Lecture 9: Group theory recalled

In order to make progress, we shall need some ideas from group theory. What is remarkable is that we don't need very much: essentially only Lagrange's theorem. I assume that you have met these topics before and that this is essentially revision.

From monoids to groups

The basic building block of many algebraic systems is the monoid: this is a set equipped with an associative binary operation, making it a semigroup, that also has an identity element, which makes it a monoid.

Let M be a monoid with identity 1. We say that an element $a \in M$ is *invertible* if there is an element $b \in M$ such that $ab = 1 = ba$. The element b is called an *inverse* of a and is, in fact, unique if it exists; we shall prove this in the exercises. If we are using multiplicative notation the inverse of a is denoted by a^{-1}; if we are using additive notation then the inverse is denoted by $-a$ and the identity is denoted by 0. This is notation not mathematics. Clearly the identity element is invertible. If a and b are invertible elements then so too is their product: it has inverse $b^{-1}a^{-1}$. It follows that the set of invertible elements of M, denoted by $U(M)$, is closed under multiplication and so is a submonoid of M but it has the additional property that every element of $U(M)$ has an inverse. Monoids in which every element is invertible are called *groups*. Thus $U(M)$ is a group, called the *group of units* of the monoid M. The word 'unit' is an alternative word for invertible element.

Examples 0.1.

(1) Let A^* be the free monoid on the finite alphabet A. The only invertible element is the empty string. Thus $U(A^*)$ has just one element.

(2) Let $T(X)$ be the monoid of all functions from the set X to itself. Then an element is invertible if and only if it is a bijection. The group $U(T(X)) = S(X)$ the group of all bijections of X to itself, also called the group of all permutations on X, or the *symmetric group on X*.

(3) Let $M_n(\mathbb{R})$ be the monoid of all $n \times n$ real matrices. Such a matrix is invertible in the above sense if and only if it is invertible in the usual sense: that is if and only if its determinant is non-zero. The group here is $GL_n(\mathbb{R})$ the *general linear group.*

(4) Let $\mathbb{Z}$ be the integers with *multiplication* as the binary operation. Then the group here is simply $\{-1, 1\}$.

Basic group definitions

For the remainder of this lecture we shall deal only with groups. Let G be a group with identity 1. The *order* of the group G, denoted by $|G|$ is the number of elements it contains. This can be either finite or infinite and so we speak of *finite groups* and *infinite groups.* In cryptography the groups are usually finite. A group is *abelian* or *commutative* if $gh = hg$ for all $g, h \in G$. A group that isn't abelian is said to be *non-abelian.* It is a fact that abelian groups are much easier to handle than non-abelian groups. In this course, our groups will generally be finite abelian groups.

If $g \in G$ then g^n where $n \geq 1$ is the element g multiplied by itself n times. We define $g^0 = 1$. We also define $g^{-n} = (g^{-1})^n$. Thus we may define g^n for any *integer* n. The usual laws of exponents hold. If A and B are subsets of G then by definition

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

If we denote by $\mathsf{P}(G)$ the set of all subsets of G then with respect to the above binary operation it becomes a monoid. If $B = \{b\}$ a singleton set then we usually just write b instead of $\{b\}$.

A subset H of G is said to be a *subgroup* if it contains the idenity element and is closed under multiplication and inverses. We write $H \leq G$ to mean that H is a subgroup of G. The smallest subgroup is $\{1\}$, called the *trivial subgroup*, and the largest is G itself. A subgroup of G not equal to G is said to be *proper.*

There is an important way of constructing subgroups of groups from elements. Let $g \in G$. Put

$$\langle g \rangle = \{g^n \colon n \in \mathbb{Z}\}.$$

Then it is an exercise to check that this is a subgroup of G called the *subgroup generated by the element g*. If this subgroup is finite we say that g has *finite order* with order the number of elements in $\langle g \rangle$. This is the case that will be of interest to us.

Lemma 0.2. *Let G be an element of finite order k in the group G. Then in fact*

$$\langle g \rangle = \{g^i \colon 0 \leq i < k\}.$$

In particular, k is the smallest integer strictly greater than 1 such that $g^k = 1$.

Proof. We suppose that the set $\langle g \rangle$ is finite. This means that there are distinct integers m and n such that $g^m = g^n$. It follows that there exist natural numbers $k \geq 1$ such that $a^k = 1$. We choose k to be the smallest. Let g^n be any power of g. Then by the Remainder Theorem, we may write $n = qk + r$ where $0 \leq k < k$ for some q. Then

$$g^n = g^{qk+r} = (g^k)^q g^r = g^r$$

which proves our claim and at the same time is a nice illustration of how the Remainder Theorem is used. □

If there is an element $g \in G$ such that $G = \langle g \rangle$ then G is said to be *cyclic*. It is clear that cyclic groups are abelian. In fact, it turns out, though we shan't prove it, that cyclic groups are the building blocks of all abelian groups. Cylic groups are very easy to calculate with.

Partitions and equivalence relations

A collection of individuals can be divided into disjoint groups in many different ways. This simple idea is the main mathematical tool needed in this lecture and forms one of the most important ideas in algebra.

Let X be a set. A *partition* of X is a set P of subsets of X satisfying the following three conditions:

(P1): Each element of P is a non-empty subset of X.
(P2): Distinct elements of P are disjoint.
(P3): Every element X belongs to at least one (and therefore by (P2) exactly one) element of P.

The elements of P are called the *blocks* of the partition.

Examples 0.3. Some examples of partitions.

(1) Let

$$X = \{0, 1, \dots, 9\}$$

and

$$P = \{\{0, 1, 2\}, \{3, 4\}, \{5, 6, 7, 8\}, \{9\}\}.$$

Then P is a partition of X containing four blocks.

(2) The set $\mathbb{N}$ of natural numbers can be partitioned into two blocks: the set of even numbers, and the set of odd numbers.

(3) The set $\mathbb{N}$ can be partitioned into three blocks: those numbers divisible by 3, those numbers that leave remainder 1 when divided by 3, and those numbers that leave remainder 2 when divided by 3.

(4) The set $\mathbb{R}^2$ can be partitioned into infinitely many blocks: consider the set of all lines l_a of the form $y = x + a$ where a is any real number. Each point of $\mathbb{R}^2$ lies on exactly one line of the form l_a.

A partition is defined in terms of the set X and the set of blocks P. However, there is an alternative way of presenting this information that is often useful. With each partition P on a set X, we can define a binary relation $\sim_P$ on X as follows:

$$x \sim_P y \Leftrightarrow x \text{ and } y \text{ belong to the same block of } P.$$

The proof of the following is left as an exercise.

Lemma 0.4. *The relation $\sim_P$ is reflexive, symmetric, and transitive.*

Any relation on a set that is reflexive, symmetric, and transitive is called an *equivalence relation*. Thus from each partition we can construct an equivalence relation. In fact, the converse is also true.

Lemma 0.5. *Let $\sim$ be an equivalence relation on the set X. For each $x \in X$ put*

$$[x] = \{y \in X \colon\ x \sim y\}$$

and

$$X/\!\sim = \{[x] \colon\ x \in X\}.$$

Then $X/\!\sim$ is a partition of X.

Proof. For each $x \in X$, we have that $x \sim x$, because $\sim$ is reflexive. Thus (P1) and (P3) hold. Suppose that $[x] \cap [y] \neq \emptyset$. Let $z \in [x] \cap [y]$. Then $x \sim z$ and $y \sim z$. By symmetry $z \sim y$, and so by transitivity $x \sim y$. It follows that $[x] = [y]$. Hence (P2) holds. □

The set

$$[x] = \{y \in X \colon\ x \sim y\}$$

is called the $\sim$-*equivalence class* containing x.

The lemmas above tells us how to construct equivalence relations from partitions, and how to construct partitions from equivalence relations. The following theorem tells us what happens when we perform these two constructions one after the other.

Theorem 0.6. *Let X be a non-empty set.*

- (i): *Let P be a partition on X. Then the partition associated with the equivalence relation $\sim_P$ is P.*
- (ii): *Let $\sim$ be an equivalence relation on X. Then the equivalence relation associated with the partition $X/\!\sim$ is $\sim$.*

Proof. (i) Let P be a partition on X. By above we can define the equivalence relation $\sim_P$. Let $[x]$ be a $\sim_P$-equivalence class. Then $y \in [x]$ iff $x \sim_P y$ iff x and y are in the same block of P. Thus each $\sim_P$-equivalence class is a block of P. Now let $B \in P$ be a block of P and let $u \in B$. Then $v \in B$ iff $u \sim_P v$ iff $v \in [u]$. Thus $B = [u]$. It follows that each block of P is a $\sim_P$-equivalence class and vice versa. We have shown that P and $X/\sim_P$ are the same.

(ii) Let $\sim$ be an equivalence relation on X. By above, we can define a partition $X/\sim$ on X. Let $\equiv$ be the equivalence relation defined on X by the partition $X/\sim$ according to our lemma above. We have that $x \equiv y$ iff $y \in [x]$ iff $x \sim y$. Thus $\sim$ and $\equiv$ are the same relation. □

Notation Let ρ be an equivalence relation on a set X. Then the ρ-equivalence class containing x is often denoted $\rho(x)$.

The theorem above tells us that partitions on X and equivalence relations on X are two ways of looking at the same thing. In applications, it is the partition itself that is interesting, but checking that we have a partition is usually done indirectly by checking that a relation is an equivalence relation.

The following example introduces some notation that we shall use throughout this chapter.

Example 0.7. Let $X = \{1, 2, 3, 4\}$ and let $P = \{\{2\}, \{1, 3\}, \{4\}\}$. Then P is a partition on X. The equivalence relation $\sim$ associated with P can be described by a set of ordered pairs, and these can be conveniently described by a table. The table has rows and columns labelled by the elements of X. Thus each square can be located by means of its co-ordinates: (a, b) means the square in row a and column b. The square (a, b) is marked with $\surd$ if $a \sim b$ and marked with $\times$ otherwise. Strictly speaking we need only mark the squares corresponding to pairs which are $\sim$-related, but I shall use both symbols.

	1	2	3	4
1	$\surd$	$\times$	$\surd$	$\times$
2	$\times$	$\surd$	$\times$	$\times$
3	$\surd$	$\times$	$\surd$	$\times$
4	$\times$	$\times$	$\times$	$\surd$

In fact, this table contains redundant information because if $a \sim b$ then $b \sim a$. It follows that the squares beneath the leading diagonal need not be marked. Thus we obtain

	1	2	3	4
1	$\surd$	$\times$	$\surd$	$\times$
2	$*$	$\surd$	$\times$	$\times$
3	$*$	$*$	$\surd$	$\times$
4	$*$	$*$	$*$	$\surd$

We call this the *table form* of the equivalence relation.

Lagrange's theorem

Let's begin by stating the theorem we shall prove.

Theorem 0.8 (Lagrange)**.** *Let G be a finite group and let H be a subgroup of G. Then the order of H divides the order of G.*

It's important to be clear about what this theorem is saying. It does **not** say that if a number n divides $|G|$ that there will be a subgroup H with order n; this is the converse to Lagrange's theorem and is not true in general (there are counterexamples).

The most important application of the theorem is the following corollary.

Corollary 0.9. *Let G be a finite group with order n. Let g be any element of G. Then $g^n = 1$.*

Proof. Let $H = \langle g \rangle$ have order k. Then by Lagrage's theorem $k \mid n$. But $g^k = 1$ and so $g^n = 1$, as required. □

Now let's turn to the proof of Lagranges's theorem. The key idea we need is that of a coset. Let $H \leq G$ be a subgroup. let $g \in G$ be any element. The subset

$$Hg = \{hg \colon h \in H\}$$

is called a *right coset* of H in G. Denote by G/H the set of all right cosets of H in G. Here is the main result.

Proposition 0.10. *Let G be a group and H a subgroup of G.*

(1) *G/H is a partition of G.*
(2) *Any two blocks of this partition contain the same number of elements.*

Proof. We sketch the proof, and I shall leave you to fill in the details. (1) Let $Ha \cap Hb \neq \emptyset$. We prove that $Ha = Hb$. By assumption there exists $g = ha = kb$ where $h, k \in H$. Thus $a = (h^{-1}k)b$. But $h^{-1}k \in H$ because H is a subgroup. It follows that if $h'a \in Ha$ then $h'a = h'(h^{-1}k)b$ and so $ha \in Hb$. Hence $Ha \subseteq Hb$. By symmetry $Hb \subseteq Ha$. We have therefore proved that $Ha = Hb$.

(2) Define a function $\alpha \colon H \to Ha$ by $\alpha(h) = ah$. Then this function is a bijection. □

Notation When the group operation is denoted by addition then a right coset of H is written $H + g$ and consists of the elements $h + g$ where $h \in H$. We shall use this notation when we come to talk about error-correcting codes.

We finish off with an important result.

Lemma 0.11. *Let g be an element of order k in a group G. Then $g^n = 1$ if and only if $k \mid n$.*

Proof. Suppose that $k \mid n$. Then $n = dk$ for some d. We calculate

$$g^n = g^{dk} = (g^k)^d = 1.$$

Suppose now that $g^n = 1$. By the remainder theorem we may write $n = qk + r$ where $0 \leq r < k$. Thus $g^n = g^{qk+r} = (g^k)^q g^r = g^r$. But we are assuming that this is the identity and that $r < k$ the order of g. It follows that $r = 0$ and so $k \mid n$, as required. □