9.15.2025: Math 122 Lecture 4 Notes

Vasily Krylov

1 Last Time

Last time, we defined the notion of a subgroup and a cyclic subgroup. Main theorem from last time: Every subgroup S of ($\mathbb{Z}$, +) is trivial or is equal to $\mathbb{Z}a$, where $a \in S$ is the smallest positive element in the subgroup.

2 Corollaries

Pick $a, b \in \mathbb{Z}$ nonzero and let $S = \mathbb{Z}a + \mathbb{Z}b = \{ra + sb : r, s \in \mathbb{Z}\}$. We can check that this is a subgroup of $\mathbb{Z}$, as $(ra + sa) + (r'a + s'b) = (r + r')a + (s + s')b \in S$, and we also observe that the group contains inverses of its elements and the identity element 0.

By the theorem from last time, $S = \mathbb{Z}d$ for some positive $d \in S$.

Cor. 1 For such d, the following hold:

1. $d|a, d|b$
2. if $k|a, k|b$, then $k|d$
3. $\exists r, s \in \mathbb{Z} : d = ra + sb$

The first two properties imply that $d = \gcd(a, b)$.

Proof. We start with the third statement. Since $d \in S$, then $d = ra + sb$ for some $r, s \in \mathbb{Z}$ (by definition of S).

Next, we prove the first statement. By definition, $a, b \in S = \mathbb{Z}d$, which implies $d|a, d|b$.

Finally, we prove the second property. We assume $k|a, k|b$, and we know $d = ra + sb$ for some r, s. We want to deduce that $k|d$. We can write $a = lk, b = l'k$, so $d = rlk + sl'k \implies k|d$. □

We just proved that $\exists r, s \in \mathbb{Z} : \gcd(a, b) = ra + sb$. This equality is important and will be necessary for the HW!

Example: $a = 10, b = 16 \implies \gcd(10, 16) = 2$. By the previous result, we should be able to write $2 = 10r + 16s$. We see that $2 = (-3) * 10 + 2 * 16$. This is not unique; there are infinitely many such presentations (think about why this is true).

Cor. 2 Elements a, b are coprime, i.e. $\gcd(a, b) = 1$, if and only if $\exists r, s \in \mathbb{Z} : ra + sb = 1$.

So far, we have considered the group $\mathbb{Z}a + \mathbb{Z}b$ and used the theorem to get interesting corollaries. Next, consider $\mathbb{Z}a, \mathbb{Z}b \subset \mathbb{Z}$, and let $S = \mathbb{Z}a \cap \mathbb{Z}b$. This is also a subgroup of $\mathbb{Z}$.

Lemma Let G be a group, with $S, S' \subset G$ subgroups. Then $S \cap S'$ is always a subgroup of G.

Proof. If $a, b \in S \cap S'$, then $a \in S, b \in S \implies ab \in S$, and similarly $a \in S', b \in S' \implies ab \in S'$, so $ab \in S \cap S'$. The same argument shows that $S \cap S'$ contains inverses, and $e \in S, e \in S' \implies e \in S \cap S'$. □

We know from the theorem that $\mathbb{Z}a \cap \mathbb{Z}b = \mathbb{Z}m$ for some $m \in \mathbb{Z}$. What is this m?

Example: Let $a = 4, b = 6$. What is $4\mathbb{Z} \cap 6\mathbb{Z}$? Answer: $12\mathbb{Z}$. We see that $12 = \text{lcm}(4, 6)$.

Lemma/Exercise For $a, m \in \mathbb{Z}$, $a|m \iff \mathbb{Z}m \subset \mathbb{Z}a$.

Cor. 3 We know $\mathbb{Z}a \cap \mathbb{Z}b = \mathbb{Z}m$ for some $m \in \mathbb{Z}$. We have that

1. $a|m, b|m$
2. $a|n, b|n \implies m|n$

These two properties imply that $m = \text{lcm}(a, b)$.

Proof. First, $\mathbb{Z}m \subset \mathbb{Z}a \implies a|m$ by the previous lemma. Similarly, $b|m$.

Next, we know that $a|n, b|n$, so by the lemma, $\mathbb{Z}n \subset \mathbb{Z}a, \mathbb{Z}n \subset \mathbb{Z}b$. This implies $\mathbb{Z}n \subset \mathbb{Z}a \cap \mathbb{Z}b = \mathbb{Z}m$, so $m|n$. □

Exercise: Using groups, prove that $\gcd(a, b) * \text{lcm}(a, b) = ab$. (In Artin's book).

Upshot: Every nontrivial subgroup of $\mathbb{Z}$ is $\mathbb{Z}a$. Further,

1. $\mathbb{Z}a + \mathbb{Z}b = \mathbb{Z}\gcd(a, b)$
2. $\mathbb{Z}a \cap \mathbb{Z}b = \mathbb{Z}\text{lcm}(a, b)$
3. $a|m \iff \mathbb{Z}m \subset \mathbb{Z}a$
4. $\gcd(a, b) = ra + sb(r, s \in \mathbb{Z}$
5. a, b coprime $\iff ra + sb = 1$ for some $r, s \in \mathbb{Z}$

3 Cyclic Subgroups

If $x \in G$, then $\langle x\rangle_G = \{x^k | k \in \mathbb{Z}\}$. Idea: from $\langle x\rangle_G$, can construct a subgroup $S \subset \mathbb{Z}$ that "knows" everything about $\langle x\rangle_G$. For $\langle x\rangle_G$, we consider the subgroup $S = \{k \in \mathbb{Z} : x^k = e\} \subset \mathbb{Z}$. Claim: this is a subgroup (proven later).

Example:

1. If $G = (\mathbb{R}^\times, \cdot), x = -1 \implies S = 2\mathbb{Z}$.
2. If $G = (\mathbb{Z}/n\mathbb{Z}, +), x = 1 \implies S = n\mathbb{Z}$.
3. If $G = S_3, x = (123) \implies S = 3\mathbb{Z}$.
4. If $G = (\mathbb{Q}, +), x = 2/3 \implies S = \{0\}$.

. We now prove that S is a subgroup.

Lemma Let S be the subset of $\mathbb{Z}$ associated with $\langle x \rangle_G$ as defined previously. Then

1. S is a subgroup of $\mathbb{Z}$
2. If $x^r = x^s$, then $r - s \in S$

Proof. Let $k, p \in S$. We want $k + p \in S$. Since $x^k = x^p = 1$, we have $x^k x^p = x^{k+p} = 1$. If $k \in S$, we want to show that $-k \in S$. We have that $x^k = 1$, so $1 = (x^k)^{-1} = x^{-k} \implies -k \in S$. Finally, $x^0 = 1 \implies 0 \in S$.

If $x^r = x^s$, then we claim that $r - s \in S$. Equivalently, $x^{r-s} = 1$. To show this, we see that $x^r x^{-s} = x^0 = 1 \implies x^{r-s} = 1$. If $r - s \in S$, then $x^{r-s} = 1 \implies x^{r-s}x^s = x^r = x^s$. □

Remark (Cancellation Law) In general, for $a, b, c \in S$ with S a group, $ab = ac \iff b = c$.

Proposition (Classification of Cyclic Subgroups).

1. Case 1: S is nontrivial, i.e. $S = \mathbb{Z}n$. Then $\langle x \rangle_G = \{1, x, x^2, \ldots, x^{n-1}\}$ with all of these distinct, and the multiplication rule is the same as in $(\mathbb{Z}/n\mathbb{Z}, +)$. (Later, we will see that these groups are isomorphic to one another). In this case, we say ord$(x) = n$.
2. Case 2: $S = \{0\}$. Then $\langle x \rangle_G = \{\ldots, x^{-1}, 1, x, x^2, x^3, \ldots\}$, where all of these are distinct, and this is identified with the group $(\mathbb{Z}, +)$. In this case, we say ord$(x) = \infty$.

Proof. Case 1: $S = n\mathbb{Z}$, so by part 2 of the lemma ($x^r = x^s \iff r - s \in S$), $\{1, x, x^2, \ldots, x^{n-1}\}$ are distinct. If $x^r = x^s$ for some $r, s \in \{0, \ldots, n-1\}, r \geq s$, then $x^r = x^s \iff r - s \in S = n\mathbb{Z}$. We have that $r - s \in \{0, \ldots, n-1\}$, so we must have that $r - s = 0 \implies r = s$.

We already know $\langle x \rangle_G = \{1, x, x^2, \ldots, x^{n-1}\}$, and $x^{nk} = 1$ for $k \in \mathbb{Z}$. For $a, b \in \{0, \ldots, n-1\}$, $x^a x^b = x^{a+b} = x^{a+b}x^{-nk} = x^{a+b-nk}$, which is exactly how the group law is defined in $\mathbb{Z}/n\mathbb{Z}$.

Case 2 is left as an exercise. □