Introduction to Algebra

Shu Sasaki

26th January 2024

1 Introduction

What this course is about?

We axiomatise (=express a theory as a set of axioms) what we know very well (integers, GCD, LCM, Euclid's algorithm, modular arithmetic, complex numbers, polynomials etc), i.e., spot 'common denominators (structures)' of mathematical concepts we have learned (or will have learned), and build/extrapolate a theory out of them. For example, we will see that the set $\mathbb{Z}$ of integers and the set of polynomials in one variable with rational coefficients have the same 'algebraic' structure– they are examples of what we call rings. Similarly, the set of rational numbers (with addition, subtraction, multiplication and division) is 'similar (algebraically)' to the set of Laurent series $\sum_{n\geqslant N} c_n X^n$ in X (where N is an integer) with rational coefficients– they are examples of fields.

This means that if we can prove a statement about a ring (a set that satisfies a bunch of axioms as $\mathbb{Z}$ does for example), then the assertion would hold for any ring we find. Conversely, any abstract statement can always be specialised to examples. In my opinion, algebra is a concrete subject, contrary to the prevailing opinion amongst those who haven't seen the magic.

Related modules: NSF, Number Theory, Group Theory, Cryptography...

Books:
R. Allenby, *Rings, Fields and Groups: Introduction to Abstract Algebra*, Butterworth-Heinemann,
P. Cameron, *Introduction to Algebra*, Oxford University Press,
B. Hartley and T. O. Hawkes, *Rings, Modules and Linear Algebra*, Chapman and Hall,
M. A. Armstrong, *Groups and Symmetry*, Springer-Verlag,
D. J. H. Garling, *Galois theory*, Cambridge University Press,
M. Artin, *Algebra*, Prentice Hall,
NRICH, *Development of Algebra*, https://nrich.maths.org/6485, https://nrich.maths.org/6546

2 Revising bits and bobs from NSF

By $\mathbb{Z}$, we mean the set of integers. By a non-negative (resp. positive) integer, we mean an integer $\geqslant 0$ (resp. $\geqslant 1$). You will never hear 'natural numbers' from me.

2.1 Integer division

Proposition 1. Let a and b be integers. Assume that $b > 0$ (but a can be negative). Then there exist integers q and r such that

$$a = bq + r$$

with $0 \leq r < b$. Moreover, q and r are unique, i.e., if (q_1, r_1) and (q_2, r_2) are two pairs of integers satisfying $a = bq_1 + r_1$ with $0 \leq r_1 < b$ and $a = bq_2 + r_2$ with $0 \leq r_2 < b$ respectively, then $q_1 = q_2$ and $r_1 = r_2$.

Remark. The numbers q and r are referred to as the quotient and remainder when a is divided by b.

Examples.

$a = 100, b = 7$: $100 = 7 \times 14 + 2$.

$a = -100, b = 7$: $-100 = 7 \times (-15) + 5$. Note that q is forced to be a negative integer for the reminder to be in the range $[0, 7)$!

$a = 2, b = 3$: $2 = 3 \times 0 + 2$. It is possible for q to be zero!

$a = -2, b = 3$: $-2 = 3 \times (-1) + 1$.

Proof of the proposition. To see the existence of q and r, let S denote the set of integers of the form $a + sb \geqslant 0$ where s ranges over $\mathbb{Z}$.

We firstly show that S is non-empty. If $a \geqslant 0$, then $a = a + 0b$ defines an element of S; on the other hand, if $a < 0$, then $a + (-a)b = a(1 - b) = (-a)(b - 1) \geq 0$ and therefore defines an element of S (note that b assumed to be a positive integer, therefore $b - 1 \geqslant 0$). Since S is non-empty, it makes sense to take the smallest element, say r, of S. By definition, In this case, r is of the form $a + (-q)b \geq 0$ for some integer q.

We show that $r < b$. If $r \geqslant b$, then $0 \leqslant r - b = a - (q + 1)b < a - bq = r$ and $r - b$ would define an element of S that is strictly smaller than r. This contradicts the minimality of r. Therefore $r < b$.

The uniqueness is left as an exercise! □

Definition. Let a and b be integers. We say that a divides b if and only if there exists an integer c such that $b = ac$.

Remark. Note that a and b can be negative; in fact a can be zero! According to the definition, for the statement 'zero divides b' to hold, there has to be an integer c such that $b = 0 \times c$; but the RHS is nothing other than 0, forcing b to be zero! In other words, the only integer zero divides is zero itself! We are only considering 'zero divides zero' and are NOT trying to make sense of $\dfrac{b}{a} = \dfrac{0}{0}$.

Examples.

Every integer, including zero, divides 0. Indeed, $0 = a \times 0$.

If a and b are non-negative integers such that a divides b as well as b divides a, then $a = b$. This seems 'obvious' but proving this formally requires a bit of work: Firstly, suppose $a = 0$. It then follows, by the remark above and the assumption, a divides b, that $b = 0$. So $a = b$ holds. Swapping the roles, we can also prove, if $b = 0$, then $a = b(= 0)$. Having dealt with these two degenerate case, we may now assume that a and b are both positive integers. By assumption, there exist integers r and s such that $a = rb$ and $b = sa$– since a and b are positive integers, r and s are positive integers. We see that $a = rb = r(sa) = rsa$. Because a is non-zero, we may divide this through and get $rs = 1$. As we know r and s are positive integers, we deduce $r = 1$ and $s = 1$. It therefore follows that $a = rb = b$.

2.2 GCD and Euclid's algorithm

Definition. Let a and b be integers. A common divisor of a and b is a *non-negative* integer r with the property that r divides a and r divides b. We call a common divisor r of a and b the high common factor, or the greatest common divisor (GCD) in this course, if any other common divisor is smaller than r, i.e. if s is another common divisor of a and b, then $s < r$ holds.

Remark (important). The GCD of a and b, written often as $\gcd(a, b)$, is defined to be a non-negative integer, even if a and b are negative.

Example.
$a = 12, b = 18$: $\gcd(12, 18) = 6$.
$a = 12, b = -18$: $\gcd(12, -18) = 6$.
If a is a non-zero integer, then $\gcd(a, 0) = a$ (see below as to why).

Remark (not so important but useful to know) For $r = \gcd(a, b)$ to be 'the greatest', it is decreed, as part of the definition of GCD, that if s is a common divisor of a and b, then $s < r$ needs to hold. In fact, $s < r$ is equivalent to:

Proposition 2. s divides r.

Example. $a = 50, b = 100$. Then $r = \gcd(50, 100) = 50$. For example, $2, 5, 10, 25$ are all common divisors s of 50 and 100, and they all divide r.

Remark. If we know the Fundamental Theorem of Arithmetic– any positive integer can be written as a product of primes numbers, and this product expression is unique up to recording of the factors, then it is possible to completely unravel the common divisors, and this proposition follows immediately. A lowbrow approach requires the Bezout's identity– if p and q are integers, there exist integers x and y such that $px + qy = \gcd(p, q)$.

Proof. Firstly, if $s = 0$, then it forces both a and b to be 0, which in turn forces $r = 0$. But this contradicts the assumption that s is 'another' common divisor. So we may assume $s > 0$ (note that s is assumed to be non-negative). Since $s < r$, we see that r is also positive. It then follows that $r = sq + \gamma$ for some integers $q(> 1)$ and $0 \leq \gamma < s$. It suffices to see $\gamma = 0$.

Firstly, $a = rp$ and $b = rq$ for some integers. Since r is GCD, we see that p and q have no common divisor (i.e. $\gcd(p, q) = 1$); indeed, if it did have a common divisor, then multiplying r by that common divisor (necessarily a positive integer) would yield a common divisor greater than r (which contradicts r being the 'greatest'). On the other hand, $a = (sq + \gamma)p$ and $b = (sq + \gamma)q$ and it follows (from the assumption that s is also a common divisor of a and b) that s divides both γp and γq. Since $\gcd(p, q) = 1$, it follows from Bezout's identity that there exist integers x, y such that $px + qy = 1$. Since $\gamma px + \gamma qy = \gamma$ and the LHS is divisible by s, the RHS, γ, is also divisible by s. However, since $0 \leq \gamma < s$, the only possibility left is that $\gamma = 0$. □

Definition. We say that a pair of integers a and b are coprime, if $\gcd(a, b) = 1$.

Example. 2 and 5 are coprime, but 2 and 4 are not comprime.

Definition. Let a and b be as above. A positive integer s is a common multiple of a and b if a divides s and b divides s. A common multiple of a and b is the least common multiple of a and b, $\mathrm{lcm}(a, b)$, if it is smaller than any other common multiple, in the sense that if s is another common multiple of a and b, then $r < s$.

Analogous to the case of GCD, we know:

Proposition 3. r divides s.

Proof. Observe, firstly, that there exist q and $0 \leq \gamma < r$ such that $s = rq + \gamma$. It suffices to show that $\gamma = 0$. By definition, a divides s, hence it also divides γ (as a divides r). Similarly, b divides s, therefore b divides γ. Combining, both a and b divide γ. This implies $\gamma = 0$ as if γ was non-zero, then it would mean that γ is a common multiple of a and b but is also smaller than r (by definition); and this contradicts the minimality of $r = \mathrm{lcm}(a, b)$. □

Example.
$a = 12, b = 18$: $\mathrm{lcm}(12, 18) = 36$.

Proposition 4. Let a be a non-negative integer. Then $\gcd(a, 0) = a$.

Proof. Let $\gamma = \gcd(a, 0)$. By definition, γ divides a; this means that there exists an integer λ such that $a = \gamma\lambda$. On the other hand, because a divides both a (itself) and 0 (as $0 = a0$), a is a common divisor of a and 0, and therefore a divides γ (Proposition 2) and we may write $\gamma = a\mu$ for some integer μ. Plugging this into $a = \gamma\lambda$, we obtain $a = a\lambda\mu$. From this equality, we deduce that if a is zero, then $\gamma = 0\mu = 0$; if, on the other hand, a is non-zero, then $\lambda\mu = 0$, i.e. $(\lambda, \mu) = (1, 1)$ or $(-1, -1)$. However, since both γ (by definition) and a (by assumption) are non-negative, $(\lambda, \mu) = (1, 1)$, i.e., $\gamma = a$. □

Euclid's algorithm is a very useful tool to compute gcd.

Example.

$\gcd(198, 78) = 6$.

$$\begin{aligned} 198 &= 78 \cdot 2 + 42 \\ 78 &= 42 \cdot 1 + 36 \\ 42 &= 36 \cdot 1 + 6 \\ 36 &= 6 \cdot 6 + 0 \end{aligned}$$

$\gcd(-78, 198) = 6$

$$\begin{array}{rcl} -78 & = & 198\cdot(-1)+120 \\ 198 & = & 120\cdot 1+78 \\ 120 & = & 78\cdot 1+42 \\ 78 & = & 42\cdot 1+36 \\ 42 & = & 36\cdot 1+6 \\ 36 & = & 6\cdot 6+0 \end{array}$$

In fact,

Lemma 5. If a and b are (positive) integers, then $\gcd(a,b) = \gcd(-a,b) = \gcd(a,-b) = \gcd(-a,-b)$.

Proof (non-examinable). Let us prove the first quality. If $\gcd(a,b) = 0$, then it forces $a = b = 0$. In this case, $\gcd(-a,b) = 0$. We may therefore assume that $\gcd(a,b) > 0$ (note that $\gcd(a,b)$ is defined to be non-negative). Since $\gcd(a,b)$ divides a and b, it also divides $-a$ and b. Therefore $\gcd(a,b)$ is a common divisor of $-a$ and b. By the Proposition ? above, $\gcd(a,b)$ divides $\gcd(-a,b)$. Swapping the role of $\gcd(a,b)$ and $\gcd(-a,b)$, we may also conclude that $\gcd(-a,b)$ divides $\gcd(a,b)$. Combining (together with the fact that they are both positive integer), $\gcd(a,b) = \gcd(-a,b)$. □

Euclid's algorithm is based on the following proposition– by the lemma above, we can always make 'b' positive when it comes to computing $\gcd(a,b)$.

Proposition 6. Let a and b be integers and suppose that $b > 0$ and $a = bq+r$ for some uniquely determined integers q and $0 \leqslant r < b$. Then $\gcd(a,b) = \gcd(b,r)$.

Proof. Let $\gamma = \gcd(a,b)$ and $\lambda = \gcd(b,r)$.

Firstly, suppose that $\gamma = 0$. Since γ divides a and b, the assumption forces both a and b to be zero. This in turn forces $r = 0$ and therefore $\lambda = 0$.

We may henceforth assume that γ is non-zero; since GCD is assumed to be non-negative integer, it is forced that $\gamma > 0$. It then follows that $\lambda > 0$. Indeed, if $\lambda = 0$, an argument similar to the one above would force $\gamma = 0$ which contradicts the running assumption $\gamma > 0$.

We claim that λ divides γ. Since γ divides a, and b, by definition, it follows that γ divides $a - bq = r$. Combined the fact that γ divides b by definition, γ makes a common divisor of b and r. By Proposition 2, we may therefore conclude that λ divides γ.

We also claim that γ divides λ. Since λ divides b, and r, by definition, it follows that λ divides $bq + r = a$. Combined with the assumption that λ divides b, λ defines a common divisor of a and b. By Proposition 2 (again!), we conclude that γ divides λ.

Since γ divides λ, as well as λ divides γ, it follows that $\gamma = \lambda$. □

2.3 Euclid's algorithm extended

Theorem 7 (Bezout's identity). Let a and b be integers. Then there exist integers r and s such that $ar + bs = \gcd(a,b)$. These integers r and s can be found from Euclid's algorithm.

Proof (non-examinable). Let S be the set of integers of the form $a\lambda + b\mu$, where λ and μ range over $\mathbb{Z}$. Since both a and b lie in S, the set is non-empty and let γ denote the smallest *non-negative* integer in S. We show that $\gamma = \gcd(a, b)$.

Since $\gcd(a, b)$ divides both a and b, it divides any integer linear combination of a and b (i.e. any element of S). In particular, $\gcd(a, b)$ divides γ and consequently $\gcd(a, b) \leqslant \gamma$ (since both $\gcd(a, b)$ and γ are non-negative integers).

Let $a = \gamma q + r$ for some integer $0 \leqslant r < \gamma$. Since γ is an element of S, so is r. If r is non-zero, it contradicts the minimality of γ. Therefore $r = 0$, in other words, γ divides a. We may similarly prove that γ divides b. Combining, γ divides both a and b, i.e. γ is a common divisor of a and b. Therefore $\gamma \leqslant \gcd(a, b)$.

As we have shown that $\gcd(a, b) \leqslant \gamma$, as well as $\gamma \leqslant \gcd(a, b)$, it follows that $\gamma = \gcd(a, b)$. □

Examples. Looking at the steps computing $\gcd(198, 78) = 6$ in the reverse order,

$$\begin{aligned} 6 &= 42 - 1 \cdot 36 \\ &= 42 - 1 \cdot (78 - 1 \cdot 42) \\ &= 2 \cdot 42 - 1 \cdot 78 \\ &= 2 \cdot (198 - 2 \cdot 78) - 1 \cdot 78 \\ &= 2 \cdot 198 - 5 \cdot 78 \end{aligned}$$

so $\gcd(198, 78) = 6 = 2 \cdot 198 + (-5) \cdot 78$.

Looking at the steps computing $\gcd(-78, 198) = 6$ in the reverse order,

$$\begin{aligned} 6 &= 42 - 1 \cdot 36 \\ &= 42 - 1 \cdot (78 - 1 \cdot 42) \\ &= 2 \cdot 42 - 1 \cdot 78 \\ &= 2 \cdot (120 - 1 \cdot 78) - 1 \cdot 78 \\ &= 2 \cdot 120 - 3 \cdot 78 \\ &= 2 \cdot 120 - 3 \cdot (198 - 1 \cdot 120) \\ &= 5 \cdot 120 - 3 \cdot 198 \\ &= 5 \cdot (1 \cdot (-78) + 1 \cdot 198) - 3 \cdot 198 \\ &= 2 \cdot 198 - 5 \cdot (-78) \end{aligned}$$

so $\gcd(198, -78) = 6 = 2 \cdot 198 + 5 \cdot (-78)$.

Subtexts (evidently non-examinable). In this section, we set off by leaning that '$\mathbb{Z}$ is a Euclid domain'. The set S in the proof of Bezout is, by definition, an 'ideal' of the ring (actually a domain) $R = \mathbb{Z}$; and 'γ divides $\gcd(a, b)$' sees the standard technique of proving that $\mathbb{Z}$ is a principal ideal domain. It is because of the comparative 'easier' direction– '$\gcd(a, b)$ divides γ' – that $\mathbb{Z}$ is a Bezout domain. The FTA below sees $\mathbb{Z}$ is a UFD; note however that Bezout is not necessarily a UFD.

2.4 Prime numbers

A prime number is (defined to be) a positive integer which can only be divided by 1 or itself (i.e. no *proper* factors). From the viewpoint of theory of algebra, the right definition of a prime number is that it is a positive integer p which satisfies the property that if p divides the product ab of integers a and b (not necessarily positive), then p divides either a or b. We will go with the standard definition though.

Remark (non-examinable, though it really touches upon the essence of this course). In $\mathbb{Z}$, the only elements that divide 1 are 1 and -1; and they are called *units* of $\mathbb{Z}$ (we will learn more about this towards the end of the course).

We say that an element π of $\mathbb{Z}$ (i.e. π is an integer) is *irreducible* if the following condition holds: if $\pi = ab$ (for a, b in $\mathbb{Z}$), then either a, or b, is a unit. For example, a prime number p in the standard sense (e.g. $2, 3, 5, \ldots$), is irreducible in $\mathbb{Z}$. In fact, the negative integer $-p$ is also irreducible, by definition.

On the other hand, we say that an element π is *prime* if the following condition holds: if π divides ab, then either π divides a, or π divides b; this is the definition that pins down what it means for an integer to be prime.

If π is prime, then it is irreducible. Let π be a prime element of $\mathbb{Z}$, and suppose that $\pi = ab$. Since π divides π, it follows that π divides ab. Since π is assumed to be prime, π divides either a, or b. Without loss of generality, suppose that π divides a. Let $a = \pi c$ for some integer c. Feeding this back into $\pi = ab$, we deduce $\pi = \pi bc$, i.e. $\pi(bc - 1) = 0$. Since π is non-zero, and there is no 'zero-divisor', $bc - 1$, i.e. $bc = 1$. Hence b is a unit. Similarly, if π divides b, one can deduce a is a unit. In both cases, a or b is a unit, hence π is irreducible.

To prove the converse, we use Bezout's identity. Let π be an irreducible element of $\mathbb{Z}$. Suppose that π divides ab for a pair of integers a and b. Suppose furthermore that π does not divide a. The assertion– π is prime– follows if we establish that π divides b.

We claim that $\gcd(a, \pi) = 1$. To see this, let $\gamma = \gcd(a, \pi)$. Since γ divides π, it follows from the irreducibility of π (and the assumption that π does not divide a) that γ is a unit. Since γ is by definition positive, $\gamma = 1$. It then follows from Bezout that there exist integers r and s such that $ar + \pi s = 1$. Multiplying the equality through by b, we obtain $b = b(ar + \pi s)$. The both terms on the RHS are divisible by π (π divides ab by assumption!). It therefore follows that π divides b, as desired.

Theorem 8. (The Fundamental Theorem of Arithmetic) Every integer can be expressed as the product $(-1)^r \prod_p p^{r_p}$ of prime numbers (in the standard sense), where r is an element of $\{\pm 1\}$ and, for every prime number p, r_p is a non-negative integer. Furthermore, the expression is unique up to re-ordering of the prime factors.

Proof. See Example Sheet. □

Remarks.

The FTA is the reason why you often here 'the prime numbers are the building blocks of the (whole) numbers'.

You might find discussions of T. Gowers (a Fields medalist):

https://gowers.wordpress.com/2011/11/13/why-isnt-the-fundamental-theorem-of-arithmetic-obvious/

https://gowers.wordpress.com/2011/11/18/proving-the-fundamental-theorem-of-arithmetic/

enlightening.

What else do we know about prime numbers?

Proposition. There are infinitely many prime numbers.

Proposition. There are infinitely many prime numbers congruent to -1 mod 4.

Proof. Example Sheet. □