Lecture Notes for Abstract Algebra: Lecture 3

1 The integers

1.1 The integers

The set of integers is denoted by $\mathbb{Z}$ and the naturals by $\mathbb{N}$. We take $\mathbb{N} = \{1, 2, 3, \dots\}$.

Well ordering principle: Any nonempty set of non-negative integers have a smallest element.

Proposition 1. *(Division algorithm) If a, b are integers with $b > 0$, there exist integers q and r with $0 \leq r < b$ such that $a = bq + r$.*

Proof. Consider the non-empty set $S = \{a - bk \,|k \in \mathbb{Z} \text{ and } a - bk \geq 0\}$ and let r be the smallest element of S. Then $r = a - bk$ for some integer k and $r \geq 0$. If $r = a - bk \geq b \Rightarrow a - b(k-1) = r' \in S$ and $r' < r$, which contradicts the fact that r is the smallest element in S. □

Definition 2. Let a, b integers (not both zero). We say that a divides b if there exist an integer c such that $b = ca$. We write that $a|b$. The greatest common divisor d of two integers a, b is a positive number satisfying:

1. $d|a$ and $d|b$.
2. if d' is an integer such that $d'|a$ and $d'|b$. Then $d'|d$.

The number d is denoted $(a, b) = d$ or $gcd(a, b) = d$.

Remark 3. The relation $(\mathbb{Z}, |)$ is not symmetric ($x|y$ and $y|x \;\; \Rightarrow x = \pm y$).

Definition 4. Let $n \geq 1$. We say that a is congruent to b mod n, written

$$a \equiv b \bmod n, \text{ if and only if } n|a - b.$$

The relation $\equiv$ is an equivalent relation on $\mathbb{Z}$ and the associated partition is say to determine the congruence classes $\bar{x}$ mod n. The multiplication and addition on $\mathbb{Z}$ descend to operations on the quotient $\mathbb{Z}/\sim$ and we have the following properties:

(a) The addition $\overline{x+y} = \bar{x} + \bar{y}$ has a neutral element $\bar{0}$.

(b) Every element $\bar{x}$ has an inverse $\overline{-x}$.

(c) We respect associativity $\bar{x} + \overline{y+z} = \overline{x+y} + \bar{z} = \overline{x+y+z}$.

Proposition 5. *Let a, b integers (not both zero). The greatest common divisor $d = gcd(a, b)$ exist, is unique and can be expressed as a linear combination $am + bn = d$ for some integers $m, n \in \mathbb{Z}$.*

Proof. Consider the non-empty set $S = \{ax + by \,|\, x, y \in \mathbb{Z} \text{ and } ax + by > 0\}$ and denote by $d' > 0$ the smallest element of S. The element d' is a linear combination $d' = am + bn$. Also:
Use the division algorithm for a and d'. If $a = d'q + r$, then $r = a - q(ma + nb) < d'$ cannot be an element of S and therefore $r = 0$. We can do the same for b and obtain that d' divides both a and b.
Now if d'' is a common divisor of a and b, we will have that d'' divides also any integral linear combination of a, b. In particular $d''|d'$.
Conclusion: $d = d'$ is the $gcd(a, b)$. □

Euclid's algorithm: The $\gcd(a, b) = \gcd(b, r)$, where $a = bq + r$ and $0 \leq r < b$.

Example 6. The $\gcd(24567, 2456) = \gcd(2456, 7) = \gcd(7, 6) = 1$.

Definition 7. We say that a, b are relatively prime if $\gcd(a, b) = 1$ or equivalently, if there are suitable $m, n \in \mathbb{Z}$ such that $1 = ma + nb$.

Definition 8. The Euler function $\phi(n)$ denotes the numbers of integers in the set $\{1, 2, \ldots, n\}$ that are relatively prime to n.

Example 9. For instance $\phi(8) = 4$ since, in the set $\{1, 2, 3, 4, 5, 6, 7, 8\}$, the numbers $1, 3, 5$ and 7 are relatively prime to 8.

Definition 10. We say that a natural number $p > 1$ is prime if it is only divisible by 1 and itself.

Lemma 11. *(Euclid's lemma) If a prime number p divides a product ab, where $a, b \in \mathbb{Z}$, then either $p|a$ or $p|b$.*

Proof. Suppose that p divides ab and does not divide a. Then, the numbers a and p are relatively prime and there exist therefore integers x, y such that

$$ax + py = 1 \Rightarrow (ax + py)b = b \Rightarrow abx + pby = b.$$

Since the number p divides the product abx and the term pby, it must also divide the sum $abx + pby = b$. □

Theorem 12. *(Fundamental theorem of Arithmetic) Any integer $n > 1$ can be written in the form $n = p_1^{n_1} \ldots p_k^{n_k}$, where p_i are distinct primes and $n_i \geq 1$. The factorization is unique, except possible for the order of the factors.*

Proof. Existence of prime factorization using Induction: It must be shown that every integer greater than 1 is either prime or a product of primes. First, 2 is prime. Then, by induction, assume the theorem is true for all numbers in the range $1 < x < n$. If n is prime, there is nothing more to prove. Otherwise, the number n is the product of two numbers $n = ab$ in the range $1 < a, b < n$. Since both numbers a and b can be written as product of primes by induction hypothesis, the assertion is true also for the product $n = ab$.
Uniqueness using Infinite Descent: If there is a number n with two different prime factorization, say $n = p_1 p_2 \dots p_k = q_1 q_2 \dots q_j$, then, by Euclid's lemma, the prime p_1 will divide some of the q_i. But all q_i are prime numbers, hence they must be equal and there is a prime, for example q_1, such that $q_1 = p_1$. If we simplify the expression by p_1, we get a smaller number with two different prime factorizations $n/p_1 = p_2 \dots p_k = q_2 \dots q_j$. □

1.2 Mathematical Induction and Infinite Descent

Induction: In order to prove that a property $P = P(n)$ **is true for all natural numbers** $n \geq n_0$, we can prove:

1. $P(n_0)$ is True.
2. For all $k \geq n_0$, $P(k)$ is True $\Rightarrow P(k+1)$ is also True.

In this way for example, if n_0 where to be $n_0 = 10$ and we will have proven steps (1) and (2), then we will have the validity of P for n_0 as well as the chain of implications:

$$P(n_0) \text{ is True} \Rightarrow P(n_0+1) \text{ is True} \Rightarrow P(n_0+2) \text{ is True} \Rightarrow \dots,$$

that guarantees the validity of P for all natural numbers $n \geq n_0$.

Alternative or strong induction: In order to prove a property $P = P(n)$ for all natural numbers $n \geq n_0$, we can prove:

1. $P(n_0)$ is True.
2. For all $k \geq n_0$, $P(k_0), \dots, P(k)$ are True $\Rightarrow P(k+1)$ is also True.

Infinite Descent: In order to prove that a property $P = P(n)$ **is not satisfied by any positive integer**, we can prove:

1. If the property P is true for the integer $n_0 > 0$, there exist $n_1 < n_0$, such that n_1 also satisfies P.

Practice Questions:

1. Let p be a prime number. Prove that $\sqrt{p}$ is irrational.

2. Prove using induction (or otherwise) that for $\alpha \in \mathbb{R}$, such that $\alpha > -1$, we have:

$$(1+\alpha)^n \geq 1 + \alpha n \qquad \forall n \in \mathbb{N}.$$

3. Prove the following properties for the function ϕ of Euler:

1. $\phi(p) = p - 1$.
2. $\phi(p^k) = p^k - p^{k-1}$.
3. $\phi(nm) = \phi(n)\phi(m)$ for positive integers m, n with $\gcd(m, n) = 1$.