ker(\phi)$. Then there is a unique group homomorphism $\tau : G/M \to H$, with $\mathrm{Im}(\tau) = \mathrm{Im}(\phi)$, and such that $\tau \circ \pi = \phi$. In other words, the following diagram commutes:

$$\begin{tikzcd} G \arrow[r, "\phi"] \arrow[d, "\pi"'] & H \\ G/M \arrow[ur, "\tau"'] & \end{tikzcd}$$

Example

Let $G = (\mathbb{R}, +, 0)$ and let $H = \mathbb{C}^*, *, 1)$, and define

$$\begin{aligned} \phi &: G \to H \\ \phi(x) &= \exp(2\pi x i) \end{aligned}$$

1. Then $\mathrm{ker}(\phi) = \mathbb{Z}$, and $\mathrm{Im}(\phi) = \mathfrak{T}$. So first iso yields $\mathbb{R}/\mathbb{Z} \simeq \mathfrak{T}$.
2. Let $M = 2\mathbb{Z}$. Convenient thm implies surj grp. hom. $\tau : \mathbb{R}/(2\mathbb{Z}) \to \mathfrak{T}$ well-defined by $\tau(x + (2\mathbb{Z})) = \phi(x)$. We can think of $\mathbb{R}/(2\mathbb{Z})$ as a "larger circle".

Example

Let G be a group, and $g \in G$. The map

$$\mathbb{Z} \ni n \mapsto g^n \in G$$

is a group homomorphism, with image $\langle g \rangle$, and kernel $\{0\}$ if $o(g) = \infty$, $k\mathbb{Z}$ if $o(g) = k$. Thus first iso thm yields

$$\mathbb{Z} \simeq \langle g \rangle$$

in the first case, and

$$\mathbb{Z}/(k\mathbb{Z}) \simeq \langle g \rangle$$

in the second case.

Example

Let GL_n denote the group of invertible, real, n by n matrices, with matrix multiplication. The subset SGL_n of matrices with determinant $+1$ forms a subgroup. We claim that this subgroup is normal, and that the quotient is isomorphic to $\mathbb{R}^*$, the group of the non-zero real numbers, under multiplication.

Rather than proving this directly, note that the map

$$\mathrm{GL}_n \ni M \mapsto \det(M) \in \mathbb{R}^*$$

is a surjective group homomorphism, with kernel SGL_n.

Theorem (Second iso thm)

Suppose G group, $H \leq G$, $N \triangleleft G$. Then $HN \leq G$, $(H \cap N) \triangleleft H$, $N \triangleleft HN$, and

$$\frac{H}{H \cap N} \simeq \frac{HN}{N}$$

Proof.

We omit the proofs that HN subgroup et cetera. Define a map

$$\phi : H \to \frac{HN}{N}$$
$$\phi(h) = hN$$

Group hom., surj. by def. But

$$\ker(\phi) = \{ h \in H | \phi(h) = 1N \} = \{ h \in H | h \in N \} = H \cap N$$

First iso. thm. gives

$$\frac{HN}{N} \simeq \frac{H}{\ker(\phi)} = \frac{H}{H \cap N},$$

as desired. $\square$

Example

$G = \mathbb{Z}$, $H = 10\mathbb{Z}$, $N = 12\mathbb{Z}$. Then $H + N = 2\mathbb{Z}$, $H \cap N = 60\mathbb{Z}$, and

$$\frac{10\mathbb{Z}}{60\mathbb{Z}} = \frac{H}{H \cap N} \simeq \frac{H+N}{N} = \frac{2\mathbb{Z}}{12\mathbb{Z}}$$

This quotient is furthermore isomorphic to

$$\frac{\mathbb{Z}}{6\mathbb{Z}} \simeq \mathbb{Z}_6 \simeq C_6$$

Theorem (Third iso. thm.)

G group, N, H normal subgroups of G, $N \subseteq H$. Then $N \triangleleft H$, and $H/N \triangleleft G/N$, and

$$\frac{G/N}{H/N} \simeq \frac{G}{H}$$

Proof.

Consider the surjective (and well-defined) group homomorphism

$$\phi : \frac{G}{N} \to \frac{G}{H}$$
$$\phi(gN) = gH$$

Its kernel is H/N, so an appeal to the first iso. thm. finishes the proof. □

Example

Let $G = \mathbb{Z} \times \mathbb{Z}$, $H = \langle (0,1) \rangle$, $N = \langle (0,2) \rangle$. Then $G/N \simeq \mathbb{Z} \times \mathbb{Z}_2$, $G/H \simeq \mathbb{Z}$, $H/N \simeq \mathbb{Z}_2$, and

$$\frac{G/N}{H/N} \simeq \frac{\mathbb{Z} \times \mathbb{Z}_2}{\mathbb{Z}_2} \simeq \mathbb{Z} \simeq \frac{G}{H}$$

Example

$$12\mathbb{Z} \triangleleft 6\mathbb{Z} \triangleleft \mathbb{Z},$$

and

$$\frac{\mathbb{Z}/(12\mathbb{Z})}{(6\mathbb{Z})/(12\mathbb{Z})} \simeq \frac{\mathbb{Z}}{6\mathbb{Z}}$$

Theorem (Correspondence thm)

G group, N normal subgroup, $\pi : G \to G/N$ canonical quotient epimorphism, $\mathcal{A}$ set of all subgroups of G which contain N, $\mathcal{B}$ set of all subgroups of G/N. Then

$$
\begin{aligned}
&\sigma : \mathcal{A} \to \mathcal{B} \\
&\sigma(H) = \pi(H) = H/N \\
&\tau : \mathcal{B} \to \mathcal{A} \\
&\tau(K) = \pi^{-1}(K) = \{ g \in G | gN \in K \}
\end{aligned}
$$

are inclusion-preserving and each others inverses, thus establishing an inclusion-preserving bijection between $\mathcal{A}$ and $\mathcal{B}$. Furthermore, in this bijection, normal subgroups correspond to normal subgroups.

Example

Since $\mathbb{Z} \lhd \mathbb{R}$ and $\mathbb{R}/\mathbb{Z} \simeq \mathfrak{T}$, subgroups of $\mathfrak{T}$ correspond to those subgroups of $\mathbb{R}$ that contain $\mathbb{Z}$.

Example

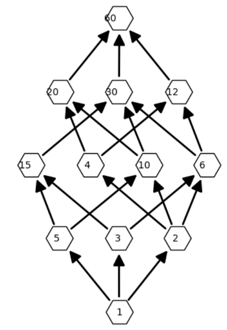
The set of subgroups of GL_n which contain all matrices of determinant one is in bijective correspondence with subgroups of $\mathbb{R}^*$.

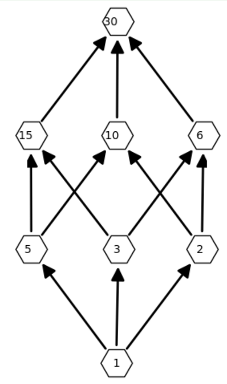
Example

Subgroups of $\mathbb{Z}$ which contains $4\mathbb{Z}$ correspond to subgroups of $\mathbb{Z}/(4\mathbb{Z}) \simeq \mathbb{Z}_4$, which has **one** proper, nontrivial subgroup, namely $\{[0]_4, [2]_4\}$. The relevent subgroup of $\mathbb{Z}$ is $2\mathbb{Z}$.

Example

We show $C_{60} = \langle g \rangle$ and its subgroups, and then the quotient by the subgroup $\langle g^{30} \rangle$ and its subgroups; the subgroups in the quotient correspond to subgroup in the large group containing thab by which we mod out.





Conjugacy

- G group
- Equivalence relation: $h_1 \sim_c h_2$ iff exists $g \in G$ s.t. $h_2 = gh_1g^{-1}$.
- Eg invertible matrices are conjugate if they correspon to the same linear transformation, after change of basis
- Conjugacy classes: equivalence classes under $\sim_c$.
- In S_n, correspond to cycle type
- In $G \leq S_n$, necessary but not sufficient, must have $g \in G$, not $g \in S_n$.

- G still group, $H \leq G$ subgroup
- The following are equivalent:
  1. For all $g \in g$, $h \in h$ it holds that $ghg^{-1} \in H$.
  2. For all $g \in G$ it holds that $gHg^{-1} = \{ ghg^{-1} | h \in H \} \subseteq H$
  3. H is the union of conjugacy classes
  4. H is the kernel of some group homomorphism $\phi : G \to K$, K some group
  5. H is the kernel of some group epimorphism $\phi : G \to K$, K some group
  6. There is some *congruence* τ on G such that $H = [1]_\tau$.
  7. The left congruence $x \sim_L y$ iff $y^{-1}x \in H$ is a congruence
  8. The right congruence $x \sim_R y$ iff $xy^{-1} \in H$ is a congruence
  9. For all $g \in G$, the left coset gH is equal to the right coset Hg
  10. The multiplication $(g_1H)(g_2H) = (g_1g_2)H$ is well defined
  11. The multiplication $(Hg_1)(Hg_2) = H(g_1g_2)$ is well defined

Example

Let $G = S_4$, $H = \{(), (12)(34), (13)(24), (14)(23)\}$. We check that $H \leq G$. Is H normal in G? If so, what is G/H?

Example

Let H, K be groups, and let $G = H \times K$. Put $\tilde{H} = \{ (h,k) \in G | k = 1 \}$ and $\tilde{K} = \{ (h,k) \in G | h = 1 \}$. Is $\tilde{H}$ normal in G? If so, what is G/H?