Algebraic Structures 1 - Tirgul 1

Yonatan Harpaz

October 14, 2010

Let us start this TA session by recalling the definition of the most fundamental object of study in this course:

Definition 0.1. A **group** is set G together with a binary operation $(a, b) \longrightarrow a \cdot b \in G$ (called the multiplication) satisfying the following axioms:

1. **Associativity**: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
2. **Neutral element**: There exists an element $e \in G$ such that
$$a \cdot e = e \cdot a = a$$
3. **Inverse elements**: For every $g \in G$ there exists an element g^{-1} (called its **inverse**) satisfying
$$g \cdot g^{-1} = g^{-1} \cdot g = e$$

Examples:

1. The integers $\mathbb{Z}$ are a group with respect to addition of numbers. They do not form a group with respect to multiplication of numbers, because many elements don't have inverses with respect to multiplication.
2. For every n the set $\{0, ..., n-1\}$ is a group with respect to addition modulu n (i.e. the operation is to take two numbers, add them, and then take the residue of dividing in n). This group is denoted by $\mathbb{Z}/n$ or sometimes $\mathbb{Z}_n$.
3. Let F be a field. Then F is a group with respect to addition and $F \setminus \{0\}$ is a group with respect to multiplication. The latter group is also denoted by F^*.
4. Every vector space V is a group with respect to addition of vectors (in fact the axioms above should be familiar to the reader from the definition of vectors spaces when replacing the $\cdot$ symbol with $+$).

   Recall that addition of vector spaces satisfies one further axiom which states that $a + b = b + a$. A group in which the multiplication satisfies this property is called **abelian** or **commutative**.

5. For every set A we denote by $S(A)$ or perm(A) the set of one-to-one onto maps from A to itself (called **permutations** of A). When A is the set $\{1, ..., n\}$ we also write S_n for $S(A)$. $S(A)$ forms a group with respect to composition of permutation. The neutral element is the identity permutation. If $\sigma \in S(A)$ is a permutation then σ^{-1} is its inverse as a map (which exists because τ is one-to-one and onto).

6. Let F be a field and V a vector space over F. We denote by GL(V) the set of invertible linear maps from V to V. These form a group under composition and as in the previous example the neutral element is the identity map. When $V = F^n$ we can identify GL(V) with the set of invertible $n \times n$ matrices over F. In this case we denote $GL(V)$ by $GL_n(F)$.

7. The post stamp machine group (see demonstration in class).

Note that in the last three examples the group was the collection of maps from a set to itself which preserved some structure. These are sometimes referred to as **symmetries** of the structure (for examples, the symmetries of a vector space are its invertible self maps which preserve its vector space structure - i.e. linear maps). Many of the groups you will encounter in real life will arise as symmetries of certain structures. This is one of the reasons groups are so important in mathematics.

1 Permutations

Let us return now to the example of the permutation group. This is a rather important example is worth some explicit handling. Let us start with notation. The most straight forward to write a permutation τ is by specifying for every $i \in \{1, ..., n\}$ what is $\tau(i)$. This can be done, for example, by writing the values $\sigma(1), ..., \sigma(n)$ in a line underneath a line of $1, ..., n$. For example if $\tau \in S_3$ is the permutation defined by $\tau(1) = 2, \tau(2) = 1$ and $\tau(3) = 3$ we will write it as

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

This notation is a bit cumbersome and it is rather hard to get an "overall" picture of the permutation. For example, the permutation

$$\sigma_0 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 4 & 2 \end{pmatrix}$$

can be described in a more human language as "switch 3 with 1 and 5 with 2". This example generalizes to the observation that we can break a permutation in **cycles**. Suppose that $\sigma \in S_n$ is a permutation and $a_0 \in \{1, ..., n\}$ is any element. Start applying σ iteratively to a_0 until we end up with a_0 again. You will end up with a sequence $a_0, ..., a_k$ such that $a_i = \sigma(a_{i-1})$ and $a_0 = \sigma(a_k)$. This is called the **cycle** of σ starting with a_0 and is usually denoted by $(a_0 \ a_1 \ ... \ a_k)$.

For example in the permutation σ_0 the cycle of 1 is $(1\ \ 3)$ and the cycle of 4 is just (4).

The notational idea is to use the cycle $(a_0\ \ a_1\ \ ...\ \ a_k)$ in order to **denote** the permutation satisfying $\sigma(a_i) = a_{i+1}$, $\sigma(a_k) = a_0$ and $\sigma(x) = x$ for $x \notin \{a_0, ..., a_k\}$. By abuse of notation we call such a permutation a **cycle**.

Now every permutation can be written as a product of cycles. In order to see this do the following: given a permutation σ begin by taking some element of $\{1, ..., n\}$ (for example 1) and constructing its cycle. If this cycle includes all the elements in $\{1, ..., n\}$ then σ is itself a cycle. If not take some element not in the cycle and construct its cycle. Continue in this way until no more elements of $\{1, ..., n\}$ are left. The product of the resulting cycles forms σ. Note that the resulting cycles are pairwise disjoint.

For example the permutation σ_0 can be written as the product

$$\sigma_0 = (1\ \ 3) \cdot (2\ \ 5)$$

We will usually omit the $\cdot$ sign and just write

$$\sigma_0 = (1\ \ 3)(2\ \ 5)$$

2 Homomorphisms

When studying algebraic objects such as fields, vector spaces or groups, the maps between them are just as important as the objects them selves. We want to consider maps between groups which preserve the group structure. Fortunately this comes down to a very simple property (note the similarity to the definition of linear maps in linear algebra. It is not accidental):

Definition 2.1. A map $\varphi : G \longrightarrow H$ is called a **homomorphism** if for every $a, b \in G$ one has

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$$

where the first multiplication is the multiplication in G and the second is the multiplication in H.

Examples:

1. For every n the map $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}/n$ given by $\varphi(x) = x \mod n$ is a homomorphism.
2. The map $\varphi : (\mathbb{R}, +) \longrightarrow (\mathbb{R}^*, \cdot)$ given by

   $$\varphi(x) = e^x$$

   is a homomorphism.
3. Let F be a field and recall the group $GL_n(F)$ discussed above. Then the determinant map $\det : GL_n(F) \longrightarrow F^*$ is a homomorphism (the identity $\det(A)\det(B) = \det(A) \cdot \det(B)$ is proven in linear algebra 1).

4. Let F be a field. Consider the map $\varphi : S_n \longrightarrow \mathrm{GL}_n(F)$ which associates to σ the matrix A^σ defined by

$$A^\sigma_{i,j} = \begin{cases} 1 & i = \sigma(j) \\ 0 & i \neq \sigma(j) \end{cases}$$

We will show that it is a homomorphism. Let $\sigma, \tau \in S_n$ be permutations. Calculating explicitly we get:

$$(A^\sigma A^\tau)_{i,j} = \sum_{k=1}^{n} A^\sigma_{i,k} A^\tau_{k,j}$$

Now the summand $A^\sigma_{i,k} A^\tau_{k,j}$ is non-zero if and only if $i = \sigma(k)$ and $k = \tau(j)$. Note that such a k exists if and only if $i = \sigma(\tau(i)) = (\sigma \cdot \tau)(i)$, in which case it is unique. Hence we get that

$$(A^\sigma A^\tau)_{i,j} = \begin{cases} 1 & i = (\sigma \cdot \tau)(i) \\ 0 & i \neq (\sigma \cdot \tau)(i) \end{cases}$$

which is equal to $A^{\sigma \cdot \tau}$ by definition.

5. Recall the notion of a sign of a permutation: given $\sigma \in S_n$ we define

$$\mathrm{sign}(\sigma) = \prod_{i<j} \frac{j-i}{\sigma(j) - \sigma(i)}$$

Note that this expression always gives either 1 or -1. Indeed if one considers the absolute value

$$|\,\mathrm{sign}(\sigma)| = \prod_{i<j} \frac{|j-i|}{|\sigma(j) - \sigma(i)|}$$

then for each $i < j$ the term $|j - i|$ appears exactly once in the nominator and exactly once in the denominator. Hence $|\,\mathrm{sign}(\sigma)| = 1$ and $\mathrm{sign}(\sigma) = \pm 1$.

We want to show that the sign map is a homomorphism from S_n to the group $\{1, -1\}$ (with multiplication of numbers as operation). In order to do this we recall that if A is a matrix then

$$\det(A) = \sum_{\sigma \in S_n} \mathrm{sign}(\sigma) \prod_{j=1}^{n} A_{\sigma(j),j}$$

Hence if we take a matrix of the form A^σ as above we get that

$$\det(A^\sigma) = \mathrm{sign}(\sigma)$$

Hence the sign map can be viewed as a composition of the homomorphism $\sigma \mapsto A^\sigma$ with the homomorphism det.

A composition of two homomorphisms is in fact always a homomorphism: if G, H, K are three groups and $\varphi : G \longrightarrow H, \psi : H \longrightarrow K$ homomorphism then $\psi \circ \varphi$ is a homomorphism as well. Indeed:

$$\psi(\varphi(a \cdot b)) = \psi(\varphi(a) \cdot \varphi(b)) = \psi(\varphi(a)) \cdot \psi(\varphi(b))$$

Algebraic Structures 1 - Tirgul 2

Yonatan Harpaz

October 22, 2010

1 The Cayley Graph

It is sometimes worthwhile to use combinatoric and geometric tools in order to study groups. In this section we will introduce one such basic tool - the Cayley graph. First let us recall what a graph is.

Definition 1.1. A (directed) **graph** is an ordered pair (V, E) where V is a set (whose elements are called **vertices**) and $E \subseteq V \times V$ is a set of ordered pairs of elements of V (referred to as **edges**).

Graphs are used to model many real life structures, such as computer networks, etc. Here we will see that we can also use them to describe groups. Let G be a group and $S \subseteq G$ a subset of elements. We define the **Cayley graph** $C_{G,S}$ of G with respect to S to be the graph whose vertex set is G and whose edge set is the set of all pairs $(g, h) \in G \times G$ such that $hg^{-1} \in S$. The set S us usually taken to be a generator set of G.

Examples (see drawings in class):

1. The Cayley graph of $(\mathbb{Z}, +)$ with respect to $\{1\}$ is an infinite chain. The Cayley graph of the finite cyclic group of order n is a cycle of length n. Draw for yourself the Cayley graph of $\mathbb{Z}^2$ with respect to the sets $\{(0, 1)\}$ and $\{(0, 1), (1, 0)\}$.

2. The Cayley graph of D_4 (the dihedral group, or the post stamp machine group) with respect to the generator set $\{\sigma, \tau\}$ (where τ is 90 degrees rotation and σ is one of the reflections) looks like the the vertices and edges of a 3-dimensional cube.

The question of whether S generates G is reflected in a very natural property of its Cayey graph:

Definition 1.2. Let (V, E) be a directed graph. We say that V is **connected** if for every two vertices $v, u \in V$ there exists a sequence

$$v = v_0, v_1, ..., v_n = u$$

such that for each $i = 1, ..., n$ either $(v_{i-1}, v_i) \in E$ or $(v_i, v_{i-1}) \in E$. Such a sequence is called an (undirected) **path** from v to u.

In human terms this means that one can get from each vertex to each other vertex.

Proposition 1.3. *Let G be a group and $S \subseteq G$ a subset of elements. Let C be the Cayley graph $C_{G,S}$ is connected if and only if S generates G.*

Proof. Assume first that S generates G and let $g, h \in G$ be two elements. We need to construct a sequence

$$g = g_0, g_1, ..., g_n = h$$

such that $g_i g_{i-1}^{-1} \in S$ or $g_{i-1} g_i^{-1} \in S$ for every $i = 1, ..., n$. Consider the element $hg^{-1} \in G$. Since S generates G there exist elements $s_1, ..., s_n$ such that

$$hg^{-1} = s_n^{\varepsilon_n} s_{n-1}^{\varepsilon_{n-1}} ... s_1^{\varepsilon_1}$$

where $\varepsilon_i \in \{1, -1\}$. Now define a sequence $g_0, ..., g_n$ by setting

$$g_k = s_k^{\varepsilon_k} s_{k-1}^{\varepsilon_{k-1}} ... s_1^{\varepsilon_1} g$$

By definition we get

$$g_n = s_n^{\varepsilon_n} s_{n-1}^{\varepsilon_{n-1}} ... s_1^{\varepsilon_1} g = h$$

Clearly $g_i = s_i^{\varepsilon_i} g_{i-1}$ and so

$$g_i g_{i-1}^{-1} = s_i^{\varepsilon_i}$$

Note that if $\varepsilon_i = 1$ then $g_i g_{i-1} \in S$ and if $\varepsilon = -1$ then $g_{i-1} g_i^{-1} \in S$. Hence we've constructed a path from g to h.

To prove the other direction we assume that $C_{G,S}$ is connected. Let $g \in G$ be an element. We wish to show that it is a product of elements in S. Since $C_{G,S}$ is connected there is a path from the neutral element $e \in G$ to g, i.e. there exists a sequence of elements

$$e = g_0, g_1, ..., g_n = g$$

with $g_i g_{i-1} \in S$ or $g_i g_{i-1}^{-1} \in S$ for every $i = 1, ..., n$, i.e. there exists a sequence of s_i's and $\varepsilon_i \in \{-1, 1\}$ such that $g_i = s_i^{\varepsilon_i} g_{i-1}$. By induction one gets that

$$g_k = s_k^{\varepsilon_k} s_{k-1}^{\varepsilon_{k-1}} ... s_1^{\varepsilon_1}$$

for $k = 1, ..., n$ and in particular

$$g = g_n = s_n^{\varepsilon_n} s_{n-1}^{\varepsilon_{n-1}} ... s_1^{\varepsilon_1}$$

This means that g is generated by S and we are done. □

2 Subgroups of Cyclic Groups

Theorem 2.1. *Let G be a cyclic group. Then every subgroup of G is cyclic.*

Proof. Let $H \subseteq G$ be a subgroup. If $H = \{e\}$ then it is trivially cyclic and we are done. If $H \neq \{e\}$ them there exists a minimal $k > 0$ such that $g^k \in H$. We claim that H must be generated by g^k. Assume otherwise: then there exists an element $h \in H$ such that $h \neq (g^k)^i = g^{ik}$ for every $i \in \mathbb{Z}$. Since G itself is cyclic there exists some j such that $h = g^j$. This j has to satisfy that $j \neq ik$ for every i, i.e. it is not divisible by k.

Let $r \in \{0, ..., k-1\}$ be the remainder in the division of j by k. There there exists an $i \in \mathbb{Z}$ such that $r = j + ik$. Since j is not divisible by k we get that $r \neq 0$. But

$$g^r = g^{j+ik} = g^j(g^{ik}) = h(g^k)^i \in H$$

which contradicts the minimality of k. □

Corollary 2.2. *Let G be a finite cyclic group of order n. Then G has exactly one subgroup of order d for each $d|n$.*

Proof. Let g be a generator of G. For each $d|n$ let $r = \frac{n}{d}$ and consider the subgroup $H_d \subseteq G$ generated by g^r. Clearly d is the smallest positive number such that $(g^r)^d = e$ and so d is the order of g^r. This means that $|H_d| = d$. We need to show that these are all the subgroups.

Consider the homomorphism $\mathbb{Z} \longrightarrow G$ sending $m \in \mathbb{Z}$ to $g^m \in G$. Let $H \subseteq G$ be any subgroup. From Theorem 2.1 there exists a k such that $H = \langle g^k \rangle$. Consider the subset

$$M = \{m \in \mathbb{Z} | g^m \in H\} =\subseteq \mathbb{Z}$$

Clearly M contains 0 and is closed under addition and negation. Hence it is a subgroup of $\mathbb{Z}$. Since $\mathbb{Z}$ is cyclic we get from Theorem 2.1 that there exists an $r \in \mathbb{Z}$ such that

$$M =< r >= \{ar | a \in \mathbb{Z}\}$$

and we can always take r to be positive. Note $n \in M$ and so r must also divide n. Hence there exists a positive $d|n$ such that $r = \frac{n}{d}$.

Since the homomorphism $m \mapsto g^m$ is surjective we get that

$$H = \{g^m | m \in M\} = \{g^{ar} | a \in \mathbb{Z}\} = \langle g^r \rangle = H_d$$

and we are done.

□

3 The Group $SL_2(\mathbb{Z})$

For the rest of the TA session we will play with the group $\mathrm{SL}_2(\mathbb{Z})$, which is a very interesting group. Recall that $\mathrm{SL}_2(\mathbb{Z})$ is the group of 2×2 matrices with coefficients in $\mathbb{Z}$ and the multiplication is the usual matrix multiplication.

Note that if $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is a matrix with determinant 1 then its inverse is given by $\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ (check to verify!).

This group is infinite and not-abelian. However it is finitely generated, and in fact has a generator set of size 2. This is the content of the following theorem:

Theorem 3.1. *The group $SL_2(\mathbb{Z})$ is generated by the elements*

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

$$B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

Proof. Let $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ be any element. We will perform a process which is analogous to Euclid's algorithm for finding a greatest common denominator. This algorithm takes a pair of numbers (a, c) and alternates between two steps: if $|c|$ is bigger then $|a|$ then it **switches** a and c and if $0 < |c| \leq |a|$ it replaces a with the remainder of the division of a with c. The algorithm stops when c equals 0.

We will perform something similar to the left column of M. Formally we will do the following: define a sequence of matrices $M_0, ..., M_k \in \mathrm{SL}_2(\mathbb{Z})$ recursively as follows: set $M_0 = M$ and if

$$M_i = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

define M_{i+1} according to the following rules:

1. (move 1) If $|c_i| > |a_i|$ set $M_{i+1} = BM_i$.
2. (move 2) If $0 < |c_i| \leq |a_i|$ find the remainder r of the division of a_i by c_i. Then $r = a_i + kc_i$ for some $k \in \mathbb{Z}$ and $|r| < |c_i|$. Set $M_{i+1} = A^k M_i$.
3. If $c_i = 0$ stop.

Observe that if $|c_i| > |a_i|$ then $|c_{i+1}| < |a_{i+1}|$ and if $0 < |c_i| \leq |a_i|$ then $|c_{i+1}| > |a_{i+1}|$. Hence until the process stops we alternate between move 1 and move 2. Note that move 1 strictly decreases c_i and move 2 doesn't change it. Hence c_i must arrive at 0 after a finite number of steps. The final step is a matrix of the form

$$M_k = \begin{pmatrix} a_k & b_k \\ 0 & d_k \end{pmatrix}$$

Note that if M_k is a generated by $\{A, B\}$ then so is M, so it is enough to prove for M_k. Now the determinant of this matrix is $a_k d_k$ and since it has to equal 1 we see that $a_k = d_k = \pm 1$. Now it is enough to observe that if $a_k = d_k = 1$ then

$$M_k = A^{b_k}$$

and if $a_k = d_k = -1$ then

$$M_k = B^2 A^{-b_k}$$

□

Algebraic Structures 1 - Tirgul 4

Yonatan Harpaz

November 9, 2010

1 The Diameter of S_n

Recall that you saw in exercise 2 that the pair $\tau = (1\ \ 2), \sigma = (1\ \ 2\ \ ...\ \ n)$ generates S_n. Recall that this corresponded to the fact that the Cayley graph of S_n with respect to $S = \{\tau, \sigma\}$ is connected. This means that one can get from every vertex of the graph to any other vertex though an undirected path. We define the length of an undirected path to be the number of edges in it. It is then natural to define the **distance** $d(v, u)$ between two vertices to be the minimal length of an undirected path connecting them.

Definition 1.1. Let V, E be a connected graph. We define the **diameter** of V to be the supremum of all distances:

$$\mathrm{diam}(V) = \sup_{v,u} d(v, u)$$

Note that the diameter of a graph might be ∞. However if V is finite then $\mathrm{diam}(V)$ has to be finite as well. Now given a group G and a generator set S one can wonder as to the diameter of the Cayley graph $C_{G,S}$. Note that the distance between two vertices $g, h \in G$ on the Cayley graph of G is the minimal number k such that

$$hg^{-1} = \prod_{i=1}^{k} s_i^{\varepsilon_i}$$

for some $s_i \in S, \varepsilon_i \in \{-1, 1\}$. In particular one sees that the diameter of a Cayley graph coincides with the minimal distance between a vertex g and the vertex e. We will be interested in the diameter d_n of S_n with respect to $\{\sigma, \tau\}$.

Theorem 1.2.

$$d_n = \Theta(n^2)$$

Proof. We need to prove that there are constants $C_1, C_2 > 0$ such that for large enough n

$$C_1 n^2 \leq d_n \leq C_2 n^2$$

Let us start with the upper bound. For this we will show the following two facts:

1. Every permutation can be written as a product of at most $n-1$ swaps.

   Proof. It is enough to show that a cycle of size k is a product of $k-1$ swaps. But this is clear because

   $$(a_1 \;\; a_2 \;\; \ldots \;\; a_k) = (a_1 \;\; a_2)(a_2 \;\; a_3)\cdots(a_{k-1} \;\; a_k)$$

   □

2. The distance between a swap $(i \;\; j)$ and the identity e is at most $8n$.

   Proof. First observe that

   $$\sigma^{i-1}\tau\sigma^{-(i-1)} = (i \;\; i+1)$$

   which means that

   $$(i \;\; i+1 \;\; \ldots \;\; j) = (i \;\; i+1)(i+1 \;\; i+2)\cdots(j-1 \;\; j) =$$

   $$\sigma^{i-1}\tau\sigma^{-(i-1)}\sigma^{i}\tau\sigma^{-i}\cdots\sigma^{j-2}\tau\sigma^{-(j-2)} = \sigma^{i-1}(\tau\sigma)^{j-i}\sigma^{-(j-2)}$$

   and so the distance between $(i \;\; i+1 \;\; \ldots \;\; j)$ end e is at most

   $$(i-1) + 2(j-i) + (j-2) \leq 4n$$

   Now since

   $$(i \;\; j) = (i \;\; i+1 \;\; \ldots \;\; j)(i \;\; i+1 \;\; \ldots \;\; j-1)^{-1}$$

   we see that the distance between $(i \;\; j)$ and e is at most $8n$. □

Now from these two facts we see that the distance between any permutation and e is at most $(n-1)8n \leq 8n^2$ so we can choose $C_2 = 8$.

We now need to show that d_n is eventually at least a multiple of n^2. For this consider the following concept: we will call a trio i, j, k with $i < j < k$ **good** with respect to a permutation $\varphi \in S_n$ if either $\varphi(i) < \varphi(j) < \varphi(k)$, $\varphi(j) < \varphi(k) < \varphi(i)$ or $\varphi(k) < \varphi(i) < \varphi(j)$. For example if $\varphi = (1 \;\; 2 \;\; 3)(4 \;\; 5)$ then the trio $1, 2, 3$ is good but the trio $3, 4, 5$ is bad.

Now for each permutation φ let $c(\varphi)$ denote the number of good trios of φ. Now the key observation is that $c(\sigma\varphi) = c(\varphi)$ (in fact, composing with σ does not change the set of good trios) and that $c(\tau\varphi)$ is at most $c(\varphi) + n - 2$. The reason here is because composing with τ can only change the goodness of trios of the form i, j, k such that $1, 2 \in \{\varphi(i), \varphi(j), \varphi(k)\}$ (why?) and there are exactly $n-2$ such ordered trios. This gives us the inequality

$$c(\varphi) \leq d(\varphi, e)(n-2)$$

Now consider the permutation ω defined by $\omega(i) = n+1-i$. Then for every $i < j < k$ we have

$$\varphi(k) < \varphi(j) < \varphi(i)$$

and so all the trios are bad. Hence we get that

$$c(\omega) = \binom{n}{3} = \frac{n(n-1)(n-2)}{6}$$

This means that

$$d(\omega, e) \geq \frac{n(n-1)(n-2)}{6(n-2)} = \frac{n(n-1)}{6}$$

and so

$$d_n \geq \frac{n(n-1)}{6}$$

note that for when $n \geq 2$ we have

$$\frac{n-1}{6} \geq \frac{n}{12}$$

so that for $n \geq 2$ we have

$$d_n \geq \frac{n^2}{12}$$

To conclude we get that for all $n \geq 2$

$$\frac{n^2}{12} \leq d_n \leq 8n^2$$

□

Algebraic Structures 1 - Tirgul 5

Yonatan Harpaz

November 17, 2010

1 A_5 is Simple

Theorem 1.1. *The group A_5 is simple.*

Proof. Let $\{e\} \neq H \triangleleft A_5$ be a normal subgroup. We will show that $H = A_5$. The proof will be divided into three steps:

1. We will show that H has to contain a 3-cycle.
2. We will show that if H contains a 3-cycle then it contains all 3-cycles.
3. We will show the 3-cycles generate all of A_5.

We begin with the first part. Since $H \neq \{e\}$ there exists a permutation $\sigma \in H$ which is not the identity. Since $H \subseteq A_5$ this permutation has to be even, so its cycle structure is either a single 5-cycle, a single 3-cycle, or two disjoint swaps. Assume first that σ is a 5-cycle, i.e. $\sigma = (a\ \ b\ \ c\ \ d\ \ e)$ for mutually distinct $a, b, c, d, e \in \{1, ..., 5\}$. Now note that

$$(a\ \ c\ \ e)(a\ \ b\ \ c\ \ d\ \ e)(a\ \ c\ \ e)^{-1} = (c\ \ b\ \ e\ \ d\ \ a)$$

and $(a\ \ c\ \ e) \in A_5$. Since H is normal we have $(c\ \ b\ \ e\ \ d\ \ a) \in H$. Now direct computation verifies that

$$(a\ \ b\ \ c\ \ d\ \ e)(c\ \ b\ \ e\ \ d\ \ a) = (b\ \ a\ \ d)$$

and so H contains the 3-cycle $(b\ \ a\ \ d)$.

If σ is composed of two disjoint swaps then $\sigma = (a\ \ b)(c\ \ d)$ for some mutually distinct $a, b, c, d \in \{1, 2, 3, 4, 5\}$. Let $e \in \{1, 2, 3, 4, 5\}$ be the one that is different then a, b, c and d. Then

$$(a\ \ e)(c\ \ d)\sigma((a\ \ e)(c\ \ d))^{-1} = (b\ \ e)(c\ \ d)$$

and $(a\ \ e)(c\ \ d) \in A_5$. Since H is normal we have $(e\ \ b)(c\ \ d) \in H$. Now since

$$(a\ \ b)(c\ \ d)((e\ \ b)(c\ \ d))^{-1} = (a\ \ b\ \ e)$$

we get that H contains the 3-cycle $(a\ \ b\ \ e)$.

We now need to show that if H contains a 3-cycle $(a\ \ b\ \ c)$ then it contains any other 3-cycle $(x\ \ y\ \ z)$. Note a delicate point: we know that every two 3-cycles are conjugated in S_5, but that does not guarantee that they are conjugates in A_5. However we will show that this is true specifically for 3-cycle. The reason is as following: let $d \neq e \in \{1, 2, 3, 4, 5\}$ be two elements which are different from a, b and c. Then we know that

$$(d\ \ e)(a\ \ b\ \ c)(d\ \ e) = (a\ \ b\ \ c)$$

now let $\tau \in S_5$ be such that

$$\tau(a\ \ b\ \ c)\tau^{-1} = (x\ \ y\ \ z)$$

if τ is in A_5 then $(x\ \ y\ \ z) \in H$ and we are done. If not then $\tau \cdot (d\ \ e)$ is in A_5 and

$$\tau(d\ \ e)(a\ \ b\ \ c)(d\ \ e)\tau^{-1} = (x\ \ y\ \ z)$$

so $(x\ \ y\ \ z) \in H$ and we're good to go.

Now for the final part, we need to show that 3-cycles generate all of A_5. So let $\sigma \in A_5$ be any element. We now that we can write σ is a product of (not necessarily disjoint) swaps:

$$\prod_{i=1}^{n}(a_i\ \ b_i)$$

Since σ is even n is even as well, so if σ is not the identity n has to be at least 2. Then we get that

$$(a_1\ \ b_1)(a_2\ \ b_2) = (a_1\ \ b_1)(b_1\ \ a_2)(b_1\ \ a_2)(a_2\ \ b_2)$$

note that $(a_1\ \ b_1)(b_1\ \ a_2)$ is either the identity or a 3-cycle and so is $(b_1\ \ a_2)(a_2\ \ b_2)$. This finishes the proof.

□

Algebraic Structures 1 - Tirgul 6

Yonatan Harpaz

November 27, 2010

1 The First Isomorphism Theorem

The first isomorphism theorem is a theorem which lets us compute in practice quotient groups. What do we mean here by compute? Well, to compute an abstractly given group, such as a quotient G/N usually means to find a familiar group H such that $G/N \cong H$. The first isomorphism theorem gives us a tool to do so. It says that all we need to do is to find a homomorphism from G to a familiar group H whose kernel is exactly N. In this section we are going to do this very thing with a few examples:

1. Consider the additive group $(\mathbb{R}, +)$ and its subgroup $\mathbb{Z} \subseteq \mathbb{R}$. Since $\mathbb{R}$ is abelian $\mathbb{Z}$ is normal in $\mathbb{R}$ and we can wonder as to the quotient group $\mathbb{R}/\mathbb{Z}$. We claim that this group is actually isomorphic to what is known as the circle group

$$S^1 = \{z \in \mathbb{C}^* | \|z\| = 1\} = \{a + bi \in \mathbb{C}^* | a^2 + b^2 = 1\}$$

   In order to prove this all we need to do is to find a homomorphism $\mathbb{R} \longrightarrow S^1$ whose kernel is exactly $\mathbb{Z}$. This homomorphism is the following:

$$\varphi(x) = e^{2\pi x} = \cos(2\pi x) + i \sin(2\pi x)$$

   Note that indeed $|e^{2\pi x}| = \cos^2(2\pi x) + \sin^2(2\pi x) = 1$ so $\varphi(x) \in S^1$. Further more φ is a homomorphism because $e^{2\pi(x+y)} = e^{2\pi x} e^{2\pi y}$.

2. Let us do a more complicated example. Recall the group $\mathrm{SL}_2(\mathbb{Z})$ which consists of all 2×2 matrices with integer coefficients and determinant 1. We already saw in previous TA session that this is a group with respect to matrix multiplication (the delicate point is why there are inverses, and the easiest way to see this is to note that the inverse of $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is $\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. Now let p be a prime number and consider the subgroup $H < \mathrm{SL}_2(\mathbb{Z})$ given by all matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that $a = 1 \pmod p$, $b = 0 \pmod p$, $c = 0 \pmod p$ and $d = 1 \pmod p$. In other words, the subgroup of all matrices which are equal to $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod p$.

It is not hard to check explicitly (as we have explicit formulas for multiplication and inverses of elements in $\mathrm{SL}_2(\mathbb{Z})$) that H is indeed a subgroup. In order to show that H is a **normal** subgroup, it is convenient to note that a matrix $A \in \mathrm{SL}_2(\mathbb{Z})$ is in H if and only if it can be written as a sub $I + pA$ with A a matrix with integer coefficients. Then if $B \in \mathrm{SL}_2(\mathbb{Z})$ is any element then

$$B(I + pA)B^{-1} = BB^{-1} + pBAB^{-1} = I + pBAB^{-1}$$

and since BAB^{-1} is a product of matrices with integer coefficients it also has integer coefficients. Hence H is closed under conjugation and is thus normal.

We wish to use the first isomorphism theorem in order to compute the quotient $\mathrm{SL}_2(\mathbb{Z})/H$. For that we need to find a homomorphism $G \longrightarrow H$ which is surjective (onto) and which has H as its kernel. Consider the homomorphism $\varphi : \mathrm{SL}_2(\mathbb{Z}) \longrightarrow \mathrm{SL}_2(\mathbb{Z}_p)$ given by reducing each of the components of the matrix modulu p. To be more explicit, if we denote the mod p homomorphism $\mathbb{Z} \longrightarrow \mathbb{Z}_p$ by $a \mapsto \overline{a}$ then φ is given by

$$\varphi \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix}$$

It is immediate from the definition of φ that the kernel of φ is exactly H. It is left to check that φ is surjective. For convenience we will denote elements in $\mathbb{Z}_p$ by $\overline{a}$ for $a \in \mathbb{Z}$.

Theorem 1.1. *For every* $\begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix} \in SL_2(\mathbb{Z}_p)$ *there exists an element* $\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in SL_2(\mathbb{Z})$ *such that*

$$\begin{pmatrix} \overline{a'} & \overline{b'} \\ \overline{c'} & \overline{d'} \end{pmatrix} = \begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix}$$

Proof. Let $\begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}_p)$. Since $\overline{a}\overline{d} - \overline{b}\overline{c} = 1$ we see that at least one of $\overline{a}, \overline{c}$ must be non-zero. Assume first that $\overline{c} \neq 0$. Then there exists an $\overline{r} \in \mathbb{Z}_p$ such that $\overline{cr} = \overline{a}$. Define $c' = c, a' = c'r + p$. Then $\overline{a'} = \overline{a}$ and $\overline{c'} = \overline{c}$. Further more c' and a' are coprime: indeed if a number q divides both c' and $c'r + p$ then q has to divide p which means that q is either 1 or p. But q can't be p because $\overline{c'} \neq 0$.

Now since c' and a' are coprime there exist numbers $x, y \in \mathbb{Z}$ such that

$$a'x + c'y = 1$$

Let $\Delta = a'd - c'b \in \mathbb{Z}$. Then

$$\overline{\Delta} = \overline{a'd} - \overline{c'b} = \overline{a}\overline{d} - \overline{c}\overline{b} = 1$$

and so $\Delta = 1 + pz$ for some $z \in \mathbb{Z}$. Define $b' = b + yzp, d' = d - xzp$. Then

$$a'd' - b'c' = a'(d - xzp) - c'(b + yzp) = a'd - c'b - a'xzp - c'yzp = \Delta - (a'x + c'y)zp = \Delta - zp = 1$$

which means that $\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. Clearly

$$\begin{pmatrix} \overline{a'} & \overline{b'} \\ \overline{c'} & \overline{d'} \end{pmatrix} = \begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix}$$

so we have proven the claim for the case $\overline{c} \neq 0$. Then case $\overline{a} \neq 0$ is completely analogous. $\square$

Algebraic Structures 1 - Tirgul 7

Yonatan Harpaz

December 26, 2010

1 Composition Series

Let us recall some of the concepts you've learned in the last week.

Definition 1.1. Let G be a group. We say that a sequence of subgroups $G = G_0 > G_1 > ... > G_n = \{e\}$ is a **composition series** if each G_i is normal in G_{i-1} and the quotient G_{i-1}/G_i is simple (in other words - G_i is a maximal normal subgroup of G_{i-1}).

Note that in a composition series each G_i is assumed to be a proper subgroup of G_{i+1} so the quotient is always non-trivial. Note further that not every group admits a composition series. Fir example, the group $\mathbb{Z}$ cannot contain any composition series - since all the non-trivial subgroups in $\mathbb{Z}$ are infinite cyclic one would get that $G_{n-1}/G_n \cong G_{n-1}$ is infinite cyclic and hence can't be simple.

Finite groups, however, must admit composition series. The reason is that each finite group contains a maximal normal (proper) subgroup so we can start with and construct the sequence downwards: $G > G_1 > G_2 > ....$ Since G is finite the sequence of orders $|G| > |G_1| > ...$ is strictly decreasing and so there has to be an $n \in \mathbb{N}$ such that $G_n = \{e\}$.

The sequence of quotients G_{i-1}/G_i will be referred to as the sequence of**simple components** or **simple factors** of the composition series. Note that a simple group may appear in this sequence more then once. Now although a group may have various different composition series, the sequence of components will be essentially the same - the only thing that can change is the order of the components. This is the content of the Jordan-Holder theorem:

Theorem 1.2. *Let G be a group and $G = G_0 > G_1 > ... > G_n = \{e\}$, $G = H_0 > H_1 > ... > H_m = \{e\}$ two composition series. Then $n = m$ and for each $i \in \{1, ..., n\}$ there exists a $j \in \{1, ..., n\}$ such that*

$$G_{i-1}/G_i \cong H_{j-1}/H_j$$

This theorem can be thought of as an analogue of the unique decomposition theorem in arithmetic which says that every positive number can be written as a product $n = \prod_{i=1}^{k} p_i$ of positive prime numbers in an essentially unique way - if $n = \prod_{j=1}^{m} q_j$ is any other decomposition then $m = n$ and for each $i \in \{1, ..., n\}$ there is a $j \in \{1, ..., n\}$ such that $p_i = q_j$.

In fact, the arithmetic unique decomposition theorem can actually be deduced from the Jordan-Holder theorem in the following way: Let G be a cyclic group of order n and let $x \in G$ be a generator. We saw in previous TA sessions that for every positive $d|n$ there exists a unique subgroup of G of order d and it is the cyclic subgroup generated by $x^{\frac{n}{d}}$ (and these are all the subgroups of G). From this description it is easy to see that the subgroup $\left\langle x^{\frac{n}{d_1}} \right\rangle$ contains $\left\langle x^{\frac{n}{d_2}} \right\rangle$ if and only if $d_2|d_1$. In this case we saw that the quotient

$$\left\langle x^{\frac{n}{d_1}} \right\rangle / \left\langle x^{\frac{n}{d_2}} \right\rangle$$

is cyclic and its order is simply the quotient of orders d_1/d_2

This means that decreasing sequences of subgroups $G = G_0 > G_1 > ... > G_k = \{e\}$ correspond to decreasing sequences of numbers $n = d_0 > d_1 > ... > d_k = 0$ such that $d_{i+1}|d_i$. Under this correspondence $G_i = \left\langle x^{\frac{n}{d_i}} \right\rangle$. Now in order for the relative quotients G_{i-1}/G_i to be simple we need that their order be prime (because a cyclic group is simple if and only if its order is prime). Hence composition series of G are in one-to-one correspondence with sequences of numbers

$$n = d_0 > d_1 > ... > d_k = 0$$

such that $d_{i+1}|d_i$ and the quotient d_{i+1}/d_i is a positive prime number (call it p_i). This corresponds exactly to was of writing n as a product

$$n = \prod_{i=1}^{k} p_i$$

Now applying the Jordan Holder to this case we get that the sequence of simple components is unique up to permutation and so we get exactly the unique decomposition theorem of arithmetic.

Let us now see some non-abelian examples: consider the case $G = S_n$. If $n = 2$ then $S_n \cong \mathbb{Z}_2$ is simple. Otherwise one can always start with $G_1 = A_n$ as the quotient $S_n/A_n \cong \mathbb{Z}_2$ is simple. Now if $n = 3$ then $A_n \cong \mathbb{Z}_3$ is simple and we are done. For $n = 5$ we have also proven that A_n is simple, and the same will be proven for all $n \geq 5$ in the next TA session. What about $n = 4$?

In the case $n = 4$ the group A_4 has a non-trivial composition series. Let

$$\sigma = (1\ \ 2)(3\ \ 4)$$

$$\tau = (1\ \ 3)(2\ \ 4)$$

Then one can compute directly and see that $\sigma\tau = \tau\sigma$ (the easiest way to see this is to use our formula for conjugation to see that $\sigma\tau\sigma^{-1} = \tau$). Since both σ and τ are elements of order 2 they for a subgroup $V = \{e, \sigma, \tau, \sigma\tau\}$. This subgroup is normal because the set

$$\{\sigma, \tau, \sigma\tau\} = \{(1\ \ 2)(3\ \ 4), (1\ \ 3)(2\ \ 4), (1\ \ 4)(2\ \ 3)\}$$

contains all the permutations whose cycle structure is two disjoint swaps and so is closed under conjugation. Since $|A_4| = 12$ and $|V| = 4$ we get that $|A_4/V| = 3$ so it has to be a cyclic group of order 3, i.e. simple. Now V has a proper subgroup $W =< \sigma >< V$ which is normal because V is abelian. Since $|W| = |V/W| = 2$ we see that they are both cyclic groups of order 2 and hence simple. Hence we have found a composition series

$$S_4 > A_4 > V > W > \{e\}$$

and the simple factors are $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_2, \mathbb{Z}_2$.

2 Direct Product

A composition series is a way to take a group and decompose it into simple factors. The obvious question now is how can we reconstruct information about a group from its simple factors. We already know that a group is not determined by its simple factors. However, given simple factors, there are natural constructions which give groups with these simple factors.

Let start with the simplest case. Suppose we are given two groups A, B. Can we construct a group G with a normal series $G \triangleright B \triangleright \{e\}$ such that $G/B \cong A$? Well there are many such groups, but there is one which is in some sense the "simplest" (using it here in the natural language and not mathematical meaning). This group is called the direct product of A and B, and is denoted by $A \times B$. Its elements are ordered pairs (a, b) with $a \in A, b \in B$ and the multiplication of two pairs is defined as follows:

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2, b_1 b_2)$$

it is very easy to see that this operation is associative. If we denote the neutral elements of A, B both by e (for simplicity) then (e, e) is the neutral element of $A \times B$. Then inverse of the element (a, b) is given by (a^{-1}, b^{-1}).

Note that $A \times B$ comes with two natural homomorphisms

$$p_A : A \times B \longrightarrow A$$

and

$$p_B : A \times B \longrightarrow B$$

given by $p_A(a, b) = a$ and $p_B(a, b) = b$. Note that both these homomorphisms are surjective. Now the kernel of p_A consists of all pairs (a, b) such that $a = e$, i.e.

$$\ker(p_A) = \{(e, b) | b \in B\} = \{e\} \times B$$

and similarly

$$\ker(p_B) = \{(a, e) | a \in A\} = A \times \{e\}$$

Clearly we have natural isomorphisms $\ker(p_A) \cong B$ and $\ker(p_B) \cong A$ (given by $(e, b) \leftrightarrow b$ and $(a, e) \leftrightarrow a$). In particular we see that $A \times B$ has a normal

subgroup isomorphic to B with the quotient being isomorphic to A, and vice-versa.

Now given a group G with a normal series $G \triangleright B$ with $G/B \cong A$ one can ask whether G happens to be isomorphic to the product $A \times B$. First of all we know that G must also have a normal subgroup isomorphic to A, so we write $A \triangleleft G$. The natural question now is the following, given a group G with two normal subgroups $A, B \triangleleft G$, when is G isomorphic to $A \times B$?

Note that we don't want an arbitrary isomorphism. If we construct an isomorphism from $A \times B$ to G then we want it to respect the inclusions of A, B, i.e. we want it to send (e, b) to b and (a, e) to a. This means in particular that the intersection of A and B in G must be trivial, i.e. $A \cap B = \{e\}$. Further we must have $AB = G$, i.e. every element in G would admit a presentation as a product $a \cdot b$. It turns out that these conditions are also sufficient:

Theorem 2.1. *Let G be a group and $A, B \triangleleft G$ two normal subgroups such that $A\cap = \{e\}$ and $AB = G$. Then there exists an isomorphism $\varphi : A \times B \longrightarrow G$ such that $\varphi((e, b)) = b$ and $\varphi((a, e)) = a$.*

Proof. Define $\varphi : A \times B \longrightarrow G$ by

$$\varphi((a, b)) = a \cdot b \in G$$

We want to show that φ is a homomorphism. For this we need to show that for every $(a_1, b_1), (a_2, b_2) \in A \times B$ we have

$$\varphi((a_1, b_1))\varphi((a_2, b_2)) \stackrel{?}{=} \varphi((a_1a_2, b_1b_2))$$

substituting the definition of φ on both sides we get that we need to prove

$$a_1b_1a_2b_2 = a_1a_2b_1b_2$$

or simply that

$$b_1a_2 = a_2b_1$$

which is equivalent to

$$b_1a_2b_1^{-1}a_2^{-1} = 1$$

Now this is true because this commutator has to belong to both A and B (why?), and $A \cap B = \{e\}$. So we've obtained that φ is a homomorphism. We now need to show that it is one-to-one and onto. The onto part is easy - it is a direct consequence of the fact that $AB = G$. So we will concentrate on showing that the kernel of φ is trivial. If $(a, b) \in \ker(\varphi)$ then $ab = e \in G$. Hence $b = a^{-1} \in A$. Since b is also in B we get that $b \in A \cap B = \{e\}$ so $b = e$. Since $b = a^{-1}$ we get that $a = e$ as well. Hence $(a, b) = (e, e)$ which is the neutral element of $A \times B$ and we are done. $\square$

Algebraic Structures 1 - Tirgul 8

Yonatan Harpaz

December 13, 2010

1 Solvable Groups

Let G be a group. We say that G is solvable if it has a normal series $G = G_0 > G_1 > G_2 > ...G_n = \{e\}$ such that the quotient G_{i-1}/G_i is abelian. This class of groups is a natural extension of the class of abelian groups, and it is characterized by the following property:

Definition 1.1. Let $\mathcal{A}$ be a class of groups. We say that $\mathcal{A}$ is **closed under extensions** if whenever we have a group G with a normal subgroup $N \triangleleft G$ such that $N, G/N \in \mathcal{A}$ then G is also in $\mathcal{A}$.

In exercise 8 you will prove that the class of all solvable groups is closed under extensions. Now by induction it follows that every class of groups containing the abelian groups and closed under extensions contains all solvable groups. Hence we see that the class of solvable groups is the smallest class of groups containing the abelian groups and closed under extensions.

There exists also an alternative description for solvable groups. Recall that the derived subgroup $G' < G$ (also denoted by $[G, G] < G$) is the subgroup generated by elements of the form $aba^{-1}b^{-1}$ (called commutators). In this TA session we will use the notation $[G, G]$ (for reasons that will be clear later).

Now as you saw in class and in exercise 5 the quotient $G/[G, G]$ is abelian and in fact $[G, G]$ is the smallest normal subgroup with that property, in the sense that it is contained in any other normal subgroup $H \triangleleft G$ such that G/H is abelian.

Definition 1.2. Let G be a group. Define the **derived series** to be the descending sequence of subgroups $G = G^{(0)} > G^{(1)} > G^{(2)} > ...$ defined inductively by

$$G^{(i)} = [G_{i-1}, G_{i-1}]$$

for $i \geq 1$.

Proposition 1.3. *Let G be a group. Then G is solvable if and only if there exists an n such that $G^{(n)} = \{e\}$.*

Proof. One direction is obvious - if the derived series stops after a finite number of steps then it constitute a normal series in which the consecutive quotients

$G_{i-1}/G_i = G_{i-1}/[G_{i-1}, G_{i-1}]$ are abelian. In the other direction if G admits a normal series $G = G_0 > G_1 > ...G_n = \{e\}$ such that G_{i-1}/G_i are abelian then we claim that

$$G^{(i)} \subseteq G_i$$

and so in particular $G^{(n)} = \{e\}$. We prove this by a simple induction. Clearly this is true for $i = 0$ because then $G^{(0)} = G = G_0$. Now assume that $G^{(i)} \subseteq G_i$ for some $i \geq 0$. Then since the quotient G_i/G_{i+1} is abelian we get that $[G_i, G_i] \subseteq G_{i+1}$. Then

$$G^{(i+1)} = [G^{(i)}, G^{(i)}] \subseteq [G_i, G_i] \subseteq G_{i+1}$$

and we are done. □

Corollary 1.4. *If G is solvable then it has a normal series with abelian quotients in which all the subgroups are normal in G.*

We can think of the derived series as follows: among all the normal series with abelian quotients, the derived series is the one in which the subgroups are the smallest, or alternatively the quotients are maximal.

Examples:

1. If G is finite then you can refine the derived series and get a composition series with abelian quotients, i.e. a composition series whose quotients are all isomorphic to some $\mathbb{Z}_p$. Hence we see that a finite group is solvable if and only if all of its simple factors are $\mathbb{Z}_p$'s. For example: S_3, S_4, D_4, Q.

2. Let F be a field and consider the subgroup $G < \mathrm{GL}_n(F)$ composed of all upper triangular matrices. Then we claim that G is solvable. For simplicity we will prove this just for the case of $n = 2$ but the principle can be extended to the case of general n. Consider the map $\mathrm{GL}_2(F) \longrightarrow F^* \times F^*$ given by
$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = (a, b)$$
It is easy to verify that this is indeed a homomorphism. Its kernel is the subgroup composed of all upper triangular matrices with 1's on the diagonal. This subgroup is isomorphic to the additive group $(F, +)$ and so is abelian. Hence we have a normal series with abelian quotients.

We can do a similar thing with $\mathbb{Z}$ instead of F, but we need to define $\mathrm{GL}_n(\mathbb{Z})$ properly: it is the group of all matrices with integers coefficients whose inverses are also with integer coefficients. This is equivalent to the determinant of a matrix being ± 1.

2 Nilpotent Groups

There is another important class of groups which contains all abelian groups and is contained in the class of solvable groups (this class of groups is hence not closed under extensions). This is the class of **nilpotent groups**.

Definition 2.1. Let G be a group. We say that G is **nilpotent** if it has a normal series $G = G_0 > G_1 > ... > G_n$ such that all the G_i's are normal in G and such that each quotient G_{i-1}/G_i is contained in the center of G/G_i.

Since the center of any group is abelian it follows that in a normal series such as in the definition the quotients G_{i-1}/G_i are abelian. Hence every nilpotent group is solvable. Further more it's clear that every abelian group is nilpotent.

This class of groups is defined as follows. First of all for a normal subgroup $H \triangleleft G$ we define $[G, H] < H$ to be the subgroup generated by all elements of the form $ghg^{-1}h^{-1}$ with $g \in G, h \in H$. It is not hard to show that $[G, H]$ is actually normal in both H and G. This construction has the following important property:

Proposition 2.2. *The subgroup $H/[G, H] < G/[G, H]$ is contained in the **center** of $G/[G, H]$. Further more $[G, H]$ is the smallest group with that property, i.e. if $N < H$ is subgroup which is normal in G such that H/N is contained in the center of G/N then $[G, H] \subseteq N$.*

Proof. Let $g[G, H] \in G/[G, H], h[G, H] \in H/[G, H]$ be two elements. Their commutator is the coset $ghg^{-1}h^{-1}[G, H]$. We want to show that this is the trivial coset, i.e. that $ghg^{-1}h^{-1} \in [G, H]$. But $[G, H]$ contains exactly all these elements by definition.

Now let $N < H$ be a subgroup which is normal in G such that H/N is contained in the center of G/N. Let $g \in G, h \in H$ be two elements. Then the commutator of the cosets gN and hN in G/N is the coset of $ghg^{-1}h^{-1}$. Since H/N is contained in the center of G/N this coset is trivial, so $ghg^{-1}h^{-1} \in N$. This implies that $[G, H] \subseteq N$ and we are done. □

Note that if $G = H$ that the claim of this proposition is the familiar claim that $G/[G, G]$ is abelian (contained in its own center) and is contained in any other normal subgroup with that property.

Definition 2.3. Let G be a group. The **descending central series** is the series $G = C_0 > C_1 > C_2 > ...$ defined inductively by

$$C_i = [G, C_{i-1}]$$

for $i \geq 1$.

Proposition 2.4. *Let G be a group. Then G is nilpotent if and only if there exists an n such that $C_n = \{e\}$.*

Proof. First suppose that the descending central series stops after a finite number of steps. Then by induction we get that each C_i is normal in G. Further more by Proposition 2.2 we get that C_{i-1}/C_i is contained in the center of G/C_i.

In the other direction if G admits a normal series $G = G_0 > G_1 > ...G_n = \{e\}$ such that each G_i is normal in G and such that G_{i-1}/G_i is contained in the center of G/G_i then we claim that

$$C_i \subseteq G_i$$

and so in particular $C_n = \{e\}$. We prove this by a simple induction. Clearly this is true for $i = 0$ because then $C_0 = G = G_0$. Now assume that $C_i \subseteq G_i$ for some $i \geq 0$. Then since the quotient G_i/G_{i+1} is contained in the center of G/G_{i+1} we get that $[G, G_i] \subseteq G_{i+1}$. Then

$$C_{i+1} = [G, C_i] \subseteq [G, G_i] \subseteq G_{i+1}$$

and we are done. □

There is also a third equivalent definition for nilpotent groups. Let G be a group and $H \triangleleft G$ a normal subgroup. We define the relative center $Z(G, H)$ as

$$Z(G, H) = \{g \in G | gH \in Z(G/H)\}$$

i.e. the group of all elements whose image in G/H lies in the center of G/H. Since $Z(G/H)$ is normal in G/H we get that $Z(G, H)$ is a normal subgroup of G.

Proposition 2.5. *The quotient $Z(G, H)/H$ is contained in the center of G/H (it is actually equal to it) and further more if $N \supseteq H$ is any subgroup such that N/H is contained in the center of G/H then $N \supseteq Z(G, H)$.*

Proof. Immediate from the definition. □

Definition 2.6. Let G be a group. The **ascending central series** is the ascending sequence of groups

$$\{e\} = C^0 < C^1 < C^2 < ...$$

defined inductively as

$$C^i = Z(G, C^{i-1})$$

Proposition 2.7. *Let G be a group. Then G is nilpotent if and only if there exists an n such that $C^n = G$.*

Proof. First suppose that $C^n = G$. Then by defining $G_i = C^{n-i}$ we get a normal series in which all groups ae normal in G and such that $G_{i-1}/G_i = C^{n-i+1}/C^{n-i}$ is actually equal (and hence in particular contained) in the center of $G/G_i = G/C^{n-i}$.

In the other direction suppose that G is nilpotent. Then descending central series stops after a finite number of steps so there exists an n such that $C_n = \{e\}$. We claim that $C^i \supseteq C_{n-i}$ and so in particular $C^n = G$. We prove this by induction. For $i = 0$ we have $C^0 = \{e\} = C_n$. Now suppose that

$$C^i \supseteq C_{n-i}$$

for some $i \geq 0$. Then

$$C^{i+1} = Z(G, C^i) \supseteq Z(G, C_{n-i}) \supseteq C_{n-i-1}$$

and we are done. □

Algebraic Structures 1 - Tirgul 10

April 9, 2011

1 Group Actions

1.1 Classification of Group Actions

In this section we will fix a group G and study sets X together with an action of G on them. A set X together with such an action is simply called a G-set. A map $f : X \longrightarrow Y$ between two G-sets is called **equivariant** if it respects the action of G, i.e. if

$$f(gx) = gf(x)$$

for every $x \in X, g \in G$. An equivariant map $f : X \longrightarrow Y$ between two G-sets is called an **isomorphism** if it is both one-to-one and onto, or equivalently if there exists an equivariant map $g : Y \longrightarrow X$ such that both $f \circ g$ and $g \circ f$ are the identity maps.

In this section we will classify all possible G-sets up to an isomorphism. The first step in such a classification is two break a G-set X to its **orbits**. We use the following notion

Definition 1.1. A G-set X is called **transitive** if for every $x, y \in X$ there exists a $g \in G$ such that

$$gx = y$$

Note that X is transitive if and only if all the elements are in the same orbit. If this is not the case, we can still divide X to the different orbits. Each one of the orbits is a sub G-set (i.e. it is a subset which is preserved by G) which is transitive. This means that every G-set is a disjoint union of transitive G-sets. It is left to classify transitive G-sets.

Recall the following familiar example for a G-set: let $H < G$ be a subgroup and let $X = G/H$ be the set of left cosets of H in G. Then G acts on X by multiplication on the left, i.e.

$$g(xH) = gxH$$

Note that this makes X into a transitive G-set, because for each $xH, yH \in X$ the element $g = yx^{-1}$ sends xH to yH. It is also not hard to check that the stabilizer of the element $H \in X$ is the subgroup H itself. It turns out that this covers all the transitive G-sets up to isomorphism.

Theorem 1.2. *Let X be a transitive G-set and $x \in X$ an element. Then X is isomorphic to G/H where $H = St_G(x)$ is the stabilizer of x in G.*

Proof. We need to construct an equivariant map $\varphi : G/H \longrightarrow X$ and show that it is an isomorphism. We will define φ is follows:

$$\varphi(gH) = gx$$

We need to show that this map is well defined, i.e. we need to show that if $g'H = gH$ then $gx = g'x$. But just note that if $g'H = gH$ then there exists an $h \in H$ such that $g' = gh$. Then $g'x = ghx = gx$ because H is the stabilizer of x. We now need to show that φ is equivariant. This is real easy too:

$$\varphi(g(g'H)) = \varphi(gg'H) = gg'x = g\varphi(g'H)$$

We will now show that φ is surjective. Let $y \in X$ be any element. Since X is transitive there exists a $g \in G$ such that $gx = y$. Then $\varphi(gH) = gx = y$ so y is in the image of φ.

It is hence left to show that φ is injective. Let $g_1H, g_2H \in G/H$ be two elements such

$$\varphi(g_1H) = \varphi(g_2H)$$

Then $g_1x = g_2x$ so $g_2^{-1}g_1x = x$. This means that $g_2^{-1}g_2$ is in the stabilizer of x which is H. Hence g_1, g_2 are in the same left coset of H, which means that $g_1H = g_2H$. This finishes the proof. □

1.2 Burnside's Lemma and Counting Problems

Burnside's lemma is a lemma which is useful for counting objects up to symmetries. Let X be a G-set. Suppose we want to count the objects of X but if two objects are in the same orbit we think of them as identical. Hence we just want to count the number of orbits. The set of orbits is usually denoted by X/G. Burnside's lemma is the following calculation:

$$|X/G| = \sum_{x \in X} \frac{1}{|O(x)|} = \sum_{x \in X} \frac{|\operatorname{St}_G(x)|}{|G|} = \frac{1}{|G|} \sum_{x \in X} |\operatorname{St}_G(x)| =$$

$$\frac{|\{(x, g) \in X \times G | gx = x\}|}{|G|} = \frac{1}{|G|} \sum_{g \in G} |X^g|$$

where $X^g = \{x \in X | gx = x\}$ is the set of fixed points of g. A nice way to state this lemma is that number of orbits is the average size of the fixed points sets. Let us demonstrate the usefulness of this lemma by an example. Suppose we are joule makes and we have n different kinds of diamonds. Suppose we live in a culture where it is customary to marry many spouses, but in order for them not to be jealous of each other we need to make each of them a different wedding ring.

Now according to the strict rules of our culture a wedding ring must contain exactly 25 diamonds in equal distances. A natural question then arises, how many different spouses can I marry (as a function of n). Note that a-priori there are n^{25} different ways to put the diamonds on the ring. However if two diamond configurations become the same after I rotate the ring or turn it upside down then the rings are actually the same (and your possible romantic interests will see if you try anything funny).

So we are left with a set X of size n^{25} of all diamond configurations. We have a natural action of D_{25} on it, and we want to count the number of **orbits**. Using Burnside's lemma we get

$$|X/G| = \frac{1}{50} \sum_{g \in D_2 5} |X^g|$$

So we are left to calculate the sizes of the fixed points sets X^g. Let $a \in D_{25}$ be rotation by $1/25$ a circle and b a reflection. What is the size of X^g when $g = a^n$? well if $n = 0$ then $g = 1$ and $|X^g| = n^{25}$. If $n = 5, 10, 15$ or 20 then we see that $|X^g| = n^5$ (because a configuration fixed by g in this case is freely determined by the values of the first consecutive 5 diamonds). Finally if n is not divisible by 5 then a^n has exactly n fixed points, and those are the configurations in which all the diamonds are the same.

As for reflections $a^n b$ it is not hard to see that since 25 is odd each reflection preserves exactly one of the diamonds, and the swaps the other 24 diamonds in pairs. Hence $|X^g| = n^{13}$ in this case. We conclude that

$$|X/G| = \frac{1}{50} \sum_{g \in D_{25}} |X^g| = \frac{1}{50} \left(n^{25} + 4n^5 + 20n + 25n^{13} \right)$$

2 Classification of Groups of size pq

Let $p < q$ be prime numbers. In this section we will use Silow theorem in order to classify all groups of size $|pq|$. We will show that if q is not equal to 1 mod p then the only group size pq is the cyclic group $\mathbb{Z}_{pq}$, and if q is equal to 1 mod p then there is a unique non-cyclic group of size pq (up to isomorphism). In the case $p = 2$ these are the familiar dihedral groups D_q. The generalization for all p goes as follows.

Let $\mathbb{F}_q$ be the field with q elements (its additive group is isomorphic to $\mathbb{Z}_q$). Recall that D_p can be identified with the subgroup of $S(\mathbb{F}_q)$ consisting of permutations of the form

$$x \mapsto \pm x + b$$

We will generalize this construction to an arbitrary p which divides $q - 1$ (this is equivalent to q being 1 mod p). The key idea is the theorem which says that the multiplicative group $\mathbb{F}_q^*$ is cyclic. Since its order is $q - 1$ is has a unique subgroup of order p.

Let G be a group of size pq. Let $P, Q < G$ be a p-Silow and a q-Silow subgroups respectively. The fundamental step is to use the last section of Silow's

theorem, which states that the number of q-Silow subgroups of G is 1 mod q. Since this number has to divide pq it is one of the numbers $1, p, q, pq$, but since $p < q$ the only one of them which is 1 mod q is 1. Hence Q is normal in G. If q is not equal to 1 mod p then the same argument shows that P is normal in G. Note that $P \cap Q = \{1\}$ because their sizes are coprime and $PQ = G$ because PQ is a subgroup of size pq. Hence in this case $G \cong P \times Q$. Since P, Q are of prime orders they are cyclic and so

$$G \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$$

We are left with the more complicated case when q is equal to 1 mod p. Let $a \in P, b \in Q$ be generators. Since Q is normal we get that $aba^{-1} \in Q$ so there exists an m such that

$$aba^{-1} = b^m$$

Note that $m \neq 0$ (because $aba^{-1} = 1$ implies $b = 1$) and we can always take m to be in $\{1, ..., q-1\}$. Now recall that the order of a is p and so

$$b = a^p b a^{-p} = a^{p-1} b^m a^{-(p-1)} = a^{p-2} b^{m^2} a^{-(p-2)} = ... = b^{m^p}$$

Hence $b^{m^p} = b$ which means that $m^p = 1$ mod q. Now we can think of m as an element in the multiplicative group $\mathbb{F}_q^*$, and the condition $m^p = 1$ is just saying that m is element of order p in $\mathbb{F}_q^*$. Now $\mathbb{F}_q^*$ is a cyclic group of order $q-1$ and $q-1$ is divisible by p. Hence $\mathbb{F}_q^*$ has a unique subgroup of size p, $H_p \leq \mathbb{F}_q^*$ which is composed of all elements $s \in \mathbb{F}_q^*$ such that $s^p = 1$. Hence we interpret m as an element of H_p.

Now if $m = 1$ (i.e. the trivial element of H_p) then $aba^{-1} = b$ which means that a and b commute and so P is normal as well and we return to the previous case

$$G \cong P \times Q \cong \mathbb{Z}_p \times \mathbb{Z}_q$$

We claim that the cases with $m \neq 1$ all give isomorphic groups. In order to do so we will show that they are all isomorphic to a certain generalization of the dihedral group.

Let $s \in \mathbb{F}_q^*, t \in \mathbb{F}_q$ be elements and let $\sigma_{s,t} \in S(\mathbb{F}_q)$ be defined by the formula

$$\sigma_{s,t}(x) = sx + t$$

Note that

$$(\sigma_{s,t} \circ \sigma_{r,u})(x) = s(rx + u) + t = srx + su + t = \sigma_{sr,su+t}(x)$$

Let $D_{p,q} \subseteq S(\mathbb{F}_q)$ be the subgroup consisting of all permutations $\sigma_{s,t}$ such that $s \in H_p$. From the computation above and since H_p is a subgroup we see that $D_{p,q}$ is indeed a subgroup. For example, if $p = 2$ then $H_p = \{-1, 1\}$ and so $D_{2,q}$ is just the dihedral group D_q. Clearly the size of $D_{p,q}$ is pq (the product of the size of H_p and the size $\mathbb{F}_q$).

Now return to our G of size pq as above with its elements $a, b \in G$ satisfying

$$a^p = 1$$

$$b^q = 1$$

$$aba^{-1} = b^m$$

We want to construct an isomorphism T from G to $D_{p,q}$. Since $G = QP$ and $P = \langle a \rangle, Q = \langle b \rangle$ we get that every element $g \in G$ can be written uniquely as a product

$$g = b^i a^j$$

for $i \in \{0, ..., q-1\}, j \in \{0, ..., p-1\}$. In particular we can interpret i as an element in $\mathbb{F}_q$. We also interpret m as an element of H_p. This leads to the following definition of T:

$$T(b^i a^j) = \sigma_{m^j, i}$$

We need to start by showing that this is even a homomorphism. By applying the relation $ab = b^m a$ many times we get that $a^j b^k = b^{m^j k} a^j$. Hence

$$T(b^i a^j b^k a^l) = T(b^i b^{m^j k} a^j a^l) = T(b^{m^j k + i} a^{j+l}) =$$

$$\sigma_{m^{j+l}, m^j k + i} = \sigma_{m^j, i} \circ \sigma_{m^l, k} = T(b^i a^j) \circ T(b^k a^l)$$

So T is indeed a homomorphism. Since G and $D_{q,p}$ have the same size we only need to show that T is injective. Let i, j be such that $\sigma_{m^j, i}$ is the identify permutation. Then in particular

$$\sigma_{m^j, i}(0) = 0$$

which means that

$$m^j \cdot 0 + i = 0$$

or simply $i = 0$ (because $i \in \{0, ..., q-1\}$). Similarly since now

$$\sigma_{m^j, 0}(1) = 1$$

we get that

$$m^j \cdot 1 = 1$$

or $m^j = 1$. But we assumed that $m \neq 1$ and since H_p is a cyclic group of order p it has no proper subgroups. Hence m must be a generator of H_p. This means that the equation $m^j = 1$ (together with the range $j \in \{0, ..., p-1\}$ implies that $j = 0$. Hence the kernel is trivial and T is an isomorphism.

Algebraic Structures 1 - Tirgul 11

December 22, 2010

1 Finite Abelian Groups

Theorem 1.1. *Let G be a finite abelian group. Then G is a product of cyclic groups.*

Proof. Since all the p-Silow subgroup in G are normal we get that G is a product of its p-Silow subgroups. Hence it is enough to prove the theorem for abelian p-groups. For this we will use the following concept:

Definition 1.2. A finite set $\{x_1, ..., x_n\} \subseteq G$ is called **independent** if whenever

$$\sum_i a_i x_i = 0$$

then $a_i x_i = 0$ for all $i = 1, ..., n$.

It is easy to see (using our generalized criterion for direct product) that $\{x_1, ..., x_n\}$ is independent if and only if

$$\langle x_1, ..., x_n \rangle \cong \langle x_1 \rangle \times \langle x_2 \rangle \times ... \times \langle x_n \rangle$$

For each independent set $A = \{x_1, ..., x_n\}$ we call the size of $\langle A \rangle$ the **order** of A. In order to prove the question we need to show that there is an independent set of order $|G|$.

Clearly independent sets exists (for example every set with on element is independent). Let $A = \{x_1, ..., x_n\}$ be an independent set of **maximal** order. We will show that $\langle A \rangle = G$.

Suppose that $\langle A \rangle \neq G$. Then there exists an $y \in G$ which is not in $\langle A \rangle$. In particular there exists a y which is not in $\langle A \rangle$ but such that $py \in A$. Note that in this case p is the minimal number k such that $ky \in \langle A \rangle$. Let $a_1, ..., a_n$ such that

$$py = \sum_i a_i x_i$$

Let $S \subseteq \{1, ..., n\}$ be the subset of all the i's such that $p | a_i$. Define

$$z = y - \sum_{i \in S} \frac{a_i}{p} x_i$$

note that $z \notin \langle A \rangle$ but

$$pz = \sum_{i \notin S} a_i x_i \in \langle A \rangle$$

so we can work with z instead of y. We now separate into two cases: the first case is when $S = \{1, ..., n\}$. In that case $pz = 0$ and it is not hard to see that $A \cup \{z\}$ is an independent set with larger order then A - a contradiction.

The second case is when $S \neq \{1, ..., n\}$. In that case Let r be the minimal number such that $p^r x_i = 0$ for all $i \notin S$. Since A is independent the order of

$$pz = \sum_{i \notin S} a_i x_i \in \langle A \rangle$$

is p^r and hence the order of z is p^{r+1}. Let $j \in \{1, ..., n\} \setminus S$ be such that the order of x_j is in fact p^r. Assume for simplicity that $j = 1$. Then we claim that the set $A' = \{z, x_2, ..., x_n\}$ is an independent set of order greater then that of A. First we need to show that A' is independent. Suppose that

$$b_1 z + \sum_{i=2}^{n} b_i x_i = 0$$

Since $b_1 z \in \langle A \rangle$ we get that $b_1 = p b_1'$ for some b_1'. Then

$$0 = b_1 z + \sum_{i=2}^{n} b_i x_i = b_1' \left[\sum_{i \notin S} a_i x_i \right] + \sum_{i=2}^{n} b_i x_i =$$

$$b_1' a_1 x_1 + \sum_{i \in \{2, ...n\} \setminus S} b_1' a_i x_i + \sum_{i=2}^{n} b_i x_i$$

Since A is independent we get that

$$b_1' a_1 x_1 = 0$$

and so $p^r | b_1' a_1$. Since p does not divide a_1 we get that $p^r | b_1'$ and so $p^{r+1} | b_1$. This means that

$$b_1 y = 0$$

and since $\{x_2, ..., x_n\}$ is independent $b_i x_i = 0$ for all $i = 2, ..., n$. This shows that A' is independent. Since we've replaced the element $x_1 \in A$ of order p^r with an element z of order p^{r+1} we got an independent set of larger order - contradiction.

Hence $\langle A \rangle = G$ and we are done. $\square$

Algebraic Structures 1 - Tirgul 12

January 6, 2011

1 Rings and Ideals

In this TA session we give and compute examples of rings, ideals, and quotient rings.

1.1 Non Commutative Rings

1. Let F be a field and consider the ring $R = M_n(F)$ of $n \times n$ matrices over F. What are the ideals in this ring? note that R is not commutative, so we need to distinguish between left ideals, right ideals and two-sided ideals. Left ideals $I \subseteq R$ are subsets of matrices which are closed under addition and multiplication from the left. We will now classify all of them:

   Theorem 1.1. *If $I \subseteq R$ is a left ideal then there exists a sub vector space $V \subseteq F^n$ such that*
   $$A \in I \Leftrightarrow Av = 0, \forall v \in V$$

   Proof. There is a natural way to "guess" what V should be: we define
   $$V = \{v \in \mathbb{R}^n | Av = 0, \forall A \in R\} = \cap_{A \in R} \ker(A)$$
   and consider
   $$I_V = \{A \in R | Av = 0, \forall v \in V\}$$
   Since $Av = 0$ implies $BAv = 0$ for all B we see that I_V is a left ideal. Further more from the definitions it is clear that $I \subseteq I_V$. We need to show that this inclusion is actually an equality.

   First we will show that there exists an $A \in I$ such that
   $$\ker(A) = V$$
   Let $A_1, A_2 \in I$ be two matrices. By definition $V \subseteq \ker(A_1) \cap \ker(A_2)$. We claim that there exists a matrix $C \in I$ such that $\ker(C) = \ker(A_1) \cap \ker(A_2)$. Let $\{v_1, ..., v_n\}$ be a basis for $\mathbb{R}^n$ such that $B = \{v_1, ..., v_k\}$ are a basis for $\ker(A_1) \cap \ker(A_2)$, $\{v_{k+1}, ..., v_m\}$ complete B to a basis of

$\ker(A_1)$ and $\{v_{m+1}, ..., v_l\}$ complete V to a basis for $\ker(A_2)$ (this is all just standard linear algebra).

Now the set $\{A_1 v_{m+1}, ..., A_1 v_n\}$ is linearly independent so there exists a B_1 such that

$$B_1 A_1 v_i = e_i$$

for $i \in \{m+1, ..., n\}$. Similarly the set $\{A_2 v_{k+1}, ..., A_2 v_m, A_2 v_{l+1}, ..., A_2 v_n\}$ is linearly independent so there exists a matrix B_2 such that

$$B_2 A_2 v_i = e_i$$

for $i \in \{k+1, ..., m, l+1, ..., n\}$. Let $C = B_1 A_1 + B_2 A_2 \in I$. Then we see that

$$Cv_i = B_1 A_1 v_i + B_2 A_2 v_i = \begin{cases} 0 & i = 1, ..., k \\ e_i & i = k+1, ..., l \\ 2e_1 & i = l+1, ..., n \end{cases}$$

and so $\ker(C) = \ker(A_1) \cap \ker(A_2)$. By induction we see that for any finite subset $\{A_1, ..., A_n\} \in I$ there exists a $C \in I$ such that $\ker(C) = \cap_{i=1}^n A_i$. Since there can't be a strictly decreasing infinite sequences of vector spaces (because this will result in a strictly decreasing infinite sequences of dimensions) we get that there exists an $A \in I$ such that

$$\ker(A) = \cap_{A \in I} \ker(A) = V$$

Now let $B \in I_V$ be any matrix. We need to show that $B \in I$. From the definition of I_V we get that

$$\ker(A) \subseteq \ker(B)$$

We will show that there exists a matrix C such that $B = CA$, and this will imply $B \in I$. Let $\{v_1, ..., v_n\} \subseteq \mathbb{R}^n$ be a basis such that $\{v_1, ..., v_k\}$ are a basis for $\ker(A_1)$. Then the space spanned by $\{v_{k+1}, ..., v_n\}$ has a trivial intersection with $\ker(A_1)$ and so $\{A_1 v_{k+1}, ..., A_1 v_n\}$ are linearly independent. Hence there exists a matrix C such that

$$CAv_i = Bv_i$$

for $i \in \{k+1, ..., n\}$. Since

$$CAv_i = 0 = Bv_i$$

automatically for $i = 1, ..., k$ we get that

$$CA = B$$

and we are done. □

Corollary 1.2. *Let $I \in R$ be a left ideal. Then there exists an $A \in R$ such that*

$$I = \{BA | B \in R\}$$

Such ideals are called **principal** left ideals. We also say that they are **generated by** 1 **element** and in some contexts that they are **cyclic** (like groups which are generated by one element).

What about right ideals? well note that we have the transpose operation $A \mapsto A^t$ which satisfies

$$(A+B)^t = A^t + B^t$$

and

$$(AB)^t = B^t A^t$$

Hence if I is a right ideal then

$$I^t = \{A^t | A \in I\}$$

is a left ideal. Hence we get that every right ideal I is principal as well, i.e. there exists an $A \in R$ such that

$$I = \{AB | B \in R\}$$

we can also describe I as

$$I = \{A \in R | v^t A = 0, \forall v \in V\}$$

for some sub vector space $V \subseteq \mathbb{R}^n$.

What about two sided ideals? well it turns out that there aren't two many of those:

Theorem 1.3. *Let $I \subseteq R$ be a two sided ideal. Then $I = 0$ or $I = R$. Comment: we call such rings **simple rings**. This is the ring analogy of simple groups.*

Proof. Let $I \in R$ be a two sided ideal and let $A \in I$ be a non-zero element. We need to show that $I = R$. Let $E^{i,j} \in R$ be the matrix whose (i,j)-entry is 1 and all the rest are 0. Since every matrix is a linear combination of $E^{i,j}$'s it is enough to show that $E^{i,j} \in I$. Since $A \neq 0$ there exists an entry (k,m) such that $A_{k,m} \neq 0$. Then direct computation verifies that

$$E^{i,k} A E^{m,j} = E^{i,j}$$

Note that a two sided ideal is closed to multiplication from both left and right, and so this implies $E^{i,j} \in I$ and we are done.

□

2. The second important example of a non-commutative ring is the **quaternion ring**. Let F be a field. The Hamiltonian quaternion ring $\mathbb{H}(F)$ is the ring whose elements are formal combinations

$$a + bi + cj + dk$$

The addition is defined in the obvious way and the multiplication is done according to the rules

$$i^2 = j^2 = k^2 = -1$$
$$ij = -ji = k$$
$$jk = -kj = i$$
$$ki = -ik = j$$

For example let us compute the multiplication of $1 + i + j$ and $1 - 2k$:

$$(1+i+j)(1-2k) = 1+i+j-2k-2ik-2jk = 1+i+j-2k+2j-2i = 1-i+3j-2k$$

Note that the coefficients (which can be though of as the sub ring of elements of the form $a + 0i + 0j + 0k$) commute with everything.

We define the **conjugate** of an element $x = a+bi+cj+dk \in \mathbb{H}(F)$ to be

$$\overline{x} = a - bi - cj - dk$$

It is a direct computation to verify that

$$x\overline{x} = \overline{x}x = a^2 + b^2 + c^2 + d^2$$

We call this the **norm** of x and denote it by $|x|$. Note that this means in particular that

$$x \cdot \frac{x}{|x|} = \frac{x}{|x|} \cdot x = 1$$

and so if $|x| \neq 0$ then x is **invertible** in the ring $\mathbb{H}(F)$.

It turns out (although this exceeds the scope of this course) that if there exists an element such hat $|x| = 0$ then $\mathbb{H}(F)$ is actually isomorphic to $M_2(F)$. If, on the other hand $|x| \neq 0$ for every $x \in \mathbb{H}(F)$ then every element is invertible. In this case $\mathbb{H}(F)$ is what's called a **division ring**. It is clear that in such a case every two-sided ideal is trivial, so in particular $\mathbb{H}(F)$ is always simple.

Comment: for the case $F = \mathbb{C}$ the element $1 + \sqrt{-1}i$ has norm 0 and we can show an explicit isomorphism $\varphi : \mathbb{H}(\mathbb{C}) \longrightarrow M_2(\mathbb{C})$. It is given by

$$\varphi(1) = I$$
$$\varphi(i) = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}$$
$$\varphi(j) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$
$$\varphi(k) = \begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix}$$

One can formally check that the defining relations between i, j and k are satisfied by these matrices.

3. Let F be a field and consider the subfield $R \subseteq M_n(F)$ consisting of **upper triangular matrices**. Consider the direct product ring $F^n = \overbrace{F \times F \times ... \times F}^{n}$ where we add and multiply vectors coordinate wise. We have a homomorphism $\varphi : R \longrightarrow F^n$ given by

$$\varphi(A) = (A_{1,1}, ..., A_{n,n})$$

It is a direct computation to verify that this is indeed a homomorphism. Let $I = \ker(\varphi)$. Then I consists of all matrices $A \in R$ which have only zeros on their diagonal (such matrices are sometimes called **strictly upper triangular**). Since this I is a kernel it is automatically a tow-sided ideal. Since φ is surjective we get from the first isomorphism theorem that $R/I \cong F^n$.

4. Let F e a fiend and V and **infinite** dimensional vector space over F. Let $L(V)$ be the set of all linear transformation $T : V \longrightarrow V$. Then $L(V)$ has a natural ring structure - addition is addition of linear transformations and multiplication is composition. Note that if V was finite dimensional we would get something isomorphic to some $M_n(F)$.

   Let $I \subseteq L(V)$ be the subset of all linear transformations whose **image** is finite dimensional. IT is easy to check that I is closed under addition and multiplication from left and right. Hence I is a two-sided ideal.

1.2 Commutative Rings

1. Let $R = \mathbb{Z}$ be the ring of integers. What are the ideals in $\mathbb{Z}$? Since every ideal is in particular a subgroup we know that if $I \triangleleft \mathbb{Z}$ is an ideal then there exists an $n \in \mathbb{Z}$ such that

$$I = \{na | a \in \mathbb{Z}\} = \langle n \rangle$$

   Now it is clear that such for each $n \in \mathbb{Z}$ then the subgroup generated by n is in fact the ideal generated by n, so we get that these are actually all the ideals. How does the quotient ring look like? Well as an additive group it is just $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ and it is not hard to see that the multiplication is actually multiplication mod n: if $a, b \in \{0, ..., n-1\}$ and we denote by $a \cdot_n b \in \{0, ..., n-1\}$ their multiplication mod n then

$$(a + \langle n \rangle)(b + \langle n \rangle) = ab + \langle n \rangle = a \cdot_n b + \langle n \rangle$$

2. Let R be a ring. We denote by $R[x_1, ..., x_n]$ the ring of polynomials in n variables with coefficients in R.

   Theorem 1.4. *If R is a field then $R[x]$ is a Euclidian domain.*

Proof. The Euclidian norm here is just the degree $|f| = \deg(f)$. The first axiom that a Euclidian norm needs to satisfy is that

$$\deg(fg) \geq \deg(f)$$

This is satisfied because when R is a field we have $\deg(fg) = \deg(f) + \deg(g)$. This is a familiar property of polynomials but let's see exactly why this is so. If $f = ax^d + f_1$ and $g = bx^e + g_1$ where $a, b \neq 0$. $\deg(f_1) < d$ and $\deg(g_1) < e$ then

$$fg = abx^{d+e} + h$$

where $\deg(h) < de$. Since R is a field we get that $a, b \neq 0$ implies $ab \neq 0$ and so $\deg(fg) = \deg(f) + \deg(g)$. Note that if R is not a field then it might be that $0 \neq a, b \in R$ but $ab = 0$ so this argument would fail.

The second thing we need to show that for every $f, g \in R[x]$ we can write $f = qg + r$ with either $r = 0$ or $\deg(r) < \deg(g)$. We start by showing that if $\deg(f) \geq \deg(g)$ there exists a $q \in R[x]$ such that $\deg(f - qg) < \deg(f)$. Let $\deg(f) = d$, $\deg(g) = e \leq d$ and write $f = ax^d + f_1$ and $g = bx^e + g_1$ with $\deg(f_1) < d$, $\deg(g_1) < e$ and $a, b \neq 0$. Then

$$f - \frac{a}{b}x^{d-e}g = ax^d - ax^d + f_1 - \frac{a}{b}g_1 = f_1 - \frac{a}{b}g_1$$

so in particular $\deg(f - \frac{a}{b}x^{d-e}g) < d$.

From the above observation we see that we can construct a finite sequence $f = f_0, f_1, f_2, ..., f_n$ such there exist q_i with $f_i = f_{i-1} - q_i g$ and f_n is either 0 or of degree $< n$. Define $r = f_n$ and $q = \sum_{i=0}^{n-1} q_i$ and you will get

$$f = qg + r$$

□

You will see later in the course that when R is a field, every ideal of $R[x]$ is generated by a single element. This is not true when R is not a field, even if R is an integral domain ("thum shlemut"). For example if $R = \mathbb{Z}$ then the elements $2, x \in R[x]$ generate a non-trivial ideal (it contains only polynomials whose free coefficient is even) but the only polynomials which divide both 2 and x are ± 1, which generate the ideal which is all of $R[x]$.

Let us return now to the case that R is a field. The this division with remainder process can be used to find a concrete description of quotient rings $R[x]/\langle g \rangle$. In every coset $f + \langle g \rangle$ we can find a representative of degree $< n$ by simply writing $f = qg + r$ and noting that r and f are in the same $\langle g \rangle$-coset. Further more note that a coset cannot contain two different elements of degree $< n$ because their difference would be a non-zero polynomial of degree $< n$ and such a polynomial cannot be divisible by g. Hence we see that we have a one-to-one correspondence between elements of $R[x]/\langle g \rangle$ and polynomials of degree $< n$. In order multiply

two elements in this representation we multiply them as polynomial and then take the remainder when dividing by g.

Example: Let $R = \mathbb{R}$ be the field of real numbers and $f = x^2 + 1$. Then we can represent each element in $\mathbb{R}/\langle x^2 + 1\rangle$ by a polynomial of degree 1, i.e. by an element $a + bx$. How do you multiply two such elements? let $a + bx, c + dx$ be two elements. You start by multiplying them as polynomials, getting

$$(a + bx)(c + dx) = ac + (ad + bc)x + bdx^2$$

we now need to take the remainder obtained when dividing $f = ac + (ad + bc)x + bdx^2$ by $x^2 + 1$. For this we subtract from f the polynomial $bd(x^2 + 1)$ in order to cancel the coefficient of x^2 this results in

$$ac + (ad + bc)x + bdx^2 - bd(x^2 + 1) = (ac - bd) + (ad + bc)x$$

Note that we have obtained that the ring $\mathbb{R}[x]/\langle x^2 + 1\rangle$ is isomorphic to the field $\mathbb{C}$ of complex numbers by the isomorphism

$$\varphi(a + bx) = a + bi$$

This should not surprise us, because the ring $\mathbb{R}[x]/\langle x^2 + 1\rangle$ can be thought of as obtained from $\mathbb{R}$ by adding an element x which satisfying the **equation** $x^2 + 1 = 0$, i.e. by adding a square root to -1.

Algebraic Structures 1 - Tirgul 13

January 7, 2011

0.1 Quotients of Polynomial Rings and Finite Fields

Let F be a field and $R = F[x]$ the polynomial ring in one variable over F. By now you already know that R is a Euclidian domain with the norm function being the degree $|f| = \deg(f)$. The following theorem will appear in class but since the proof is short we include here for completeness:

Theorem 0.1. *Let R be a Euclidian domain and $I \triangleleft R$ and ideal. Then I is generated by an element of minimal norm in I. In particular I is principal.*

Proof. Let $x \in I$ be an element of minimal norm in I (there is always such an element because the norm takes values in non-negative integers). We need to show that $\langle x \rangle = I$. Let $y \in R$ be an element. Since R is Euclidian we can write $y = qx + r$ such that either $r = 0$ or $|r| < |x|$. The second option is not possible because x has the minimal norm of all elements in I. Hence we conclude that $r = 0$ which means that $y = qx$ and in particular $y \in \langle x \rangle$. This shows that $\langle x \rangle = I$. □

Going back to our polynomial ring $R = F[x]$ we see that if $I \triangleleft R$ is an ideal than it is generated by an element of minimal degree in I. We are interested in the question when R/I is a field. As you saw in the lectures this is equivalent to I being maximal. Hence we need to figure out for which $f \in R$ the ideal $\langle f \rangle$ is maximal. Since $\langle 0 \rangle = 0$ is clearly not maximal we can assume that $f \neq 0$.

Now $\langle f \rangle$ is maximal if whenever $\langle f \rangle$ is contained in another ideal $\langle g \rangle$ then either $\langle f \rangle = \langle g \rangle$ or $\langle g \rangle = R$. It is easy to see that $\langle f \rangle \subseteq \langle g \rangle$ if and only if $f \in \langle g \rangle$, i.e. if and only if g divides f. Now the situation $\langle f \rangle = \langle g \rangle$ means that $f|g$ as well, which means that f, g have the same degree and $f = ag$ with $0 \neq a \in F$. The second allowed situation is that $\langle g \rangle = R$. In this situation $1 \in \langle g \rangle$ so g must be of degree 0 (but it can't be the zero polynomial) so we see that g is a non-zero scalar polynomial. Note that non-zero scalar polynomials are exactly the **units** (invertible elements) of the ring R.

The conclusion from the following discussion is this: The quotient ring $R/\langle f \rangle$ is a field if and only if whenever $f = gh$ then either g is unit or h is a unit. In this situation we say that f is **irreducible**. Otherwise we say that f is **reducible**.

Let us use this observation in order to construct some small finite fields. Let p be a prime number and suppose that $F = \mathbb{F}_p$ is the field with p elements. Let

$f \in F[x]$ be an irreducible polynomial of degree n. As we saw in the previous tirgul, for each coset $g + \langle f \rangle$ we can find a unique representative whose degree is smaller than n, and each two different polynomials of degree $< n$ lie in different cosets. Hence we will get that the number of elements in $F[x]/\langle f \rangle$ is exactly p^n.

Let us try to construct a field of size 4. For this we will take $p = 2$ and $n = 2$ so we need to find an irreducible polynomial of degree 2 in $\mathbb{F}_2[x]$. Polynomials of degree 2 in $\mathbb{F}_2[x]$ look like this: $f = x^2 + ax + b$ for some $a, b \in \mathbb{F}_2$.

Note that a polynomial of degree 2 is reducible if and only if it is divisible by a polynomial of degree 1. As you saw in a previous exercise, f is divisible by $x - a$ if and only if $f(a) = 0$. Hence all we need to make sure here is that $f(0) = 1$ and $f(1) = 1$. These conditions translate to

$$b = 1$$

$$a + b + 1 = 1$$

so we see that the only solution is $b = 1, a = 1$. To conclude, we have found that there is exactly one irreducible polynomial of degree 2 in $\mathbb{F}_2[x]$, and that is the polynomial

$$f = x^2 + x + 1$$

We can now use this polynomial in order to construct a field of size 4. This field will be the quotient ring $\mathbb{F}_2[x]/\langle f \rangle$, and we will denote it by $\mathbb{F}_4$. As we saw we can work with the following representatives:

$$0, 1, x, x + 1$$

Addition and multiplication is now performed modulu $x^2 + x + 1$, i.e. we first add or multiply as polynomial and then if the result has degree > 1 we take the remainder obtained when dividing by $x^2 + x + 1$. Note that when adding two polynomials of degree 1 the result is still of degree 1, so we don't need to take the remainder. In particular we see that the additive group of $\mathbb{F}_4$ is isomorphic to the direct product $\mathbb{Z}_2 \times \mathbb{Z}_2$. The multiplcation is a bit more tricky, so let us write explicitly what one gets. Note that $0 \cdot \alpha = 0$ and $1 \cdot \alpha = \alpha$ for every $\alpha \in \mathbb{F}_4$, so all we need to calculate are the products:

$$x \cdot x = x^2 = x + 1 + (x^2 + x + 1) = x + 1$$

$$x \cdot (x + 1) = x^2 + x = 1 + (x^2 + x + 1) = 1$$

$$(x + 1) \cdot (x + 1) = x^2 + 2x + 1 = x + (x^2 + x + 1) = x$$

In particular we see that the two elements which are not $0, 1$ are the inverses of each other.

Remark 0.2. Here is some guidance on how to solve the first question in exercise 13. You need to find an irreducible polynomial of degree 3 in $\mathbb{F}_3[x]$. The key point is that for degree 3 it is still true that a polynomial is irreducible if and

only if it is not divisible by a polynomial of degree 1 (why?) and so all we need is to find a polynomial f of degree 3 such that

$$f(a) \neq 0$$

for every $a \in \mathbb{F}_3$. The second observation is that for every three values $a_0, a_1, a_2 \in \mathbb{F}_3$ there exists a polynomial of degree 3 such that

$$f(0) = a_0$$

$$f(1) = a_1$$

$$f(2) = a_2$$

and this f can found by solving linear equations.