CS174 Spr 99 Lecture 22 Summary John Canny

Group Theory

Recall that a group is a set of elements with a binary (two-argument) operation defined on it, $G = (D, \cdot)$ where D is the domain (set of elements) and $\cdot$ is the group operation, which is often called "group multiply". The group satisfies:

Closure: $a, b \in G$ implies $ab \in G$ (we usually write ab for the product of a and b rather than $a \cdot b$.

Associativity: For any $a, b, c \in G$, then $(ab)c = a(bc)$

Identity: There is an element $e \in G$ such that for all $a \in G$, $ae = ea = a$

Inverse: If e is the identity, then for every $a \in G$ there is another element b such that $ab = ba = e$. The element b is called the *inverse* of a and is often written as a^{-1}.

Some groups, called *Abelian* groups satisfy another property:

Commutativity: For all $a, b \in G$, then $ab = ba$

Example:
The group $G = (\mathbb{Z}, +)$, the group of integers under addition. The identity element is 0, and the additive inverse of a is $-a$. This group is abelian as well.

Example:
The group $G = (\mathbb{Z}_p^*, *)$, the group of integers modulo a prime p under multiplication (zero is excluded from $\mathbb{Z}_p^*$). Lets check group properties:

Closure: Multiplication $(\bmod\ p)$ of non-zero elements produces another non-zero element.

Associativity: This takes a bit of work. We note that reduction $(\bmod\ p)$ means subtracting a multiple of p:

$a(bc(\bmod\ p))(\bmod\ p) = a(bc - k_1 p) - k_2 p = abc - k_3 p$

and doing the same calculation for $(ab)c$ gives:

$(ab)c(\bmod\ p))(\bmod\ p) = (ab - k_4 p)c - k_5 p = abc - k_4 p$

and then we remark that there is only one multiple of p that can be added to abc to give a value in the range $[0, \ldots, p-1]$, which implies that $k_3 = k_4$. Therefore $(ab)c = a(bc)$. Because the order of taking mods doesnt matter, we would often just write $abc(\bmod\ p)$ for the result.

Identity: The identity element is 1.

Inverse: To find an inverse for non-zero a, we can use the extended Euclid algorithm to compute x and y such that

$$1 \; = \; \gcd(a, p) \; = \; ax + py$$

and then rewrite this as $ax \; = \; 1 - py$ or in other words $ax \; = \; 1 (\bmod \; p)$. That is, x is the multiplicative inverse of $a \pmod{p}$.

Commutativity: Commutativity follows from commutativity of ordinary multiplication of integers.

Cyclic Groups:
A *cyclic* group has one or more elements g which are *generators* of the group. If g is a generator, then every element in the group is expressible as a power of g.

Example:
The group $G \; = \; (\mathbb{Z}_{11}^*, \cdot)$. Notice that when elements are pared with their inverses, there is mirror symmetry in the group:

$$1 - 1, 2 - 6, 3 - 4, 5 - 9, 7 - 8, 10 - 10$$

This is a cyclic group. It has several generators, including 2:

$$\begin{aligned} 2^1 &= 2 \\ 2^2 &= 4 \\ 2^3 &= 8 \\ 2^4 &= 5 \\ 2^5 &= 10 \\ 2^6 &= 9 \\ 2^7 &= 7 \\ 2^8 &= 3 \\ 2^9 &= 6 \\ 2^10 &= 1 \end{aligned}$$

which are all the elements of $\mathbb{Z}_{11}^*$.

Finite Fields

A *field* F is a set D which has two operations $+, *$ defined on it. There are two groups, an additive group $(D, +)$ and a multiplicative group $(D^*, *)$, where $D^* = D - \{0\}$.

Example: Therefore $\mathbb{Z}_p$ is a field for prime p.

If n is not prime, $\mathbb{Z}_n$ is not a field. However, we can define a multiplicatively closed set:

$$\mathbb{Z}_n^* \; = \; \{a \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}$$

and then $(\mathbb{Z}_n^*, *)$ will be a group. You can check yourself that it satisfies closure and inverse. Basically, those are guaranteed by the $gcd(a, n) = 1$ property.

Chinese Remainder Theorem

The Chinese Remainder Theorem (CRT) gives a way to reconstruct a number from its values $(\bmod\ n_1), \ldots, (\bmod\ n_k)$ for some sequence of moduli $n_1, \ldots, n_k$. That is:

Theorem: Let $n_1, \ldots, n_k$ be a sequence of pairwise prime numbers and let $n = \prod n_i$. Pairwise prime means $gcd(n_i, n_j) = 1$ for every pair (n_i, n_j) of distinct numbers. Then for any sequence

$$r_1 \in \mathbb{Z}_{n_1}, \ldots, r_k \in \mathbb{Z}_{n_k}$$

There is a unique $r \in \mathbb{Z}_n$ such that

$$\begin{array}{ccc} r & = & r_1 (\bmod\ n_1) \\ \vdots & \vdots & \vdots \\ r & = & r_k (\bmod\ n_k) \end{array}$$

Proof:
We give a formula for r, and then show that that is the only value satisfying the above constraints. Let m_i be the multiplicative inverse of $(n/n_i)(\bmod\ n_i)$, that is:

$$m_i \tfrac{n}{n_i} (\bmod\ n_i) \ = \ 1$$

And notice that n/n_i is an integer which is $n_1 \cdots n_{i-1} n_{i+1} \cdots n_k$, so that

$$m_i \tfrac{n}{n_i} (\bmod\ n_j) \ = \ 0 \qquad \text{for} \qquad j \neq i.$$

Now consider

$$r \ = \ \textstyle\sum_{i=1}^{k} r_i m_i \frac{n}{n_i} (\bmod\ n)$$

Then

$$r (\bmod\ n_j) \ = \ r_j m_j \tfrac{n}{n_j} (\bmod\ n_j) \ = \ r_j (1)$$

because all other terms in the sum vanish ($(n/n_i)(\bmod\ n_j) = 0$ for $i \neq j$, and $m_j \frac{n}{n_j} (\bmod\ n_j) \ = \ (1)$ by definition. That proves that r satisfies all the identities.

To show that r is unique, there are few steps. First, for any r there are well-defined moduli, so that

$$f(r) \rightarrow (r_1, \ldots, r_k)$$

is a well-defined function. The CRT shows that for each sequence $(r_1, \ldots, r_k)$, there is an r, so the function f must be onto (covers its range).

Since f is onto, we can define an inverse $f^{-1}(r_1, \ldots, r_k)$ for every element of the range. Either these are all unique, or there must be multiple elements in each inverse. By counting, that would mean there were more elements in the domain than the range. But the number of elements in the domain is exactly n (number of elements in $\mathbb{Z}_n$), while the number of elements in the range is $n_1 \cdots n_k$ which is also n. Since domain and range are the same size, the function must be one-to-one, implying that r is unique. QED

Euler's Totient Function

The Euler Totient function $\phi(n)$ counts the number of elements in the multiplicative group $\mathbb{Z}_n^*$,

$$\phi(n) \;=\; |\mathbb{Z}_n^*|$$

We already know that for a prime p, $\phi(p) \;=\; p-1$. For a general n, the totient function depends on the prime facorization of n. Suppose

$$n \;=\; p_1^{k_1} \cdots p_t^{k_t}$$

then the value of the totient function is

$$\phi(n) \;=\; \prod_{i=1}^{t} p_i^{k_i-1}(p_i-1) \;=\; n\prod_{i=1}^{t}(1-1/p_i)$$

We wont give a proof here, but it is not hard to derive it using the inclusion/exclusion principle. An *intuitive* proof is that totient function counts numbers that are not divisible by any of the p_i's. The probability that a number is *not* divisible by p_i is $1-1/p_i$, and we claim that those probabilities are independent. So the number of elements that are not divisible by any of the p_i's is

$$n\prod_{i=1}^{t}(1-1/p_i)$$

Order of elements and subgroups

The *order* $\mathrm{ord}(a)$ of a group element a is defined as

$$\mathrm{ord}(a) \;=\; \min\{k \mid a^k = 1\}$$

Example: In $\mathbb{Z}_{11}^*$, we have already seen that 2 is a generator, which means it has order 10 (the size of the group). The element 4 has order 5, because its power sequence is $4^1 = 4$, $4^2 = 5$, $4^3 = 9$, $4^4 = 3$, and $4^5 = 1$.

Definition: A *subgroup* H of a group G is a subset of G which is also a group. The set of powers of an elements of G is always a subgroup of G. The size of the subgroup is the order of the element, that is:

$$H \;=\; \{a, a^2, \ldots, a^{\mathrm{ord}(a)} = 1\}$$

is a subgroup and its size is $\mathrm{ord}(a)$

Proposition: The order of an element $a \in G$ divides the order of the group G.

Proof: We will partition all the elements of G into subsets of size exactly $\mathrm{ord}(a)$. Thus $\mathrm{ord}(a)|\mathrm{ord}(G)$. First let H be the subgroup generated by a. Then the size of H is $\mathrm{ord}(a)$.

Now pick any element $b \in G$ which is not in H. Let bH be the set of all products of b and some element of H. This set is called a *coset*. We claim that $bH \cap H = \emptyset$. Suppose not, then there is some equation $bh_1 = h_2$ with h_1, h_2 both in H. But then $b = h_2 h_1^{-1}$ which implies $b \in H$, a contradiction.

Now pick another element $b_2 \in G$ which is neither in H nor bH. The set $b_2 H$ is another coset. By the above reasoning, $b_2 H$ is disjoint from H, and it also disjoint from bH. Suppose not, then $b_2 h_1 = bh_2$ for some $h_1, h_2 \in H$. Thus $b_2 = bh_2 h_1^{-1} = bh_3$ where $h_3 = h_2 h_1^{-1} \in H$. But that shows that $b_2 \in bH$, a contradiction.

If we continue building cosets by picking elements of G that are not in any existing cosets, eventually we will exhaust all the elements of G. At that point we will have partitioned G into H plus cosets of the form bH which all have size $\mathrm{ord}(a)$. Thus $\mathrm{ord}(a)$ must divide $|G|$.