Galois Theory
Michaelmas 2005
Prof A J Scholl
a.j.scholl@dpmms.cam.ac.uk

Background from Groups, Rings and Modules (summary)

1 Rings

1.1. In this course, unless stated to the contrary, 'ring' means a commutative ring with unit. In detail, such a ring is a set R equipped with binary operations $+$ (addition) and $\times$ (multiplication), and distinguished elements $0, 1 \in R$ satisfying the axioms:

(i) $(R, +)$ is a commutative group with identity 0 (so for all $x \in R$, $0 + x = x$);

(ii) The operation $\times$ is commutative, associative, and for all $x \in R$, $1 \times x = x$;

(iii) [Distributive law] For all x, y, $z \in R$, $x \times (y + z) = (x \times y) + (x \times z)$.

A consequence of (iii) is that $x \times 0 = 0$ (by taking $z = 0$). The multiplication sign $\times$ is usually omitted or replaced by a dot; one writes $x \cdot y$ or simply xy instead of $x \times y$.

1.2 Some examples of rings: $\mathbb{Z}$ (integers), $\mathbb{Q}$ (rational numbers), $\mathbb{R}$ (real numbers), $\mathbb{C}$ (complex numbers), $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ (Gaussian integers), $\mathbb{Z}/n\mathbb{Z}$ for $n \geq 1$ (integers mod n), polynomial rings (see §3 below).

1.3. A *zero ring* is any ring with just one element 0, so $1 = 0$ in this ring. (Notice that if $n = 1$ then $\mathbb{Z}/n\mathbb{Z}$ is a zero ring.) If R is any nonzero ring then $1 \neq 0$ in R. (Proof: suppose that $0 = 1$. Then for any $x \in R$, $x = 1 \cdot x = 0 \cdot x = 0$, so $R = \{0\}$.)

1.4. Let R be a nonzero ring. We say R is an *integral domain* (or simply a *domain*) if it has no zero divisors; i.e if $xy = 0$ implies $x = 0$ or $y = 0$. It is a *field* if every nonzero element has an inverse under multiplication; i.e. if whenever $x \neq 0$ there exists $x^{-1} \in R$ with $xx^{-1} = 1$. The nonzero elements of a field then form a group under multiplication.

1.5. A field is automatically an integral domain: if $xy = 0$ and $x \neq 0$, then $y = x^{-1}xy = 0$. Of the examples given above, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are fields, $\mathbb{Z}$ and $\mathbb{Z}[i]$ are integral domains which are not fields. If $n = p$ is prime, then $\mathbb{Z}/p\mathbb{Z}$ is a field (also denoted $\mathbb{F}_p$). If n is not prime then $\mathbb{Z}/n\mathbb{Z}$ is not an integral domain.

1.6. If R is any ring we write R^* for the set of invertible elements (or *units*) of R. It is a group under multiplication. For example, $\mathbb{Z}^* = \{\pm 1\}$. If F is a field then $F^* = F \setminus \{0\}$.

2 Homomorphisms and ideals

2.1. By a ring homomorphism we shall always mean a mapping $\phi \colon R \to S$ between two rings such that:

(i) for every x, $y \in R$, $\phi(x + y) = \phi(x) + \phi(y)$ and $\phi(xy) = \phi(x)\phi(y)$; and

(ii) $\phi(1) = 1$.

Associated to a homomorphism $\phi \colon R \to S$ are:

- its *kernel*, defined as: $\ker(\phi) = \{x \in R \mid \phi(x) = 0\} \subset R$

- its *image*, defined as: $\mathrm{im}(\phi) = \{\phi(x) \mid x \in R\} \subset S$.

The homomorphism ϕ is injective iff $\ker(\phi) = 0$, and is surjective iff $\mathrm{im}(\phi) = S$. The image of ϕ is a subring of S.

2.2 Definition. An *ideal* of a ring R is a subset $I \subset R$ satisfying:

(i) I is a subgroup of R under addition;

(ii) for every $x \in R$ and $y \in I$, $xy \in I$.

2.3 Examples. In any ring R, R and $\{0\}$ are ideals. Let R be any ring and $a \in R$. Write (a) or aR for the subset $\{ax \mid x \in R\}$. Then (a) is an ideal of R. This is called the *ideal generated by* a. Any ideal of this form is said to be *principal*. In particular, the ideals $R = (1)$ and $\{0\} = (0)$ are principal.

2.4 Proposition. *A ring R is a field iff it is nonzero and its only ideals are* (0) *and* R.

Proof. Let R be a field, and $I \subset R$ a nonzero ideal. Let $x \in I$ with $x \neq 0$; then $x^{-1} \in R$ and so $1 = x^{-1}x \in I$, hence $I = R$. Conversely, let R be a ring with no ideals other than (0) and R. Let $x \in R$ with $x \neq 0$. Then (x) is a nonzero ideal of R, hence $(x) = R$, which implies that $xy = 1$ for some $y \in R$. Therefore R is a field. □

2.5 Proposition. *Let $\phi\colon R \to S$ be a homomorphism. Then* $\ker(\phi)$ *is an ideal of* R. *Moreover* $\ker(\phi) \neq R$ *unless S is a zero ring.*

2.6. Combining these two facts, one sees that any ring homomorphism $\phi\colon F \to K$ between fields is injective.

2.7. The converse is true: every ideal of R is the kernel of some suitable homomorphism. In fact, given an ideal $I \subset R$, define an equivalence relation on R by

$$x \equiv y \pmod{I} \iff x - y \in I.$$

Let R/I be the set of equivalence classes. If $x \in R$ denote by $\bar{x} \in R/I$ the equivalence class containing x. The conditions (i) and (ii) in the definition 2.2 imply that:

$$\left.\begin{cases} x \equiv x' \pmod{I} \\ y \equiv y' \pmod{I} \end{cases}\right\} \implies \left\{\begin{matrix} x + y \equiv x' + y' \pmod{I} \\ xy \equiv x'y' \pmod{I} \end{matrix}\right\}$$

(for the second identity, notice that $x'y' - xy = x'(y' - y) + y(x' - x) \in I$). This means that we can unambiguously define operations $+$ and $\times$ on R/I by the formulae $\bar{x} + \bar{y} = \overline{x + y}$, $\bar{x} \times \bar{y} = \overline{xy}$, which give R/I the structure of a ring, called the *quotient ring* of R by I. (This is just a generalisation of the construction of $\mathbb{Z}/n\mathbb{Z}$.) The map

$$\begin{aligned} \psi\colon R &\to R/I \\ x &\mapsto \bar{x} \end{aligned}$$

is then a homomorphism, whose kernel is I.

2.8. There is a bijection between the set of ideals of R/I and the set of ideals of R containing I; if $I \subset J \subset R$ then the corresponding ideal of R/I is J/I, and if $\bar{J} \subset R/I$ is an ideal the corresponding ideal of R is

$$\psi^{-1}(J) = \{x \in R \mid \bar{x} \in \bar{J}\}.$$

2.9. An *isomorphism* of rings is a ring homomorphism $\phi\colon R \to S$ such that there is a ring homomorphism $\psi\colon S \to R$ for which $\psi \circ \phi = id_R$ and $\phi \circ \psi = id_S$. This is equivalent to requiring that ϕ be a bijection. Isomorphisms are usually denoted $\xrightarrow{\sim}$.

2.10 Theorem (First Isomorphism Theorem). *Let $\phi\colon R \to S$ be a ring homomorphism. Then there is a unique isomorphism $\psi\colon R/\ker(\phi) \xrightarrow{\sim} \operatorname{im}(\phi)$ such that for every $x \in R$, $\phi(x) = \psi(\bar{x})$.*

2.11. A ideal $I \subset R$ is said to be *prime* if $I \neq R$ and:

- whenever $x, y \in R$ with $xy \in I$, at least one of x, y belongs to I

2.12 Proposition. *An ideal $I \subset R$ is prime iff R/I is an integral domain.*

Proof. We have $x \in I \iff \bar{x} = 0$. This shows that the definitions are equivalent. □

2.13. An ideal $I \subset R$ is *maximal* if $R \neq I$ and there is no ideal J with $I \subsetneq J \subsetneq R$.

2.14 Proposition. *An ideal $I \subset R$ is maximal iff R/I is a field. (Hence maximal $\implies$ prime.)*

Proof. By 2.8, I is maximal iff the only ideals of R/I are R/I and (0), hence by 2.4 iff R/I is a field. □

3 Polynomials and rational functions

3.1. Let R be a ring and n a positive integer. The *polynomial ring* in the variables $X_1, \ldots, X_n$ is the ring $R[X_1, \ldots, X_n]$ whose elements are finite formal sums (for some $N \in \mathbb{N}$)

$$\sum_{0 \leq i_1, \ldots, i_n \leq N} a_{i_1, \ldots, i_n} X_1^{i_1} \cdots X_n^{i_n}$$

where $a_{i_1, \ldots, i_n} \in R$, and multiplication and addition are defined in the obvious way. If R is an integral domain then so is $R[X_1, \ldots, X_n]$, and in this case the units of $R[X_1, \ldots, X_n]$ are just R^* (this is not true for general rings R).

3.2. If F is a field, then the *field of rational functions* over F is

$$F(X_1, \ldots, X_n) = \left\{ \frac{f}{g} \;\middle|\; f, g \in F[X_1, \ldots, X_n],\ g \neq 0 \right\}.$$

It is the field of fractions of $F[X_1, \ldots, X_n]$.

3.3 Theorem. *Let F be a field, $F[X]$ the polynomial ring in one variable. Then:*

(i) every ideal of $F[X]$ is principal (i.e. $F[X]$ is a UFD); and

(ii) if $f \in F[X]$ is a nonzero polynomial, then (f) is prime $\iff$ (f) is maximal $\iff$ f is irreducible.

Proof. (i) Let I be a nonzero ideal of $F[X]$. Choose $f \in I$ to be nonzero with minimal degree. Then I claim that $I = (f)$. Indeed, if $g \in I$ then there exist $q, r \in F[X]$ with $g = qf + r$ and $\deg(r) < \deg(f)$ (by the division algorithm in $F[X]$). As I is an ideal, $r = g - qf \in I$, and as f was chosen to have minimal degree among the nonzero elements of I, we must have $r = 0$, so that $g = qf \in (f)$. (This argument shows that $F[X]$ is a Euclidean domain, hence a UFD.)

(ii) Suppose f is irreducible. Then let I be an ideal with $(f) \subset I \subset F[X]$. By (i), $I = (g)$ is principal, so $f \in (g)$, which means $f = gh$ for some $h \in F[X]$. As f is irreducible either g is constant, in which case $(g) = R$, or h is constant, in which case $(g) = (f)$. Therefore (f) is maximal.

If (f) is maximal then it is certainly prime, so it remains to show that if (f) is prime, f is irreducible. Suppose not. Then $f = gh$ for some nonzero polynomials g, h of degree less than $\deg(f)$. Then $g, h \notin (f)$ but $gh \in (f)$, hence (f) is not prime. □

3.4 Theorem (Gauss's Lemma). *Let R be a unique factorisation domain with field of fractions F. Let $f \in R[X]$, and assume that f is not divisible by any non-unit of R. Then f is irreducible in $R[X]$ iff f is irreducible in $F[X]$.*

(We'll only need the case $R = \mathbb{Z}$, $F = \mathbb{Q}$, but the general case is no harder to prove.)

Proof. One direction is easy: suppose f is irreducible in $F[X]$. Then it has no nonconstant factors in $R[X]$ of degree less than $\deg(f)$. So by hypothesis it is irreducible in $R[X]$.

For any polynomial $f = a_0 + a_1 X + \cdots + a_n X^n \in R[X] \setminus \{0\}$, define its *content* $\operatorname{cont}(f)$ to be the gcd of $\{a_0, \ldots, a_n\}$ (well-defined up to multiplication by a unit in R). If $c = \operatorname{cont}(f)$ then $c^{-1} f \in R[X]$ and $\operatorname{cont}(c^{-1} f) \in R^*$. We prove:

$$\text{If } f,\, g \in R[X] \text{ then } \operatorname{cont}(fg) = \operatorname{cont}(f) \operatorname{cont}(g).$$

For this, first divide f and g by their contents, so that we may assume that $\operatorname{cont}(f) = \operatorname{cont}(g) = 1$. We need to show that $\operatorname{cont}(fg) \in R^*$. If not, there exists an irreducible $\pi \in R$ with $\pi | \operatorname{cont}(fg)$. Let

$$f = \sum_{i=0}^{m} a_i X^i, \quad g = \sum_{j=0}^{n} b_j X^j, \quad fg = \sum_{k=0}^{m+n} c_k X^k.$$

Thus we have

$$c_k = \sum_{i=0}^{k} a_i b_{k-i}.$$

As $\operatorname{cont}(f) = \operatorname{cont}(g) = 1$ not all the a_i and not all the b_j are divisible by π. Choose i and j minimal such that $\pi \nmid a_i$ and $\pi \nmid b_j$. Then $\pi \nmid a_i b_j$, and in the formula for c_{i+j}, every term is divisible by π except for the term $a_i b_j$. So $\pi \nmid c_{i+j}$, a contradiction.

Now suppose $f \in R[X]$ is reducible in $F[X]$. Then there exist nonconstant $g, h \in F[X]$ with $f = gh$. We can therefore write $af = b g_1 h_1$ where $a,\, b \in R \setminus \{0\}$ and $g_1,\, h_1 \in R[X]$ with $\operatorname{cont}(g_1) = \operatorname{cont}(h_1) = 1$. So $\operatorname{cont}(af) = \operatorname{cont}(b g_1 h_1) = b$ by what was just proved, and therefore $a | b$. So $f = (b/a) g_1 h_1$ is reducible in $R[X]$. □

3.5 Theorem (Eisenstein's Criterion for Irreducibility). *Let p be a prime number and $f = X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$ a monic polynomial of degree $n \geq 1$ such that:*

(i) Every a_i is divisible by p;

(ii) a_0 is not divisible by p^2.

Then f is irreducible in $\mathbb{Z}[X]$ (hence in $\mathbb{Q}[X]$ by Gauss's Lemma).

Proof. Suppose $f = gh$ with $g,\, h \in \mathbb{Z}[X]$. We may assume that g and h are monic of degrees m, $n - m$ respectively, where $0 < m < n$. Write $\bar{\ }$ for reduction modulo p, and consider the "reduction modulo p" homomorphism

$$\begin{aligned} \mathbb{Z}[X] &\to \mathbb{F}_p[X] \\ \sum b_i X^i &\mapsto \sum \overline{b_i} X^i \end{aligned}$$

Then $\bar{g}$ and $\bar{h}$ also have degrees m, $n - m$ and $\bar{g}\bar{h} = \bar{f} = X^n$ (by hypothesis (i)). Since $\mathbb{F}_p[X]$ is a UFD this forces $\bar{g} = X^m$, $\bar{h} = X^{n-m}$. Therefore $g(0) \equiv h(0) \equiv 0 \pmod{p}$, hence $a_0 = f(0) = g(0)h(0) \equiv 0 \pmod{p^2}$, contradicting (ii). □

The argument just given proves the following more general statement: let R be a ring and $I \subset R$ a maximal ideal. Let $f = X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \in R[X]$ with all $a_i \in I$ and $a_0 \notin I^2$. Then f is irreducible in $R[X]$.

3.6 Example. If p is prime, $(X^p - 1)/(X - 1) = X^{p-1} + \cdots + X + 1$ is irreducible in $\mathbb{Q}[X]$. (Put $T = X - 1$, so the polynomial becomes $\sum_{i=0}^{p-1} \binom{p}{i+1} T^i$ which satisfies (i) and (ii).)