Math 551 – Algebra – Fall 2000

A. Groups

1. Definition and examples.

Definition. *A group is a set G together with a binary operation $G \times G \to G$, written as multiplication, such that*

(1) The operation is associative: $g(hk) = (gh)k$ for all $g, h, k \in G$;

(2) There exists $1 \in G$ such that $g1 = 1g = g$ for all $g \in G$;

(3) For every $g \in G$ there is $g^{-1} \in G$ such that $gg^{-1} = g^{-1}g = 1$.

1a. Symmetric groups

Ex. A. Let X be any set. A permutation of X is a bijection $\sigma : X \to X$, i.e., a mapping on X which is one-to-one and onto X. Let

$$\Sigma_X = \{\sigma : X \to X \,|\, \sigma \text{ is a permutation of } X\}.$$

For $\sigma, \tau \in \Sigma_X$ define $\sigma\tau = \sigma \circ \tau$, the composite of σ and τ. Also let 1_X be the identity mapping $1_X(x) = x$, $x \in X$, and for each $\sigma \in \Sigma_X$, let σ^{-1} be the inverse mapping: $\sigma^{-1}(x) = y \iff \sigma(y) = x$. Then Σ_X is a group.

Remarks: Composition of mappings is always associative, whether or not the mappings are injective or surjective.

If X is finite, then $|\Sigma_X| = |X|!$.

We write mappings on the left, so $\sigma \circ \tau(x) = \sigma(\tau(x))$.

1b. Isomorphism

Definition. *Let G and H be groups. An isomorphism from G to H is a mapping $\phi : G \to H$ such that*

1) $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in G$.

2) ϕ is a bijection.

We write $G \cong H$ if and only if there exists an isomorphism from G to H.

In 1), the products xy and $\phi(x)\phi(y)$ are in G and H, respectively.

The relation $\cong$ is then reflexive, symmetric and transitive on the class of all groups. Indeed one sees quickly from the definition of isomorphism that

1) For any G, $id_G : G \to G$ is an isomorphism;

2) If $\phi : G \to H$ is an isomorphism, then $\phi^{-1} : H \to G$ is an isomorphism; and

3) If $\phi : G \to H$ and $\psi : H \to K$ are isomorphisms, then $\psi \circ \phi : G \to K$ is an isomorphism.

and these facts imply respectively that $\cong$ is reflexive, symmetric and transitive. Consequently (ignoring set-theoretic difficulties) the class of all groups is partitioned into "isomorphism classes" or "isomorphism types".

As an example of isomorphisms, let X and Y be sets and suppose that there exists a bijection $f : X \to Y$. Define $\phi_f : \Sigma_X \to \Sigma_Y$ by $\phi_f(\sigma) = f \circ \sigma \circ f^{-1}$. Notice that the right side is a composite of bijections so is a bijection, and maps Y to Y. Then ϕ_f is an isomorphism. Indeed $\phi_f(\sigma\tau) = (f\sigma f^{-1})(f\tau f^{-1}) = f\sigma\tau f^{-1}$. Moreover, $\phi_f\phi_{f^{-1}} : \Sigma_Y \to \Sigma_X \to \Sigma_Y$ takes σ to $\phi_f(f^{-1}\sigma f^{-1^{-1}}) = ff^{-1}\sigma f^{-1^{-1}}f^{-1} = \sigma$, so $\phi_f\phi_{f^{-1}} = 1_{\Sigma_Y}$, and similarly $\phi_{f^{-1}}\phi_f = 1_{\Sigma_X}$. Hence ϕ_f is a bijection (with inverse $\phi_{f^{-1}}$).

Thus if X and Y are two sets of the same cardinality, then $\Sigma_X \cong \Sigma_Y$.

If $\phi : G \to H$ is an isomorphism, and $\phi(1_G) = h$, then $h^2 = \phi(1_G)\phi(1_G) = \phi(1_G^2) = \phi(1_G) = h$, so $h = 1_H$. Likewise for any $x \in G$, $\phi(x)\phi(x^{-1}) = \phi(xx^{-1}) = \phi(1_G) = 1_H$ and vice-versa, so $\phi(x^{-1}) = \phi(x)^{-1}$.

We shall consider isomorphic groups to be the "same", and group theory is the study of those properties of groups which are invariant under isomorphism.

We write Σ_n for $\Sigma_{\{1,2,\ldots,n\}}$.

1c. Rudiments

Note that 1_X is the only mapping such that $1_X\sigma = \sigma$ for all $\sigma \in \Sigma_X$, and f^{-1} is the unique inverse of f.

Proposition. *Let G be a group. Then*

1) 1_G is the only identity element of G; indeed it is the unique right identity element of G and the unique left identity element.

2) For each $x \in G$, x^{-1} is the unique inverse of x; indeed it is the unique right inverse and the unique left inverse.

3) If $g, h \in G$ then the equation $gx = h$ has a unique solution in G, namely $x = g^{-1}h$.

4) If $n \geq 3$ and $x_1, \ldots, x_n \in G$, then any two associations of $x_1 \ldots x_n$ represent the same element of G.

5) If $x, y \in G$ then $(xy)^{-1} = y^{-1}x^{-1}$ and $(x^{-1})^{-1} = x$.

Proof. 1) If e is a right identity then $1_G = 1_G e = e$, and similarly for left identity elements.

2) If y is a right inverse then $x^{-1} = x^{-1}1_G = x^{-1}(xy) = (x^{-1}x)y = 1_G y = y$. Similarly for left inverses.

3) Trivial

4) Induction on n, starting with $n = 3$, where it is the associative law. Show that the element represented by any association of $x_1 \dots x_n$ equals the element represented by the standard association $[x_1 \cdots x_n] = x_1(x_2(x_3(\cdots(x_{n-1}x_n)\cdots))$. Namely any association equals a product of associations of $x_1, \dots, x_k$ and $x_{k+1}, \dots, x_n$, so equals $[x_1 \cdots x_k][x_{k+1} \cdots x_n]$ by induction. This equals

$$(x_1[x_2 \cdots x_k])[x_{k+1} \cdots x_n] = x_1([x_2 \cdots x_k][x_{k+1} \cdots x_n]) = x_1[x_2 \cdots x_n] = [x_1 \cdots x_n],$$

the three steps by associativity, induction and definition, respectively.

5) $xy(y^{-1}x^{-1}) = (y^{-1}x^{-1})xy = 1$ and $xx^{-1} = x^{-1}x = 1$. QED

Ex. B. Let G be a group. A subset H of G which is itself a group with respect to the same operation is a subgroup of G. (Notation: $H \leq G$.)

For instance, if $G = \Sigma_X$ and $x \in X$, then $G_x = \{\sigma \in \Sigma_X \mid \sigma(x) = x$ is a subgroup of G. It is isomorphic to $\Sigma_{X-\{x\}}$, via the isomorphism $G_x \to \Sigma_{X-\{x\}}$ taking $\sigma \mapsto \sigma|X - \{x\}$.

Proposition. *If G is a group and $H \subseteq G$, then $H \leq G$ if and only if H is nonempty and closed under multiplication and inversion. In that case $1_H = 1_G$ and for $x \in H$, x^{-1} has the same meaning in both H and G.*

Proof. Left to reader. QED

Theorem. *(Cayley) Let G be a group. For each $g \in G$ let $\lambda_g \in \Sigma_G$ be defined by $\lambda_g(h) = gh$. Then $G^G = \{\lambda_g \mid g \in G\}$ is a subgroup of Σ_G and is isomorphic to G.*

Proof. Notice that $\lambda_{g'}(\lambda_g(h)) = \lambda_{g'}(gh) = g'(gh) = (g'g)h = \lambda_{g'g}(h)$. So

$$\lambda_{g'} \circ \lambda_g = \lambda_{g'g}.$$

Similarly,

$$\lambda_{1_G} = id_G, \text{ whence } \lambda_g\lambda_{g^{-1}} = \lambda_{gg^{-1}} = \lambda_{1_G} = id_G = \lambda_{g^{-1}}\lambda_g.$$

It follows that each λ_g is bijective with inverse $\lambda_{g^{-1}}$, so $\lambda_g \in \Sigma_G$. Closure, identity and inverse follow easily. Define $\lambda : G \to G^G$ by $\lambda(g) = \lambda_g$. The first displayed equation is the first condition for an isomorphism. λ is surjective by definition of G^G. And if $\lambda(g) = \lambda(g')$, then $g = \lambda_g(1_G) = \lambda_{g'}(1_G) = g'$, so λ is bijective and hence an isomorphism. QED

This is generally not very useful, except for philosophical reasons: groups are inherently groups of permutations, or can be viewed as such.

1d. More examples

Ex. C. Let X be a set "with structure". A mapping $\sigma \in \Sigma_X$ is an automorphism of X if and only if it "preserves" the structure. $\mathrm{Aut}(X)$ is the set of all automorphisms of X. Then $\mathrm{Aut}(X)$ is a group, indeed a subgroup of Σ_X.

Ex. C′. Let G be a group. An automorphism of G is an isomorphism from G to G. Then $\mathrm{Aut}(G)$, the set of automorphisms of G under composition, is a group. (Check this. Need the inverse of an automorphism is an automorphism.)

Ex. C″. Let R be Rubik's cube; more precisely the set $\{s_1, \ldots, s_{54}\}$ of all 54 positions which can be held by a colored square on the surface of the cube. Let $G(R)$ be the set of all $\sigma \in \Sigma_{54}$ such that by legitimate moves one may transform a given configuration to a new one in which the square at position i has been moved to position $\sigma(i)$, $i = 1, \ldots, 54$. Then $G(R)$ is a group. (It has order $2^{10}3^7 \cdot 8! \cdot 12!$, if memory serves.)

Ex. D. Let n be an integer and $G = GL_n(\mathbf{C})$ the set of $n \times n$ nonsingular matrices over $\mathbf{C}$, the complex field. Then G is a group (under matrix multiplication). A subgroup is $SL_n(\mathbf{C}) = \{g \in GL_n(\mathbf{C}) \mid \det g = 1\}$.

The field $\mathbf{C}$ can be replaced by $\mathbf{R}$ or any commutative ring here. Also Cayley's theorem has an analogue here: any finite group G is isomorphic to a subgroup of $GL_{|G|}(\mathbf{C})$ (consisting of the permutation matrices, rows and columns indexed by G, corresponding to the permutations λ_g, $g \in G$.

Ex. D′. An example similar to, but different from, $GL_2(\mathbf{C})$ is the group of fractional linear transformations of the complex plane, that is, the group $LF(2, \mathbf{C})$ of all permutations σ of the extended complex plane (Riemann sphere) $\mathbf{C} \cup \{\infty\}$ of the form

$$\sigma(z) = \frac{az + b}{cz + d}$$

such that a, b, c, d are complex constants for which $ad - bc \neq 0$. This last condition prevents σ from being a constant mapping, so is actually redundant. We may write $\sigma = \sigma_A$, where A is the "matrix of coefficients"

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

It is then easy to check that

$$LF(2, \mathbf{C}) = \{\sigma_A \mid A \in GL_2(\mathbf{C})\}, \text{ and } \sigma_A \sigma_B = \sigma_{AB} \forall A, B \in GL_2(\mathbf{C}).$$

However, the mapping

$$\phi : GL_2(\mathbf{C}) \to LF(2, \mathbf{C}) \text{ defined by } \phi(A) = \sigma_A,$$

is not an isomorphism, because it fails to be injective. In fact $\sigma_{cA} = \sigma_A$ for every A and for every $c \in \mathbf{C}^\times$.

Exercise. *Show that for any $A, B \in GL_2(\mathbf{C})$, we have $\sigma_A = \sigma_B$ if and only if $B = cA$ for some $c \in \mathbf{C}^\times$.*

1e. Powers; cyclic groups

Ex. E. Let G be any group and $g \in G$. Define g^n for $n \in \mathbf{Z}$ as follows: $g^0 = 1_G$ and $g^{n+1} = g^n g$ for $n \geq 0$; $g^n = (g^{-n})^{-1}$ for $n < 0$.

Proposition. *Let $g \in G$ and $m, n \in \mathbf{Z}$. Then $g^m g^n = g^{m+n}$, and $(g^m)^{-1} = g^{-m}$. Moreover $(g^m)^n = g^{mn}$.*

This is a consequence of 4) of the Proposition above, when m and n have the same sign; otherwise, there are several cases, e.g. if $n \geq |m|$ with $m < 0$, then $g^n = g^{-m} g^{m+n}$, so $g^m g^n = g^m g^{-m} g^{m+n} = g^{m+n}$. The remaining assertions are left to the reader to prove.

The set $\{g^n \,|\, n \in \mathbf{Z}\}$ is a subgroup of G, and is denoted by $\langle g \rangle$. A group arising in this way–as the powers of a single element–is called cyclic, and g is called a generator.

Examples of cyclic groups: $\mathbf{Z}$, the set of integers, with respect to addition. 1 is a generator, $0 = 1_{\mathbf{Z}}$, and usually one writes $g + h$ for gh and $-g$ for g^{-1}. Also $\mathbf{Z}_n$, the integers mod n (here n is a positive integer), with elements $[i]$, $i \in \mathbf{Z}$, and $[i] = [j]$ if and only if $i \equiv j \bmod n$; $[i] + [j] = [i + j]$. A generator is $[1]$.

Proposition. *Every cyclic group G is isomorphic to exactly one of the groups $\mathbf{Z}$, $\mathbf{Z}_n$, $n = 1, 2, \ldots$. Moreover if $G = \langle g \rangle$, then there is a unique isomorphism $\mathbf{Z} \to G$ or $\mathbf{Z}_n \to G$, as the case may be, taking $1 \mapsto g$ or $[1] \mapsto g$.*

Proof. If $g^n \neq 1$ for all $n \neq 0$, then the elements g^n, $n \in \mathbf{Z}$ are all different (for $g^n = g^m$ would imply $g^{n-m} = g^n (g^n)^{-1} = 1$ and hence $n - m = 0$). Map $\mathbf{Z} \to G$ by $n \mapsto g^n$. This is clearly injective, surjective, and multiplicative.

If $g^n = 1$ for some $n \neq 0$, then $g^{-n} = (g^n)^{-1} = 1$, so we may take $n > 0$. We may also assume that n is the smallest positive integer such that $g^n = 1$. Then the elements g^i, $0 \leq i < n$, are all distinct, by a similar argument, and $g^i = g^j \iff i \equiv j \bmod n$. The mapping $\mathbf{Z}_n \to G$ taking $[m] \mapsto g^m$, $0 \leq m < n$ is then well-defined and bijective, and $g^m g^{m'} = g^{m+m'}$, providing the isomorphism.

The uniqueness of the isomorphism is clear since if 1 or $[1]$ maps to g, then $m = 1 + \cdots + 1$ or $[m] = [1] + \cdots + [1]$ maps to $g \cdots g = g^m$ by repeated use of the multiplicativity of the isomorphism. QED

Exercise. *The distinct subgroups of $\mathbf{Z}$ are the subgroups $\langle n \rangle$, $n > 0$. The distinct subgroups of $\mathbf{Z}_n$ are the subgroups $\langle [m] \rangle$, $m > 0$, m dividing n. Consequently every subgroup of a cyclic group is cyclic; and a cyclic group of order n has a subgroup of order m if and only if m divides n.*

As a corollary we can define the order of an element.

Definition. *Let G be a group and $g \in G$. The order of g is $|g| = |\langle g \rangle|$, the cardinality of $\langle g \rangle$.*

Thus the order of g is a positive integer or ∞. In a finite group, every element has finite order.

Exercise. *If $g \in G$ and $g^n = 1$ for some integer $n \neq 0$, then the order of g is finite and divides n.*

1f. Generation

Ex. F. For this example we need a lemma.

Lemma. *The intersection of any collection of subgroups of a group G is a subgroup of G.*

Proof. *Left to reader.* QED

Definition. *Let G be a group and S any subset of G. The intersection of all subgroups of G containing S (G is one of them) is a subgroup of G called $\langle S\rangle$, the subgroup of G generated by S.*

Proposition. $\langle S\rangle = \{s_1^{\epsilon_1}s_2^{\epsilon_2}\cdots s_n^{\epsilon_n} \mid n \geq 0,\ s_i \in S \text{ and } \epsilon_i = \pm 1\ \forall i\}$.

The expressions on the right are called "words in $S \cup S^{-1}$". Here if $n = 0$, the empty product is interpreted as 1_G.

Proof. Since $(xy)^{-1} = y^{-1}x^{-1}$ and $(x^{-1})^{-1} = x$, the right side H is obviously a subgroup of G, and $S \subseteq H$ via words of length 1. Therefore $\langle S\rangle \leq H$. On the other hand $\langle S\rangle$ contains each $s^{\pm 1}$, $s \in S$, and hence contains all the elements of H, as it is closed under inversion and products. QED

Though the situation is nice for cyclic groups, those generated by one element, it quickly becomes intractable for groups generated by two or more elements.

Exercise. *Σ_n is generated by two elements.*

Hint: Every permutation is the composition of "transpositions", i.e., interchanges of pairs of objects. The transposition (12) and the cycle $(12\cdots n)$ generate a subgroup containing all transpositions and hence generate Σ_n.

Furthermore, it can be shown that $\lim_{n\to\infty} P(\langle x, y\rangle = \Sigma_n) = 1$, for x and y chosen (uniformly) randomly and independently in Σ_n.

Another example of this is

$$SL_2(\mathbf{Z}) = \left\langle \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} \right\rangle.$$

Taking matters to larger extremes, Burnside proposed the following problem a hundred years ago.

Let m and n be positive integers. Let G be a group such that $g^n = 1$ for all $g \in G$, and $G = \langle S\rangle$ for some set of cardinality m. Is G necessarily finite?

The answer turns out to be "no" in general, although for some very small values of n, it is "yes". Of course it is "yes" for $m = 1$. It is not known for $(m, n) = (2, 5)$.

1g. Abelian groups

Ex. G. However, the situation is better controlled for abelian groups, those which satisfy the commutative law.

Definition. *A group G is commutative (or abelian) if and only if $xy = yx$ for all $x, y \in G$.*

Exercise. *If G is abelian then $(xy)^m = x^m y^m$ for all $x, y \in G$ and $m \in \mathbf{Z}$. Moreover if G is abelian and generated by elements $x_1, \ldots, x_r$ and $x_i^n = 1$ for all i, then G is finite and its cardinality is at most n^r.*

Examples of abelian groups are cyclic groups, the additive group of the rationals, reals, complexes (or any field), the multiplicative group of nonzero rationals, reals, complexes (or any field), the multiplicative group of all roots of unity in $\mathbf{C}$ (or in any field), and the matrix group

$$U = \left\{ \begin{bmatrix} 1 & c \\ 0 & 1 \end{bmatrix} \;\middle|\; c \in \mathbf{C} \right\}.$$

Exercise. *If G is an abelian group, then any subgroup of G is abelian.*

Definition. *A periodic group (torsion group) is one all of whose elements have finite order. The exponent of a torsion group is the least common multiple of the orders of its elements (or ∞, if there is no such common multiple). The exponent of a non-torsion group is ∞.*

Exercise. *Suppose that $G = \langle S \rangle$. If G is abelian, then the exponent of G is the least common multiple of the orders of the elements of S.*

Exercise. *A group of exponent 2 is necessarily abelian. There exist nonabelian groups of exponent 3.*

1h. Dihedral groups

Ex. H. Let $n > 2$ be an integer and let D_{2n} be the group of symmetries of the regular n-gon. Thus D_{2n} contains rotations through integer multiples of $2\pi/n$, which form a cyclic subgroup of cardinality n, generated by rotation σ through $2\pi/n$. In addition there are the reflections about an axis of symmetry; there are n of these as well. Notice that if τ is one such reflection, then $\sigma^i \tau$ is also a reflection. There are no other symmetries, so $D_{2n} = \{\sigma^1, \sigma^2, \ldots, \sigma^n, \sigma^1\tau, \ldots, \sigma^n\tau\} = \{\sigma^i \tau^j \,|\, 0 \le i < n,\ 0 \le j \le 1\}$. The multiplication is determined by the following rules:

$$\sigma^n = 1,\ \tau^2 = 1,\ \tau\sigma\tau = \sigma^{-1}.$$

For then

$$\sigma^i \tau^j \sigma^k \tau^\ell = \begin{cases} \sigma^{i+k}\tau^\ell & \text{if } j = 0 \\ \sigma^{i-k}\tau^{1+\ell} & \text{if } j = 1 \end{cases}$$

Notice however that $D_{2n} = \langle \tau, \sigma\tau \rangle$, and both of these elements have order 2.

1i. Direct products

Ex. I. Let G and H be groups. The (external) **direct product** $G \times H$ is the group based on the set which is the Cartesian product $\{(g,h) \,|\, g \in G,\ h \in H\}$ and with multiplication $(g,h)(g',h') = (gg', hh')$. Then $G \times H$ has subgroups $G_1 = \{(g,1) \,|\, g \in G\}$ isomorphic to G and $H_1 = \{(1,h) \,|\, h \in H\}$ isomorphic to H, every element of G is the product of an element of G_1 and one of H_1, and $g_1 h_1 = h_1 g_1$ for all $g_1 \in G_1$, $h_1 \in H_1$. But any nonabelianness of G and H is preserved.

Indeed if $\{G_i \,|\, i \in I\}$ is a family of groups indexed by the set I, then $\prod_{i \in I} G_i$ is the set of all functions $f : I \to \cup G_i$ such that $f(i) \in G_i$ for all i; multiplication is pointwise: $(ff')(i) = f(i)f'(i)$. Within this is the restricted direct product, the subgroup consisting of all elements f such that $f(i) = 1_{G_i}$ for all but finitely many $i \in I$.

We shall see that every finite (or even finitely generated) abelian group is isomorphic to the direct product of finitely many cyclic groups. But nothing like this is true for infinitely generated groups or for finite nonabelian groups.

Ex. J. Let $G = \Sigma_X$ and let Y be a subset of X, $\emptyset \neq Y \neq X$. Let $G_{[Y]} = \{\sigma \in G \,|\, \sigma(Y) = Y\}$. Then $G_{[Y]} \leq G$. Moreover, the mapping

$$G_{[Y]} \cong \Sigma_Y \times \Sigma_{X-Y}$$

via the isomorphism $\sigma \mapsto (\sigma|Y, \sigma|(X-Y))$. Checking this is a matter of checking that a) composition of mappings is preserved upon restriction to a subset (left invariant by the mappings in question); b) every permutation of X leaving Y invariant is made up of a permutation of Y and one of $X - Y$, and every such pair conversely together form a permutation of X.