Notes on Commutative Rings

1 A hierarchy of commutative rings

Euc. R $\Rightarrow$ P.I.D. $\Rightarrow$ U.F.D. $\Rightarrow$ Int. D. $\Rightarrow$ Comm.R.

[Comm.R.] Commutative Ring R with $1 \neq 0$.

1. The ideal generated by $\{a_1, \ldots, a_n\}$ is the set of all R-linear combinations $r_1a_1 + \ldots + r_na_n$. A principal ideal (a) has one such generator.

2. The set $R^\times$ of units is a multiplicative group. (Units are the elements with multiplicative inverses. They cannot be zerodivisors. A zerodivisor is an $a \neq 0$ such that $ab = 0$ for some other $b \neq 0$.)

3. (a) A proper ideal I is
   - prime if $ab \in I \Rightarrow a \in I$ or $b \in I$;
   - maximal if $I \subseteq J \subseteq R \Rightarrow J = I$ or $J = R$.

   [We allow $I = (0)$.]

   (b) Maximal ideal $\Rightarrow$ Prime ideal.
   In $\mathbb{Z}[x]$, $I = (x)$ is prime but not maximal. Note $\mathbb{Z}[x]/(x) \simeq \mathbb{Z}$.

   (c) I maximal $\Leftrightarrow$ R/I field.
   I prime $\Leftrightarrow$ R/I integral domain.

   (d) If ideal $I \neq R$, then there exists a maximal ideal M with $I \subseteq M \subset R$.

   (e) Thus every non-unit b (which is in a proper ideal (b)) must lie in a maximal ideal.

4. More on Maximal Ideals, Local Rings, Radical Ideals

   (a) Note: If $a \notin M$, a maximal ideal, then $R = M + Ra$, so that a is a unit mod M. Thus $R \setminus M$ consists of units mod M.

   (b) Suppose M is a proper ideal in R. We say that R is a local ring if M is the unique maximal ideal in R.

- $R\setminus M$ consists entirely of units in $R \Leftrightarrow M$ unique maximal. (For $\Leftarrow$: if x is a non-unit, then (x) is a proper ideal, hence lies in some maximal ideal, hence is contained in M by uniqueness.)
- If M is maximal and $1+M$ consists of units, then M is the unique maximal ideal and R is a local ring. (For if $u \in R\setminus M$, then $1 = xu+m$ for some $m \in M,\ x \in R$, so $xu = 1+(-m)$ is a unit, so u is a unit; see previous item.)

(c) The nilradical Nil of R consists of all nilpotent elements of R ($x^n = 0$ for some positive integer n). It's easy to prove this is an ideal; and R/Nil has no non-zero nilpotent elements. Further, Nil is the intersection of all prime ideals in R. (Note: $\supseteq$ involves the construction of a suitable prime ideal; see Reid for a Zorn's Lemma argument involving multiplicative sets.)

(d) The Jacobson radical Jac of R is the intersection of all maximal ideals. Furthermore, $x \in \mathrm{Jac}$ if–f $1-xy$ is a unit in R for all $y \in R$.

(e) The radical of an ideal I is

$$\sqrt{I} := \{x \in R : x^k \in I, \quad \text{for some} \quad k \geqslant 1\}\ .$$

Thus $\sqrt{I}$ is an ideal; $I \subseteq \sqrt{I}$; and $\sqrt{I}$ is the intersection of all the prime ideals containing I.
Thus $\sqrt{R} = R$ and $\sqrt{(0)} = \mathrm{Nil}$.

5. (a) The sum of ideals I, J is the ideal

$$I+J := \{a+b \mid a \in I,\ b \in J\}.$$

Eg. If M maximal, and $ab \in M$, then each of $M+Ra,\ M+Rb$ equals M or R. If both equal R, then $1 = m_1 + r_1a = m_2 + r_2b$; multiply to get $1 \in M$, a contradiction. Thus maximal $\Rightarrow$ prime.

(b) Ideals I, J are relatively prime if $I+J = R$.

6. Polynomials. The polynomial ring $R[x]$ is determined by the following universal property: there is a ring embedding $\mu : R \to R[x]$ and an element $x \in R[x]$ such that for any homomorphism $\varphi : R \to S$ and specific element $c \in S$ there exists a unique homomorphism $\varphi_c : R[x] \to S$ with $\varphi = \mu\varphi_c$ (compose left to right) and $x\varphi_c = c$.

$$\begin{tikzcd} R \arrow[r, "\mu"] \arrow[dr, "\varphi"'] & R[x] \arrow[d, "\varphi_c"] \\ & S \end{tikzcd}$$

If I is a proper ideal in R, we thus have

$$R[x]/I[x] \simeq (R/I)[x] \ . \tag{1}$$

That is, factor by the ideal (in $R[x]$) of all polynomials with coefficients in I.

7. Eisenstein:

   If M is maximal in R and

   $$f(x) = a_n x^n + \ldots + a_0 \qquad (n \geqslant 1)$$

   with $a_n \notin M,\ a_i \in M$ for all $i < n$, and $a_0 \notin M^2$, then f is irreducible over R. (That is, $f = gh$ forces g or h to be a constant polynomial.)

   So suppose $g = \sum_0^r b_i x^i,\ h = \sum_0^s c_i x^i$, where $r + s = n = \deg f$, with $r, s > 0$. Since $a_0 \in M$ but $a_0 \notin M^2$, we can w.l.o.g. assume $b_0 \in M$ and $c_0 \notin M$. (Note that $a_0 \equiv b_0 c_0 \equiv 0$ in the field R/M.) But $a_n = b_r c_s \notin M$, so let j be minimal with $b_j \notin M$. Thus $j \geqslant 1$. Consider

   $$a_j = b_0 c_j + \ldots + b_{j-1} c_1 + b_j c_0 \pmod{M} \ .$$

   This gives a contradiction.

8. The product IJ of ideals I, J consists of all finite sums of products ab, where $a \in I,\ B \in J$.

   We similarly define the product of ideals $I_1, \ldots, I_m$. Always we have for ideals J, I_k:

   (a) $I_1 \ldots I_m = (I_1 \ldots I_{m-1}) I_m$.

   (b) $I_1 \ldots I_m \subseteq I_1 \cap \ldots \cap I_m$.

   (c) $(I_1 + J)(I_2 + J) \ldots (I_m + J) \subseteq (I_1 \ldots I_m) + J$.

9. <u>Theorem.</u> Let $I_1, \ldots, I_m$ be pairwise relatively prime ideals, and for $1 \leqslant k \leqslant m$ let

$$\widehat{I_k} := \bigcap_{i \neq k} I_i = I_1 \cap \ldots \cap I_{k-1} \cap I_{k+1} \cap \ldots \cap I_m \ .$$

Then

(a) $I_1 \ldots I_m = I_1 \cap \ldots \cap I_m$.

(b) For $1 \leqslant k \leqslant m,\ I_k$ and $\widehat{I_k}$ are relatively prime.

<u>Proof.</u> (Induction on m.)

(i) <u>$m = 2$</u>. Part (b) follows by definition. Since $R = I_1 + I_2$, there exist $a \in I_1,\ b \in I_2$ with $1 = a + b$. Thus $x \in I_1 \cap I_2 \Rightarrow x = ax + xb \in I_1 I_2$. This proves (a).

(ii) For $m \geqslant 2$, we may assume by induction that for $1 \leqslant k \leqslant m$,

$$\widehat{I_k} = I_1 \ldots I_{k-1} I_{k+1} \ldots I_m \ .$$

Thus

$$R = (I_k + I_1) \ldots (I_k + I_{k-1})(I_k + I_{k+1}) \ldots (I_k + I_m) \subseteq I_k + \widehat{I_k} \subseteq R.$$

This proves part (b). Next note that

$$\begin{aligned} I_1 \ldots I_m &= (I_1 \ldots I_{m-1}) I_m \\ &= \widehat{I_m} I_m && \text{(induction, (a))} \\ &= \widehat{I_m} \cap I_m && \text{(induction, } m = 2) \\ &= (I_1 \cap \ldots \cap I_{m-1}) \cap I_m && \text{(induction).} \end{aligned}$$

This end the proof.
Note that if $I_k,\ \widehat{I_k}$ are relatively prime, then $I_k,\ I_i$ are relatively prime for all $i \neq k$, since $I_i \supseteq \widehat{I_k}$, so that $I_i + I_k = R$.

10. **Chinese Remainder Theorem.** Suppose that $I_1, \ldots, I_m$ are pairwise relatively prime ideals. Then the natural mapping

$$R/\bigcap_{k=1}^{m} I_k \to R/I_1 \times \ldots \times R/I_m$$

is an isomorphism.

Proof. It's easy to check this mapping is well-defined and $1-1$. By the previous theorem, for $1 \leqslant k \leqslant m$ there exist $a_k \in I_k$, $b_k \in \widehat{I_k}$ with $1 = a_k + b_k$. For any $r_1, \ldots, r_m \in R$, let $r = r_1 b_1 + \ldots + r_m b_m$. Then $r \equiv r_k \pmod{I_k}$ for $1 \leqslant k \leqslant m$, so the above mapping is onto.

[Int. D] Integral Domain – no zerodivisors, so that cancellation holds.

1. A non-unit, non-zero element p is

   - **irreducible** – if $p = ab \Rightarrow a$ or b is a unit;
   - **prime** – if $p|(ab) \Rightarrow p|a$ or $p|b$.

   Thus p prime $\Rightarrow p$ irreducible, but not conversely in general, because of (c) below.

2. Results on Principal Ideals.

   (a) $(a) = (b)$ if and only if a, b are associates. Thus the generator of a principal ideal is unique to unit factors.

   (b) A non-zero principal ideal (p) is a prime ideal if and only if the generator p is prime.

   (c) A non-zero principal ideal (m) is maximal (among principal ideals in R) if and only if the generator m is irreducible.

   Note that if (m) is maximal, then it is maximal among principal ideals. However, the converse may fail if there are non-principal ideals J with

   $$(m) \subset J \subset R.$$

   Of course, this converse will hold in a P.I.D. (see below).

3. If R is an integral domain, so is $R[x]$ (easy: look at leading coefficients).

4. Any integral domain R embeds in a unique **field of fractions** $K = \text{Frac } R$. Any isomorphism $\varphi : R \to S$ (of integral domains) extends uniquely to the respective fields of fractions. In a sense, the field of fractions is "minimal" with this property.

5. *Gauss' Lemma for an Integral Domain* R. Any prime $p \in R$ remains prime in $R[x]$.

   Proof. Let $p \in R$ be prime, so that $I = (p)$ is a prime ideal and R/I is an integral domain. Suppose $p|fg$ for $f, g \in R[x]$, say $fg = ph$. Passing to $R[x]/I[x]$, we get $fg = 0$ in the integral domain $(R/I)[x]$ (see (1). Thus f or G is in $I[x]$, so p divides one or the other. $\square$

[U.F.D.] Unique Factorization Domain.

1. By definition each $x \neq 0$ has an essentially unique factorization into irreducibles.

   (a) If p irreducible and $p|ab$, then p must appear in the factorization of either a or b. Thus

   $$\text{irreducible} \Rightarrow \text{prime.}$$

   (b) Alternatively, one may define a U.F.D. as an integral domain in which factorizations into irreducibles exist and in which irreducibles are prime.

   In any case, in U.F.D.'s we have

   $$\text{irreducible} \Leftrightarrow \text{prime.}$$

2. Any two elements in a U.F.D have a gcd and lcm, unique to units.

3. For any $f \in R[x]$, the <u>content</u>

   $$\delta = \delta(f) := \gcd(\{\text{ all coefficients of } f\})$$

   The content is thus determined to associates, and $f = \delta f_1$ for some *primitive* polynomial $f_1 \in R[x]$. A primitive polynomial is one whose content is a unit. Consequently, it cannot be 0.

4. *Gauss' Lemma for a UFD R.* The product of two primitive polynomials f and g is also primitive.

   Standard Proof. Let $f = \sum a_i x^i$, $g = \sum b_i x^i$. Say $fg = \delta h$, for $\delta \in R$ and $h = \sum c_i x^i \in R[x]$. Suppose some prime $p|\delta$. Since f, g primitive, there exist 'first' coeffs. a_r, b_s not divisible by p. But then $\delta c^{r+s} = a_r b_s +$ terms div. by p: contradiction. So δ is a unit and fg is primitive. □

   Another Proof. If fg not primitive, there exists a prime $p|(fg)$. By Gauss' Lemma for integral domains this means $p|f$ or $p|g$, contradicting primitivity of one or the other poly. □

5. Corollaries.

   (a) The content of a product of polynomials is the product of the contents.

   (b) Suppose U.F.D. R has field of fractions K. Suppose $h \in R[x]$ factors over $K[x]$ as $h = fg$. Then there is a $u \in K$ with $uf,\ u^{-1}g \in R[x]$. In short, h actually factors in the base ring $R[x]$.

   Proof. For any poly. in $K[x]$ we can find a common denom. for the coeffs. and extract a gcd for the new numerators. So there exist $a, b, c, d \in R$ and primitive $f_1, g_1 \in R[x]$ with
   $$f = \frac{a}{b} f_1\ ,\ g = \frac{c}{d} g_1\ .$$
   Thus
   $$h = \frac{\alpha}{\beta} f_1 g_1\ ,$$
   where $(ac)/(bd) = \alpha/\beta$, with α, β coprime in R. Thus $\beta h = \alpha f_1 g_1$. If some prime $p|\beta$ we get $p|(f_1 g_1)$, again contradicting Gauss' Lemma for integral domains, or the fact that $f_1 g_1$ is primitive. Hence β is a unit in R and so h factors in $R[x]$ as $h = (\alpha f_1)(\beta^{-1} g_1)$. (Thus $u = b\alpha/a$.) □

   (c) If a polynomial with coefficients in $\mathbb{Z}$ is irreducible in $\mathbb{Z}[x]$, then it is irreducible in $\mathbb{Q}[x]$.

   (d) If R is a U.F.D., then so is $R[x]$ (and so also $R[x_1, \ldots, x_n]$).

   Proof. Let K be the field of fractions for R.

   (i) if $f \in R[x]$ is irred., then either $\deg(f) = 0$, whence f is irreducible in R, or $\deg(f) > 0$, whence f is irreducible in $K[x]$ and is furthermore primitive in $R[x]$ (else the content $\delta(f)$ is a non-trivial factor).

   (ii) now any poly. $g \in K[x]$ fcators into irreducibles in $K[x]$, since the latter is a Euclidean domain (hence P.I.D., hence U.F.D.: see below). Using (i) we can now rescale scalars throughout any factorization, and exploit the essential uniqueness in $K[x]$, to get unique factorization into irreducibles in $R[x]$. $\square$

(e) Example in $\mathbb{Z}[x]$: $6x^3 - 24x^2 - 24x - 30 = 2 \cdot 3 \cdot (x^2 + x + 1) \cdot (x - 5)$.

[P.I.D.] Principal Ideal Domain.

1. From above, a proper non-zero ideal here is prime if and only if it is maximal.

2. Here is a proof, appropriate to this context, that p irreducible implies p prime.

   Proof. Say $p|ab$ and let $(q) := (a) + (p)$. Thus $p = xq$. If x is a unit, then $(p) = (q)$, so $a \in (p)$ and thus $p|a$. If q is a unit, then $1 = ya + zp$, so $b = y(ab) + (zb)p$, so $p|b$.

3. A P.I.D. satisfies the **A.C.C.** on ideals. Indeed,

   $$(a_1) \subseteq (a_2) \subseteq \ldots \subseteq (a_i) \subseteq \ldots$$

   implies there exists n with $(a_i) = (a_n)$ for all $i \geqslant n$. (The union is an ideal (b) and $b \in (a_n)$ for some n.)

4. The [**A.C.C.**] prevents an infinite sequence $a_1, a_2, \ldots$ where each a_i is a multiple of a_{i+1}. In turn, this implies factorization onto irreducibles. Now if there are two such factorizations for

   $$x = p_1 \ldots p_r = q_1 \ldots q_s,$$

   we may suppose (p_1) is the minimal ideal among all $(p_j), (q_j)$. Now work in the field $R/(p_1)$ to show that $(p_1) = (q_j)$ for some j. Essential uniqueness soon follows. This explains why

   $$\text{P.I.D.} \Rightarrow \text{U.F.D.}$$

[Euc. R.] Euclidean Rings.

1. These are P.I.D.'s. Examples include $\mathbb{Z}$ and $k[x]$, for any field k.

2 Fourth Isomorphism Theorem

. Suppose $\varphi : R \to S$ be a ring epimorphism (mapping 1_R to 1_S when rings have units.) Let $K = \ker \varphi$. On

$$\mathcal{L}_R := \{\text{ideals } J : K \subseteq J \subseteq R\} ,$$

we define $\widetilde{J} := \varphi(J)$; and on

$$\mathcal{L}_S := \{\text{ideals } L : L \subseteq S\} .$$

we let $L^* := \varphi^{-1}(L)$. Then

1. $S \simeq R/K$.
2. $J \mapsto \widetilde{J}$ and $L \mapsto L^*$ are well-defined mappings respecting inclusion of ideals; and $J = (\widetilde{J})^*$ and $L = \widetilde{(L^*)}$.
3. $\mathcal{L}_R$ and $\mathcal{L}_S$ are isomorphic as partially ordered sets.
4. J is maximal in R if and only $\widetilde{J}$ is maximal in S.
5. J is prime in R if and only $\widetilde{J}$ is prime in S.
6. $R/J \simeq S/\tilde{J}$.
7. $\widetilde{(J_1 \cap J_2)} = \widetilde{J}_1 \cap \widetilde{J}_2$.
8. $\widetilde{(J_1 + J_2)} = \widetilde{J}_1 + \widetilde{J}_2$.

Proof. This is all routine. The condition that $K \subseteq J$ eliminates problems. $\square$

3 Modules and Integrality

1. Let A be a commutative ring with identity $1 = 1_A$. Recall that

   - an A -module M is *finitely generated*, or just *finite*, if it has a finite spanning set.
   - the A-module endomorphisms $\lambda : M \to M$ form a ring $\mathrm{End}M$ with composition as multiplication and with identity $\imath = 1_{\mathrm{End}M} : M \to M$.

     It is easy to see that scalar multiplication $a\lambda$, with $a \in A, \lambda \in \mathrm{End}M$, interacts as expected with addition and multiplication of endomorphisms. Thus $\mathrm{End}M$ is also an A-module, and in fact an A-algebra.
   - M is said to be *faithful* as an A-module if $am = 0, \forall m \in M$, implies $a = 0$. In this case, A embeds isomorphically in $\mathrm{End}M$ via the scalar mappings $\mu_a : M \to M$, where $\mu_a(m) = am$.

2. Fix $\varphi \in \mathrm{End}M$ and let

$$A[\varphi] := \{a_n\varphi^n + a_{n-1}\varphi^{n-1} + \cdots + a_1\varphi + a_0\imath : a_j \in A,\ n \geqslant 0\}$$

   be the set of all polynomials in φ. Thus $A[\varphi]$ is the subring of $\mathrm{End}M$ generated by φ and all $a\,\imath$, in other words, the subalgebra generated by φ.

   Note that M now becomes an $A[\varphi]$-module, taking $\varphi \cdot m := \varphi(m)$.

3.

   Theorem 3.1. *The Determinant Trick*

   Suppose the finite A-module M is spanned by $m_1, \ldots, m_n$. Let $\varphi : M \to M$ be an A-module endomorphism such that $\varphi(M) \subseteq IM$ for some ideal I of A. (Of course, this always holds for $I = (1) = A$.) Then φ satisfies some monic relation

$$\varphi^n + c_1\varphi^{n-1} + \cdots + c_{n-1}\varphi + c_n\imath = 0 \tag{2}$$

   in $A[\varphi]$, with $c_j \in I^j$ (the product ideal) for $j = 1, \ldots, n$,

   Proof. For certain $a_{kj} \in I$ we have

$$\varphi(m_j) = \sum_{j=1}^{n} a_{kj}m_j\ .$$

   In $A[\varphi]$ this gives

$$\sum_{j=1}^{n}(\delta_{kj}\varphi - a_{kj}\imath)(m_j) = 0 \; , \tag{3}$$

where $\delta_{kj} \in A$. Let the matrix $\Delta = [\delta_{kj}\varphi - a_{kj}\imath]$ over the ring $A[\varphi]$ have adjoint $\mathrm{adj}\Delta = [b_{kj}]$. Thus for all l, j we have

$$\sum_{k=1}^{n} b_{lk}(\delta_{kj}\varphi - a_{kj}\imath) = \delta_{lj}\det(\Delta).$$

Apply this last result to each m_j and sum using (3) to conclude that all $\det(\Delta)(m_j) = 0$. Thus $\det(\Delta) = 0$ in $A[\varphi]$. Expand this determinant to get (2). $\square$

4. **Examples**

   (a) Suppose $I = A$ and M is a free module with basis $m_1, \ldots, m_n$. Then the matrix for $\varphi \in \mathrm{End}M$ is $[a_{kj}]$, with *characteristic polynomial*

   $$\chi(t) = \det[\delta_{kj}t - a_{kj}] \; .$$

   Replacing t by φ (and 1_A by $\imath$) we get

   $$\det[\delta_{kj}\varphi - a_{kj}\imath] = 0$$

   in $\mathrm{End}M$. This is the Cayley-Hamilton Theorem.

   (b) If A is a subring of B, then the determinant trick is the key to proving that the elements of B which are *integral* over A form a subring of B, i.e. the *integral closure* of A in B.

4 Finitely Generated Modules and Nakayama's Lemma

1. Nakayama's Lemma. Let V be a finitely generated R–module and I an ideal contained in the Jacobson radical of R (i.e. in the intersection of all maximal ideals). Then $IV = V$ implies $V = 0$.

   (For $V \neq 0$ let $u_1, \ldots, u_n$ be a minimal set of generators; thus $u_n = a_1u_1 + \ldots + a_nu_n$, for some $a_j \in I$; since a_n for instance is in the Jacobson radical, $1 - a_n$ is a unit, which means that u_n is redundant: contradn.)

2. Let R be a local ring with maximal ideal I. Suppose W is an R-submodule of the R-module V, where V/W is finitely generated and such that $V = W + IV$. Then $V = W$.

3. If V is finite over R, then $V/(IV)$ is a finite dimensional vector space over the residue field $k = R/I$. And a spanning subset of this vector space lifts to a spanning subset of V considered as an R-module.

5 Finitely generated Algebras

Our sources are notes from Colin Ingalls, who in turn referred to www.mathreference.com. See also Miles Reid's book *Undergraduate Commutative Algebra* [2]. The key Theorem 5.2 below appears in that book in Section 4.2. Perhaps it makes sense to take that as the starting point for a talk.

1.

Lemma 5.1. *Let R be a* UFD *which has infinitely many primes and is (embedded as) a subring of a field A. Suppose A is finitely generated as an R-algebra. Then A cannot be an algebraic extension of the fraction field F for R.*

Proof. Since A is a field, we have $R \subseteq F \subseteq A$. We must understand the field extension $F \subseteq A$. So suppose A is algebraic over F and let $A = R[z_1, \ldots, z_m]$ as a finitely generated algebra over R.

Each z_i satisfies a monic polynomial $p_i(t)$ over F. Since R is a UFD, we have a least common multiple d for all *denominators* of coefficients in the various p_i. Thus each

$$p_i \in \frac{1}{d} R[t] \ .$$

Now let $S := R[1/d]$, so

$$R \subseteq S \subseteq F \subseteq A \ .$$

Note that $A = S[z_1, \ldots, z_m]$ and that each z_i is integral over S. Since R has infinitely many primes, there exists a prime $q \in R$ such that $q \nmid d$. Note that $1/q \in F$ but $1/q \notin S$. For if

$$\frac{1}{q} = a_0 + \frac{a_1}{d} + \cdots + \frac{a_k}{d^k} \ ,$$

with $a_j \in R$, then

$$d^k = q(a_0 d^k + \cdots a_k) \ ,$$

which forces $k = 0$ and $qa_0 = 1$: contradiction, as q is not a unit.

But $1/q \in A$, so $1/q$ is integral over S. Suppose $1/q$ satisfies a monic polynomial of degree k over S. Clear denominators using a suitable power d^L to get

alternate expla-nation below

$$0 = \frac{d^L}{q^k} + \frac{b_{k-1}}{q^{k-1}} + \cdots + \frac{b_1}{q} + b_0 \ ,$$

where each $b_j \in R$. Multiply this by $d^{L(k-1)}$ to get

$$0 = 1(\frac{d^L}{q})^k + b_{k-1}(\frac{d^L}{q})^{k-1} + \cdots + (b_1 d^{Lk-2L})(\frac{d^L}{q})^1 + b_0 d^{L(k-1)} \ .$$

Thus d^L/q is integral over R. However, by a standard argument, R is integrally closed in F. (This is the argument that a rational root of an integral polynomial must actually be an integer.) Thus, $d^L/q \in R$, which is a contradiction since $q \nmid d$.

– or more simply ... –

degree k over S. For a suitable power d^L and $b_j \in R$, we can write this polynomial as

$$1x^k + \frac{b_{k-1}}{d^L} x^{k-1} + \cdots + \frac{b_1}{d^L} x + \frac{b_0}{d^L} \ .$$

Substitute $x = 1/q$ and multiply by $q^k d^L$ to get

$$0 = d^L + b_{k-1} q + \cdots + b_1 q^{k-1} + b_0 q^k \ ,$$

which implies that $q \mid d^L$, a contradiction. □

2. **Remark**. We will need only the cases $R = \mathbb{Z}$ or $R = K[x]$, where K is a field. Both are Euclidean domains; and in each case we have Euclid's proof of the infinity of primes.

3.

Theorem 5.2. *Let A be a finitely generated algebra of the field K, that is $A = K[y_1, \ldots, y_n]$ for certain $y_j \in A$. Then A is a field only if it has finite dimension as a vector space over K.*

Proof. Suppose $A = K[y_1, \ldots, y_n]$ is a field. Proceed by induction on n.

If $n = 0$, then $A = K$ and $\dim(A : K) = 0$. If $n = 1$, then we have an epimorphism $\varphi : K[t] \to A = K[y_1]$, say with kernel M. Since A is a field, M is maximal; and since $K[t]$ is a PID, $M = (p(t))$, where $p(t)$ is irreducible over K. Then $A \simeq K[t]/M$ and $\dim(A : K) = \deg(p) < \infty$.

Suppose then that any field generated as a ring over a subfield by fewer than n generators is in fact finite-dimensional over that subfield.

Now consider $A = K[y_1, \ldots, y_n]$ and let $R = K[y_1]$, a subring of A. Let F be the field of fractions of R, so F is a subfield of A. Since $y_1 \in R \subseteq F$, we have $A = F[y_2, \ldots, y_n]$. Indeed, A is even finitely generated as an R-algebra. By induction, $\dim(A : F) < \infty$, so A is algebraic over F. We are done if we can show $\dim(F : K) < \infty$.

Now if y_1 were transcendental over K, $R = K[y_1]$ would be a UFD with infinitely many primes. This violates Lemma 5.1.

Thus y_1 is a root of some polynomial $w(t) \in K[t]$ of minimal degree; $w(t)$ must be irreducible over K and $R = K[y_1]$ an field extension of finite dimension over K. But then $F = R$, so $\dim(F : K) < \infty$. □

4. **Remark**. Theorem 5.2 might be called the *Weak Nullstellensatz*.

   There is a partial converse. Suppose in addition that A is an integral domain for which $\dim(A : K) < \infty$. For each non-zero $a \in A$ we may define a K-linear map $A \to A$ by $x \mapsto ax$. This map is injective, hence surjective, so that there exists $x \in A$ such that $ax = 1$. Thus A is in fact a field.

5. **Definition**. A ring R is said to be *finitely generated* if there is some ring epimorphism

$$\varphi : \mathbb{Z}[x_1, \ldots, x_n] \to R \, .$$

   In other words, there are generators $r_1, \ldots, r_n \in R$ such that each element of R is a $\mathbb{Z}$-linear combination of various products of these r_js.

6.

Theorem 5.3. *Let M be a maximal ideal in a finitely generated ring R. Then $A := R/M$ is a finite field.*

Proof. Let R be the image of $\mathbb{Z}$ in A and let K be the field of fractions of R. Clearly, the field A is finitely generated over R. Moreover, it is also finitely generated over K. By Theorem 5.2, $\dim(A : K) < \infty$.

If K has characteristic 0, then $\mathbb{Z} \simeq R$ is embedded in A and once more we contradict Lemma 5.1.

Thus $K \simeq \mathbb{Z}_p$ for some prime p. By Theorem 5.2 we conclude that A is a finite field.

□

7.

Theorem 5.4. *Let R be a finitely generated integral domain. Then for each non-zero $z \in R$ there exists a maximal ideal P such that $z \notin P$. In short, the Jacobson radical $J(R) = \{0\}$.*

Proof. Consider the subring $R[1/z]$ in the fraction field F of R. Let M be a maximal ideal in $R[1/z]$ and set $P := M \cap R$.

Clearly P is an ideal in R. In fact, P is prime. For suppose $ab \in P$ but $a \notin P$. Then $a \notin M$ so $M + R[1/z] \cdot a = R[1/z]$. For some polynomial $q(t)$ over R and $m \in M$ we have $m + q(1/z)a = 1$. Multiply by b to see that $b \in P$.

On the other hand $z \notin P$. For if $z \in P$, then $z \in M$; since $1/z \in R[1/z]$, we get $1 = z(1/z) \in M$, a contradiction.

The inclusion $P \subseteq M$ induces a well-defined injection $\mu : R/P \to R[1/z]/M$. By Theorem 5.3, $A := R[1/z]/M$ is a finite field. Note that R is finitely generated as a ring; therefore, so also is $R[1/z]$.

Thus R/P is a finite integral domain, hence also a finite field, isomorphic to a subfield of A. Thus the ideal P is actually maximal, and we have $z \notin P$. □

8.

Theorem 5.5. *Weak Nullstellensatz*
Suppose k be an algebraically closed field. Let M be a maximal ideal in $k[x_1, \dots, x_n]$. Then

$$M = (x_1 - a_1, \dots, x_n - a_n)$$

for certain $a_i \in k$.

Moreover, for any proper ideal $J \subset R$, the variety

$$V(J) \neq \emptyset \ .$$

Proof. We have $\varphi : k[x_1, \dots, x_n] \to A := k[x_1, \dots, x_n]/M$. A is a field since M is maximal and is clearly finitely generated over $\varphi(k)$. (The elements $\varphi(x_i)$, $1 \leqslant i \leqslant n$, serve as generators.) Also, $k \simeq \varphi(k)$ since M is maximal and therefore contains no non-zero element of k.

Thus $\dim(A : \varphi(k)) < \infty$ by Theorem 5.2, so A is algebraic over $\varphi(k)$. Therefore $A = \varphi(k) \simeq k$, since k is algebraically closed. Let $\varphi(a_i) = \varphi(x_i)$ for certain $a_i \in k$. Thus each $x_i - a_i \in M$. But the ideal $W = (x_1 - a_1, \ldots, x_n - a_n)$ is itself maximal, hence must equal M. (Remark: think of W as a vector subspace of $k[x_1, \ldots, x_n]$. Since $1 \notin W$, we have $k[x_1, \ldots, x_n] = k \cdot 1 \oplus W$ as linear spaces. But as a linear space M is trapped, so $M = W$.)

For the second part, any proper ideal J must be contained in some maximal ideal $M = (x - a_1, \ldots, x - a_n)$, so that the affine point $(a_1, \ldots, a_n) \in V(J)$. $\square$

Residually Finite Groups

9.

Definition 5.6. *A group Γ is* residually finite *if for any $g \in \Gamma$, $g \neq 1$, there exists a homomorphism $\varphi : \Gamma \to G$, where G is finite and $\varphi(g) \neq 1$.*

Remarks. Any finite group Γ is clearly residually finite. We can assume in the definition that φ is onto.

10.

Theorem 5.7. *The following are equivalent for a group Γ:*

(a) Γ *is residually finite.*

(b) For any finite subset $A \subseteq \Gamma$ there exists an epimorphism

$$\varphi : \Gamma \to G$$

onto a finite group G such that $\varphi_{|A}$ is bijective, i.e. the $\varphi(a)$ are distinct for all $a \in A$.

(c) For any finite subset $A \subseteq \Gamma$, with $1 \notin A$, there exists an epimorphism

$$\varphi : \Gamma \to G$$

onto a finite group G such that $\varphi(a) \neq 1$ for all $a \in A$.

Proof. We need only prove (a) $\Rightarrow$ (b). Suppose $A = \{a_1, \ldots, a_r\}$. For each $i < j$ we have a homomorphism $\varphi_{i,j} : \Gamma \to G_{i,j}$ onto a finite group $G_{i,j}$ such that $\varphi_{i,j}(a_i a_j^{-1}) \neq 1$. Then the direct product

$$\varphi := \prod_{i<j} \varphi_{i,j} : \Gamma \to \prod_{i<j} G_{i,j}$$

does the job. $\square$

Theorem 5.8. *Let Γ be any finitely generated subgroup of $GL_n(F)$ over the field F. Then Γ is residually finite. More specifically, suppose $a_1, \ldots, a_t$ are distinct elements of Γ. Then there is a finite field K and a homomorphism*

$$\varphi : \Gamma \to GL_n(K)$$

such that the $\varphi(a_i)$ are all distinct. Furthermore, if $\operatorname{char}(F) > 0$, *then we can take* $\operatorname{char}(K) = \operatorname{char}(F)$.

Proof. Suppose Γ is generated by $\{g_1, \ldots, g_r\}$; with no loss of generality we can assume this set is closed under taking inverses. For $1 \leqslant k \leqslant r$, let $g_k = [\gamma_{i,j,k}]$; and let P be be the subring of F generated by 1. Thus, P is the prime subfield if $\mathrm{char}(F) > 0$; otherwise, $P \simeq \mathbb{Z}$.

Now let

$$R := P[\gamma_{i,j,k} : 1 \leqslant i, j \leqslant n; 1 \leqslant k \leqslant r] \ .$$

Thus R is a finitely generated integral domain and we have $\Gamma \subseteq GL_n(R)$.

For each $i < j$ we may chose an entry in which matrices a_i and a_j differ; let $b_{i,j}$ be the difference of these entries and set $b := \prod_{i<j} b_{i,j}$. Thus $b \neq 0$; and by Theorem 5.4 there exists a maximal ideal M with $b \notin M$. The natural map $\chi : R \to R/M =: K$ induces a group homomorphism $\varphi : \Gamma \to GL_n(K)$ which does the job. Note that K is a finite field by Theorem 5.3, so that $GL_n(K)$ is a finite group. If $\mathrm{char}(P) > 0$, the additive order of $1 \in P$ cannot collapse, so that also $\mathrm{char}(K) = \mathrm{char}(F)$. $\square$

11. The next result appears as Theorem 3.4B in Dixon's book *The Structure of Linear Groups* [1].

Theorem 5.9. *Let Γ be a finite irreducible subgroup of $GL_n(F)$, where F is algebraically closed. Then there is a finite extension K of the prime subfield of F such that Γ is conjugate in $GL_n(F)$ to a subgroup of $GL_n(K)$.*

Proof.

Exercise. Is it possible to prove this using the machinery outlined above? The word 'conjugate' will be the sticking point. $\square$

References

[1] J. Dixon, *The Structure of Linear Groups*, vol. 37 of Mathematical Studies, Van Nostrand Reinhold, New York, 1971.

[2] M. Reid, *Undergraduate Commutative Algebra*, vol. 29 of London Mathematical Society Student Texts, Cambridge University Press, Cambridge, UK, 1995.