

Revision Notes: a3 (Algebra).

Adam D.P. Booth

FHS Part(I)

Notation:

Lectures are the HT02 series given by Dr. Neumann. Lecture $n.m$ is the m^{th} lecture in week n . Lecture notes refer to the notes distributed by Dr. Priestley in TT02 and available on the institute website.

NST refers to Neumann, P.M., Stoy, G.A., Thompson, E.C. *Groups and Geometry*.

Green refers to Green, J.A., *Groups and sets*.

Stewart refers to Stewart, I. *Galois Theory*.

S_n is the symmetric group on n letters.

$\mathbb{F}[x]$ is the set of polynomials with coefficients in \mathbb{F}

1 Group actions.

Lectures: 2.1-4.1; NST: pp. 30-60, alternatively; Green: pp. 62-6, 73-83.

An action of a group, G , on a set, S , is a map $\mu : S \times G \rightarrow S$ such that for all $x \in S$, $g, h \in G$, $\mu(x, e) = x$, $\mu(\mu(x, g), h) = \mu(x, gh)$. We may write this as

$$x^e = x \qquad (x^g)^h = x^{(gh)}$$

Permutation representation: Given a group G and a set S of size n , then the possible G -spaces on S are in 1:1 correspondence with the homomorphisms $\rho : G \rightarrow S_n$.

If $\text{Ker } \rho = \{e\}$, then S is said to be a faithful G -space.

For $x \in S$, $x^G := \{x^g : g \in G\}$, the orbit of x . If \sim is defined as $a \sim b$ iff a, b are in an orbit together, then \sim is an equivalence relation. A transitive G -space is one which is an orbit. Equivalently, G is transitive iff there is some $c \in S$ such that for every $x \in S$ we can find a $g \in G$ s.t. $x = c^g$. Another characterization is that for every $x, y \in S$ we can find a $g \in G$ s.t. $x = y^g$.

For $x \in S$, $G_x := \text{Stab } x = \{g \in G : x^g = x\}$. $\text{Stab } x$ is a subgroup of G .

Orbit-Stabilizer theorem: For any $x \in S$, $\text{cos}(G : \text{Stab } x) \approx x^G$. Hence, if G is finite, $|G| = |\text{Stab } x| |x^G|$.

Proof:

Define a map $\theta : \text{cos}(G : \text{Stab } x) \rightarrow x^G$ by $\theta(\text{Stab } x y) = x^y$. Show θ to be well-defined, 1:1 and onto.

"Hence" comes from Lagrange's theorem.

□

2 Burnside's theorem.

Lectures: 4.2-5.1; NST: pp. 100-7.

Finding the rotation groups of regular polyhedra:

The regular polyhedra are the tetrahedron, cube, octahedron, dodecahedron and icosahedron. Cube/octahedron and dodecahedron/icosahedron are duals (joining centroids of one gives the edges of the other) so have the same rotation group.

To find $|G|$, use the orbit-stabiliser theorem (G acting on $X := \{\text{vertices}\}$). Rotations are transitive, so $|v^G| = |X|$. Find $|\text{Stab } v| =$ the number of edges coming out of each vertex.

$$|G| = |\text{Stab } v| |v^G|$$

As rotations permute things, G will be a subgroup of S_n . Guess what based on $|G|$ then seek to prove it by showing $\pi : G \rightarrow$ (what you think G is) is an isomorphism. Alternatively, just list all the rotations and draw a Cayley table.

Burnside's theorem: Let $\text{fix}(g) := \{x \in S : x^g = x\}$, $t :=$ the number of orbits.

Then,

$$t = \frac{1}{|G|} \sum_{g \in G} |\text{fix}(g)|$$

Proof:

Let R_1, \dots, R_t be the orbits. Consider $|S|$ where $S := \{(x, g) : x^g = x\}$. Summing through G ,

$$|S| = \sum_{g \in G} |\text{fix}(g)|$$

Summing through S ,

$$\begin{aligned} |S| &= \sum_{x \in S} |\text{Stab}(x)| \\ &= \sum_{i=1}^t \sum_{x \in R_i} |\text{Stab}(x)| \\ &= \sum_{i=1}^t \sum_{x \in R_i} \frac{|G|}{|R_i|} \\ &= t|G| \end{aligned}$$

□

Typical application: How many essentially different ways are there of colouring a cube red, white, blue, so that each face is painted with one colour. **Essentially different = different modulo rotation.** Use Burnside's theorem with the group of rotations of the solid acting on the set of all colourings (we are looking for the number of orbits).

3 Rings.

Lectures: 6.1-7.1; Green: pp. 111-40.

A ring is a set R endowed with two binary operations $+$ and \cdot and a special 0 s.t. $(R, +, 0)$ is an abelian group, \cdot is associative and $+, \cdot$ distribute.

A ring is commutative iff \cdot is. A ring has identity iff there is a special element 1 such that for all $r \in R$, $1r = r1 = r$. If R is a ring with 1 , then a unit is an element $r \in R$ for which there exists an $s \in R$ s.t. $sr = rs = 1$. The characteristic of a ring with 1 is the additive order of 1 .

An integral domain is a commutative ring with 1 in which $ab = 0 \Rightarrow a = 0$ or $b = 0$. A field is a ring with 1 s.t. $(R, \cdot, 1)$ is an abelian group.

A subset, J , of a ring is an ideal iff it is a subgroup of $(R, +, 0)$ and $\forall r \in R, j \in J : rj \in J$ and $jr \in J$. We write $J \triangleleft R$. An ideal is prime iff $ab \in J \Rightarrow a \in J$ or $b \in J$. An ideal is maximal iff there is no $I \triangleleft R$ with $J \subset I \subset R$.

If R is a ring and J an ideal, $R/J := \{x + J : x \in R\}$ is a ring. R/J is a field iff J is maximal. R/J is an ID iff J is prime.

A map between rings, $f : R \rightarrow S$ is a homomorphism iff it respects addition and multiplication. The isomorphism theorems transfer *mutatis mutandis* from group theory.

4 Factorisation in $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$.

Lecture notes: sec. 2.8; Stewart: pp. 18-22.

Testing for reducibility in $\mathbb{Z}[x]$:

- if $\deg(f) = 2$ or 3 then f is reducible iff it has a linear factor (which corresponds to a root).
- a is a root of f iff $a \mid$ (the constant term).
- if a polynomial is irreducible over \mathbb{Z}_p for some prime p , then the polynomial is irreducible over \mathbb{Z} .
- warning: if a polynomial is of degree ≥ 4 , then not having a root a given ring does **not** mean it is irreducible over that ring, use 'native wit' or...

Eisenstein's irreducibility criterion: Let $f(x) = (a_0 + a_1x + \dots + a_nx^n) \in \mathbb{Z}[x]$ and p be some prime s.t.

1. $p \nmid a_n$
2. $p \mid a_j, (j = 0, \dots, n-1)$
3. $p^2 \nmid a_0$

Then, f is irreducible over \mathbb{Z} .

Proof:

We proceed by reductio ad absurdum. Suppose $f = gh$, where $g = b_0 + b_1x + \dots + b_r x^r$, $h = c_0 + c_1x + \dots + c_s x^s$.

By (2), (3), $p \mid b_0$ **xor** $p \mid c_0$, wlog say $p \mid b_0$.

Let b_k be the first coefficient not divisible by p (there is one, as otherwise $p \mid a_n$).

$p \mid a_k = b_k c_0 + \dots + b_0 c_k$, so $p \mid c_0$. Contradiction.

□

Gauss' Lemma: If a polynomial with integer coefficients is irreducible over \mathbb{Z} then it's irreducible over \mathbb{Q} .

Proof:

We prove the contrapositive.

Let $f = gh$, $g, h \in \mathbb{Q}[x]$. Clearing denominators gives $(cd)f = g^*h^*$, where $g^*, h^* \in \mathbb{Z}[x]$.

If $cd = \pm 1$, we're done. Otherwise, $\pm(cd)$ is a product of primes; each prime divides all the coefficients of g^*h^* , so must divide all the coefficients of g^* or h^* (verify this by proving the contrapositive by considering $(g^*h^*)_{a+b}$ where $(g^*)_a$ and $(h^*)_b$ are the first not to be divisible), so we can cancel all the primes.

So, g^*h^* is a reduction over \mathbb{Z} .

□

5 Field extensions and polynomials.

Lecture notes: 3.5-3.13; Stewart: pp. 29-50.

Formally, a field extension is a monomorphism $i : K \rightarrow L$ (K, L fields). Informally, we identify $i(K)$ with K .

The minimum polynomial of an element a in a field K over a subfield L is the monic polynomial with coefficients in L of least degree, p , s.t. $p(a) = 0$. If it exists, a is algebraic and the minimum polynomial is irreducible.

Algebraic extensions: Let F be a field and a an algebraic element of an extension K with minimum polynomial p of degree k . Let $F(a) := \{g \in F[x] \text{ and } \deg(g) < k\}$. Then

1. $F[x]/(p) \cong F(a)$, where (p) is the ideal generated by p .
2. $F(a)$ is the smallest subfield of K containing F and a .
3. $[F(a) : F] = k$, where $[L : M]$ is the dimension of L regarded as a vector space over M .

Proof:

1. Use the 1st Isomorphism theorem on the homomorphism $E : F[x] \rightarrow F(a)$ defined by $E(p) = p(a)$ (use division algorithm to check closure).
2. p is irreducible, so (p) is maximal, so $F[x]/(p)$ is a field so (by 1), $F(a)$ is too. Any other field containing F and a would have to have $g(a)$ in too by closure, so $F(a)$ is minimal.

3. $\{a^j : j = 0, 1, \dots, k-1\}$ is a basis for $F(a)$ over F .

□

Tower law: Let F, K, L be fields with $F \leq K \leq L$. Then, $[L : F] = [L : K][K : F]$

Proof:

Let $\{x_1, \dots, x_n\}$ be a basis for K over F and $\{y_1, \dots, y_m\}$ be a basis for L over K . Show that $\{x_i y_j : i = 1, \dots, n; j = 1, \dots, m\}$ is a basis for L over F .

□

An algebraic extension is one in which elements of the big field are algebraic over the little field.

Algebraic extensions are transitive: if K is an ae of F and F is an ae of L then K is an ae of L .

Proof:

Consider arbitrary $x \in K$. We can find a polynomial $a_0 + a_1x + \dots + a_nx^n = 0$ with $a_i \in F$.

Hence, x is algebraic over $L(a_0, a_1, \dots, a_n)$ and clearly $[L(a_0, a_1, \dots, a_n) : L] < \infty$.

□

Given a polynomial f over a field F , a splitting field of f , S , is the smallest field over which f factorizes into linear factors.

Existence: If K is any field and f is any polynomial over K then f has a splitting field over \bar{K} .

Proof:

By induction on the degree of f . The base step's trivial.

If f doesn't split, it has an irreducible factor, g , say. Consider $F[x]/(g) := K$.

F is embedded in K by $a \rightarrow a + (g)$ so K is an extension and $x + (g) := \rho$ is a root of g and hence of f .

So, over $K = F(\rho)$ we have $f(t) = (t - \rho)h(t)$ where $\deg(h) < \deg(f)$

□

6 Ruler and compass constructions.

Lecture notes: 3.14-3.15; Stewart: pp. 51-7.

A point in \mathbb{R}^2 is constructible iff it can be constructed from the points $(0,0), (0,1)$ using only a rule and compass.

Non-constructibility theorem: If (X,Y) is constructible then $\mathbb{Q}(X,Y)$ lies in a finite extension of \mathbb{Q} whose degree is a power of two.

Proof:

Induct on the number of steps in the construction. Base is trivial.

Say n points $(x, y)_1, (x, y)_2, \dots, (x, y)_n$ are constructed in that order and let $K_n := \mathbb{Q}(x_1, \dots, x_n; y_1, \dots, y_n)$. We must show $[K_n : K_{n-1}] = 1$ or 2 .

But, x_n, y_n are intersections of circlines which pass through points in K_{n-1} . These will have equations

$$\frac{x-a}{b-a} = y - cd - c \quad (x-a)^2 + (y-b)^2 = (x-c)^2 + (y-d)^2 \quad a, b, c, d \in K_{n-1}$$

ie. x_n, y_n are solutions of linear or quadratic polynomials with coefficients in K_{n-1}

□

Regular polygons: A regular k -agon can be constructed iff $\cos(2\pi/k)$ can be.