Abstract Algebra II Lecture Notes

Simon Xiang

These notes were transcribed from my physical lecture notes for the Spring 2020 undergraduate/graduate section of Abstract Algebra II (Math 4510) at UNT, taught by Dr. Shepler, which I took while I was at TAMS. Source files: https://git.simonxiang.xyz/math_notes/files.html

Contents

1 January 13, 2020

Nostalgic notes...

Definition 1.1. A number $\alpha \in \mathbb{R}$ is said to be **constructable** if we can construct a line segment of length $|\alpha|$ in a finite number of steps using only a straightedge and compass.

Theorem 1.1. *If α, β are constructable, then so are $\alpha + \beta$ and $\alpha\beta$.*

Proof. We show α, β are constructable for $\alpha, \beta > 0$ (refer to [Fra03] §32, page 294). Assume α and β have been constructed. Construct a line segment B to the line containing A such that it is parallel to the line sgment from P (of length 1) to A containing B (in three steps). This yields congruent triangles $\Delta OAP, \Delta OQB$ respectively, where Q is the intersection of $\overline{OA}$ with the line parallel to $\overline{PA}$ containing B. Therefore $\overline{PA}$ is parallel to $\overline{BQ}$, and since ΔOAP and ΔOQB are congruent, $\|\overline{OA}\|/\|\overline{OP}\| = \frac{\|\overline{OQ}\|}{\|\overline{OB}\|}$. So $\alpha/1 = \|\overline{OQ}\|/\beta$, which implies $\|\overline{OQ}\| = \alpha \cdot \beta$ and is constructable. ⊠

Similar results with α/β ($\beta \neq 0$) and $\alpha - \beta$ imply the following theorem.

Theorem 1.2. *The set of all constructable numbers in $\mathbb{R}$ form a field.*

Some ancient questions answered:

(1) It is impossible to construct a cube with double the volume of another. If α is constructed, consider a cube with volume α^3. Then it is impossible to construct a β such that cube having length β satisfies $\text{vol}(\beta^3) = 2\alpha^3$.
(2) It is impossible to square the circle. Given a circle with area A, we cannot find a square with area A (constructed with a compass and straightedge).
(3) It is impossible to trisect an angle using only a compass and straightedge. (But you can biset an angle in a finite amount of steps!)

Some formulas for roots of polynomials in a single variable.

- **QUADRATIC:** Known since approximately 1000 BC.
- **CUBIC**: Known.
- **QUARTIC**: Use a flowchart.
- **QUINTIC**: There is no POSSIBLE quintic formula. The reason is that A_5 is simple. These are all connected through field extensions and Galois theory.

2 January 15, 2020

We want coefficients for polynomials from $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/5\mathbb{Z}$, etc.

Example 2.1 (Freshman's dream)**.** If the coefficients are from $\mathbb{Z}/5\mathbb{Z}$, then $(x+y)^5 = x^5 + y^5$.

Definition 2.1. For a ring R, then $R[x] = \{a_0 + a_1x + a_2x^2 + \cdots a_mx^m \mid m \geq 0 \text{ for all } a_i \in R\}$. $R[x]$ is known as the set of **polynomials over** R. A polynomial has **degree** m, **leading coefficient** a_m, and **leading term** a_mx^m.

Example 2.2. For $f(x) = 5$, $f(x)$ is a polynomial in $\mathbb{R}[x]$ and has degree 0.

Note. The zero polynomial $f(x) = 0$ has degree undefined *by convention.* (Some authors define it as having degree -1 or $-\infty$).

Note. Don't regard your polynomials as functions in order to check that two polynomials are the same! For example, $f(x) = x, h(x) = x^3$ are both polynomials in $\mathbb{Z}/3\mathbb{Z}[x]$ (the polynomials of the ring $\mathbb{Z}/3\mathbb{Z}$). If we were to view them as functions, we get the same function! If $f, h \colon \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$, then for every $x \in \mathbb{Z}/3\mathbb{Z}$, $f(x) = h(x)$. As functions, they are equivalent. However $f \neq g$ as polynomials. Two polynomials are **equal** iff for every x_i, the coefficients agree for every $i \geq 0$.

Theorem 2.1. *The set of polynomials over a ring R, known as $R[x]$, form a ring under addition and multiplication of polynomials.*

(1) $0_{R[x]} = 0_R$, the zero polynomial.
(2) We view R as a subset of $R[x]$ in this way: for every $\alpha \in R$, there exists a constant polynomial such that $f(x) = \alpha$.
(3) R is commutative implies that $R[x]$ is commutative.
(4) R has unity 1_R implies that $R[x]$ has unity $1_{R[x]} = 1$.

Theorem 2.2 (Evaluation homomorphism)**.** *For a ring R and some $a \in R$, we define the function $\phi_a \colon R[x] \to R$ by $\phi_a \colon R[x] \to R$ by $\phi_a(f(x)) = f(a) \in R$. Then ϕ_a is a ring homomorphism.*

For $a = 0$, the evaluation homomorphism $\phi_0 \colon f(x) \mapsto f(0)$ picks off constant terms of any polynomial.

Example 2.3. Let $R = \mathbb{Z}/6\mathbb{Z}$. For $f(x) = \overline{2}x + \overline{3}$, $h(x) = \overline{3}x^2 + \overline{1}$, we have $\deg(f \cdot h) = \overline{6}x^3 + \overline{9}x^2 + \overline{2}x + \overline{3} \equiv \overline{3}x^2 + \overline{2}x + \overline{3} \neq 2 \neq 1 + 3 = \deg(f) + \deg(h)$. This ring messed up because of zero divisors, zero divisors bad.

Lemma 2.1. *If R has no zero divisors, then* $\deg(fg) = \deg(f) + \deg(g)$.

References

[**Fra03**] John Fraleigh. *A First Course in Abstract Algebra, 7th edition*. 2003.