Galois theory, lecture 2
lecture notes

28 januari 2013

Examination

The course webpage is `www.math.kth.se/math/GRU/2012.2013/SF2732/` The examination consists of two homework problems and an exam. The homework problem are worth 12 points, ... The book is *Algebra* by Serge Lang.

---

1 Summary of last lecture

Recall that r is *irreducible* if $r = ab \implies a$ is a unit or b is a unit.

Theorem 1.
- *If R is an UFD, then a non zero element $r \in R$ is prime iff r is irreducible.*
- *If R is a UFD, then so is $R[x]$. (This can be proved by Gauss lemma.)*
- *If R is a PID, then R is a UFD.*
- *$R[x]$ is PID iff R is a field. (R - field $\implies R[x]$ PID is easy, the proof $R[x]$ - PID $\implies R$ - field is below:*

Assume $R[x]$ is PID, let $0 \neq r \in R$. We will show that r is invertible.[1]

To give a concrete example, why is $\mathbb{Z}[X]$ not a PID? Easy - just find an ideal minimally generated by at least two elements. After some experimentation, the simplest I could come up with was $(2, X)$.

For a general PID, we are to prove that every nonzero r with $\deg r = 0$ is invertible. We will show that if r is not invertible, we would get an ideal minimlly generated by two elemnts. Let r be a nonzero prime $\iff$ irreducible element of degree 0 (it is enough to prove that the primes are invertible, then everything else is invertible to). Then consider the ideal $(r, X) = \{a_0 + a_1 X \ldots + a_n Xn : r | a_0\}$. We have $(r) \subset (r, X)$. By assumption, $R[x]$ is a PID, so there is $a \in R[x]$ with $(a) = (r, X)$. But then $\deg a = 0$, and $a | r$. It follows that a and r are associates, so $(r) = (r, X)$. The polynomial $r + X \in (r, X)$, so $r + X = (\alpha + \beta x) r$ and β has to be the inverse of r. This proves that every prime element r is invertible, and since every element is a product of primes, every element is invertible.

[1] The red boxes are my own notes from after the lecture that explains something I havn't seen earlier, or had trouble understanding, or trouble to follow or something that the lecturer skipped during the lecture

Theorem 2. *If F is a field, then $F[x]$ is PID, $F[X,Y]$ is UFD.*

*$F[x]$ **is PID**:*
Let $I \subset F[X]$ be an ideal, let $p(x)$ be a polynomial of minimal degree in I. Then by the division algorithm, every polynomial $s(x)$ in I can be written as $s = pq + r$ with $r = 0$ or $\deg r < \deg p$. But then $r \in I$ so $r = 0$ and $I = (p)$.

The second claim follows from R - UDF $\Longrightarrow$ $R[X]$ - UDF and from the fact that $F[X]$ is UFD.

2 Lecture 2

Proposition 1. *Let $r \in R$ be a prime element (equivalently $R/(r)$ is a domain or $r|a \cdot b \Longrightarrow r|a$ or $r|b$.) Then $R/(r)$ is a field.*

Bevis. Take $S + (r) \in R/(r) \neq 0$ (that is $r \nmid s$) Consider the ideal $(r,s) = (t) \subset R$. Then $t|r$ and $t|s$. From this we get $r = t \cdot w$. We know $r \nmid t$, so $r|w$. We get $r|w \Longrightarrow r = tvr \Longrightarrow$. We want to find $ar + bs = 1$, then $(b + (r))(s + (r)) = 1 + (r)$. □

Take $\mathbb{Z}$ and a prime $p \in \mathbb{Z}$ Then the above theorem tells us that $\mathbb{Z}/(p)$ is a field.

Another example is hen F is a field, $f \in F[X]$ is an irreducible element. Then $F[X]/(f)$ is a field.

Note: The whole course is about constructing new fields from other fields. One way to do this is to quotient a PID by irreducible element. To be able to do this, we need methods to determine when an element of a ring is irreducible. This is a hard problem. Consider this example:

Example 1. *Is the polynomial $X^2 + 1$ irredubcible in $\mathbb{Q}[X], \mathbb{R}[X], \mathbb{C}[X], \left(\mathbb{Z}/(2)\right)[X]$?*

- *In $\mathbb{Q}[X]$, $X^2 + 1$ is irreducible.*
- *In $\mathbb{R}[X]$, it is irreducible.*
- *In $\mathbb{C}[X], x^2 + 1 = (x - i)(x + i)$*
- *in $\left(\mathbb{Z}/(2)\right)[x], x^2 + 1 = (x + 1)^2$*

Let R be a domain, recall that its field of fractions can be constructed from all pairs $(r_1, r_2) \in R^2$ with $r_2 \neq 0$. On these pairs, we define an equivalence ralation,

$$(a,b) \sim (c,d) \text{ if } ad = bc$$

We denote the equivalence of (a,b) by $\frac{a}{b}$. The definition of $\sim$ tells us that

$$\frac{a}{b} = \frac{c}{d} \text{ if } ad = bc$$

so these 'fractions' behave just as usual fractions in $\mathbb{Q}$ or $\mathbb{R}$. These fractions form a ring under addition

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

and multiplication

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

The class of $(0,1)$, the fraction $\frac{0}{1}$, acts as 0, and $\frac{1}{1}$ has the role of 1.

To verify that the construction works, we have to check that if $s = \frac{a}{b}$, and $s' = \frac{a'}{b'}$, then $s = s' \Longrightarrow s + t = s' + t$. This transaletes into

$$ab' + a'b = 0 \Longrightarrow \frac{ad + bc}{bd} = \frac{a'd + b'c}{b'd}$$

and this can be proven by doing some algebraic calculations. This construction is called the **field of fractions** of R.

Eisentnein's criterion

Let R be a UFD and K its field of fractions. Let $f = a_0 + a_1 x + \ldots + a_n x^n \in R[x] \subset K[x]$ (coefficients in R). We want to know when f is irreducible in $K[x]$.

Theorem 3. *Assume that there is a prime $p \neq 0 \in R$ such that $p \nmid a_n, p | a_i 0 \leq i < n, p^2 \nmid a_0$. Then f is irreducible in $K[x]$.*

First, an example:

Example 2. *Is the polynomial $g = x^4 + x^3 + x^2 + x + 1 \in \mathbb{Q}[x]$ irreducible?*

By Eisensteins criterion, $f = x^4 + 5x^3 + 10x^2 + 10x + 5$ is irreducible. But $g(x+1) = f(x)$, so g is irreducible.

Homomorphisms of polynomials rings

Theorem 4. *Let $f : R \longrightarrow S$ be a ring homomorphism. (By ring homomorphism we mean a map that maps $0 \mapsto 0$, $1 \mapsto 1$, preserves addition and multiplication.) Then for every $s \in S$, there is a unique ring homomorphism $\overline{f} : R[x] \longrightarrow S$ such that $\overline{f}(r) = f(r)$ and $\overline{f}(x) = s$.*

Field extensions

We will study the case $F \hookrightarrow E$ or (denoted E vertical line down to F)

Let $f \subset E, \alpha_1 \ldots \alpha n \in E$. Then construct $F \hookrightarrow F[\alpha_1, \ldots, \alpha_n] \hookrightarrow F(\alpha_1, \ldots, \alpha_n) \subset E$. By $F[\alpha_1, \ldots, \alpha_n]$, we mean the smallest ring containing F and $\alpha_1, \ldots, \alpha_n$. By $F(\alpha_1, \ldots, \alpha_n)$, we mean the smallest field that contains $F, \alpha_1, \ldots \alpha_n$. $F[\alpha_1, \ldots, \alpha_n]$ contains all linear combinations of monomials $\alpha_1^{k_1} \ldots \alpha_n^{k_n}$. $F(\alpha_1, \ldots, \alpha_n)$ also contains all inverses of the α_i:s.

Definition 1. $F \subset E$ *is* ***finitely generated*** *if there are $\alpha_r \ldots \alpha_n$ in E such that $E = F(\alpha_1, \ldots, \alpha_n)$*

A natural question we might ask is if a composition of finite generated extensions is finitely generated. This is a rather hard question.

Definition 2. *$F \subset E$ is **finite extension** if, as a vector space over F, E is finite-dimensional. In this case, we denote* $\dim_F(E) = [E : F]$.

The standard questions here is again, if E is a finite extension of F and K is a finite extension of E, **is K a finite extension of E?** and **if it is, what is $[K : F]$?**. This is a relatively easy question to answer.

---

assume $e_1, \dots e_n$ is a base of E over F and $k_1, \dots, k_m$ is a finite base of K over E. We claim that $\{e_i \cdot k_j\}_{1 \leq i \leq n, 1 \leq j \leq m}$ is a base of K over F. We have to prove that everything in K is a linear combination of the $\{e_i \cdot k_j\}$ and that the $\{e_i \cdot k_j\}$ are linearly independent. We write $k = a_1 k_1 + \dots a_m k_m$ with $a_i \in E$. Now we write each $a_i = (a_{i,1} e_1 + \dots + a_{i,n} e_n)$, expand and are done.

But are the $\{e_i k_j\}$ linearly independent? Assume there is a sum $\sum_{i,j} a_{i,j} e_i k_j = 0$ with coefficients $a_{i,j} \in F$. We write the sum as $\sum_j k_j (\sum_i a_{i,j} e_i) = 0$. The k_j are linearly independent over E, so all the coefficients $\sum_i a_{i,j} e_i$ are 0. But the e_i are linearly independent over F, so all $a_{i,j} = 0$ which is what we wanted.

We proved that if $F \subset E \subset K$, then $[K : F] = [E : F][K : E]$. We also showed that if $\{e_i\}$ is a basis for E as a vector space over F, and $\{k_j\}$ is a basis for K as a v-space over E, then $\{e_i k_j\}$ is a basis for K over F.

Other standard questions:
If $F \subset E \subset K$, and $F \subset K$ is finite, is $F \subset E, E \subset K$ finite? The answer is that everything is finite and that $[E : F] | [K : F]$, $[K : E] | [K : F]$, $[K : F] = [K : E][E : F]$.

When we know $[K : F]$, there are not many choices for the dimension of $F \hookrightarrow E \hookrightarrow K$

Algebraic extenions

Definition 3. *Let $F \hookrightarrow E$ be a field extension and $\alpha \in E$. We consider*

$$F \hookrightarrow F[\alpha] \hookrightarrow F(\alpha) \subset E$$

*Lookt at $F \hookrightarrow F[x] \longrightarrow F[\alpha]$ where $\phi : F[x] \longrightarrow F[\alpha]$ is the unique surjective ring homomorphism where $x \mapsto \alpha$. If ϕ is an isomorphism, we call α **trancendental**. If* $\ker \phi = (f)$*, we call α **algebraic** and the irreducible polynomial f the **minimal polynomial** of α over F. When α is algebraic, $F[\alpha]$ is a field and* $[F[\alpha] = F(\alpha) : F] = \deg f$.

Definition 4.