2019-04-12

COLTON GRAINGER

Ideas behind the fundamental theorem of Galois theory. Recall: in favorable conditions, the degree $|\mathrm{Aut}(K/F)| \leq [K : F]$. If K/F is Galois, then we have equality.

Let K/F be a Galois extension over a field F. The following are equivalent.

- The automorphism group $\mathrm{Aut}(K/F)$ is "sufficiently big".
- The action of $\mathrm{Aut}(K/F)$ on K has stabilizer subgroup $\mathrm{Stab}_{\mathrm{Aut}(K/F)}(F) = \mathrm{Aut}(K/F)$.
- $|\mathrm{Aut}(K/F)| = [K : F]$.

The fundamental theorem of Galois theory claims that there's a *bijective* and *order-reversing* correspondence between the subfields of K/F and the subgroups of $\mathrm{Gal}(K/F)$.

For example, the groups lattice of subgroups $1 \leq H \leq G$ corresponds to the lattice of field extensions $K \geq E \geq F$. That is:

$$\begin{array}{ccc} K[rr] & & 1 \\ \uparrow & & \downarrow \\ E[rr] & & H \\ \uparrow & & \downarrow \\ F[rr] & & G \end{array}$$

the degree of K/E is H, with

Moreover, $[E : F] = [G : H]$. K/E is also Galois, with $\mathrm{Gal}(K/E) = H$.

$$E \quad \text{is Galois over } F \text{ iff} \quad H \quad \text{is normal in} \quad G.$$

Example $\mathbf{Q}(\sqrt[3]{2}, \omega)$. Recall that the minimal polynomial of $\mathbf{Q}(\sqrt[3]{2}, \omega)$ over $\mathbf{Q}$ is $x^3 - 2$.

We have the tower of extensions **TODO**. Consider that $\mathbf{Q}(\sqrt[3]{2}) \leq \mathbf{Q}(\sqrt[3]{2}, \omega)$, but there's $\sigma \in \mathrm{Aut}(\mathbf{Q}(\sqrt[3]{2}, \omega)/\mathbf{Q})$ that takes $\sigma(\mathbf{Q}(\sqrt[3]{2})) = \mathbf{Q}(\sqrt[3]{2}\omega)$. (In other words, the fields $\mathbf{Q}(\sqrt[3]{2}\omega^k)$ for $k = 0, 1, 2$ correspond to the 2-cycles in S_3.

Lattice isomorphisms. What's the largest subfield contained in the subfields E_1, E_2 of K? It's the intersection. How about the largest subfield containing both E_1 and E_2? It's the composite in K. Correspondingly, for the subgroups G_1 and G_2 of $\mathrm{Aut}(K/F)$ fixing E_1 and E_2, the subgroup $G_1 \cap G_2$ fixes the composite, and the subgroup $\langle G_1, G_2 \rangle$ fixes the intersection. **TODO**

Finite fields. Exercise: prove that the algebraic closure of a field is an infinite degree extension.

Fact: consider the algebraic closure $\mathbf{F}_p^a$ of $\mathbf{F}_p$. Since $\mathbf{F}_{p^n}/\mathbf{F}_p$ is an algebraic extension, we have

$$\mathbf{F}_{p^n} \quad \text{contained in} \quad \mathbf{F}_p^a.$$

Idea: there *is* a *non-algebraic* extension of $\mathbf{C}$, e.g., $\mathbf{C}(t)$, the polynomial ring.

Date: 2019-04-12.

Consider that $\mathbf{F}_{p^n}/\mathbf{F}_p$ is an algebraic extension, since $\mathbf{F}_{p^n}$ is the splitting field of $x^{p^n} - x$ over $\mathbf{F}_p$. Whence $\mathbf{F}_{p^n}/\mathbf{F}_p$ is a *Galois* extension. So also

$$|\mathrm{Gal}(\mathbf{F}_{p^n}/\mathbf{F}_p)| = n.$$

Consider the Froebenius automorphism $\Phi\colon \mathbf{F}_{p^n} \to \mathbf{F}_p$ defined by $\Phi(a) = a^p$. Note (by Fermat's little theorem) Φ fixes $\mathbf{F}_p$ (this in general holds for prime subfields). Now we have

$$\Phi \in \mathrm{Gal}(\mathbf{F}_{p^n}/\mathbf{F}_p) \quad \text{and} \quad \Phi^k = \mathrm{id} \quad \text{iff} \quad n \mid k.$$

Proof. If $\Phi^k = \mathrm{id}$, then $\alpha^{p^k} - \alpha = 0$ for all $\alpha \in \mathbf{F}_{p^n}$. But there are not enough roots! **TODO** tighten up. □

Thus $\mathrm{Gal}(\mathbf{F}_{p^n}/\mathbf{F}_p)$ is cyclic, finitely generated by Φ.

Consider the tower $\mathbf{F}_{p^n} \geq \mathbf{F}_{p^k} \geq \mathbf{F}_p$. The degrees of the extensions are n/k and k respectively, where we *must have* $k \mid n$. The corresponding subgroups are $1 \leq$ cyclic of order $n/k \leq$ cyclic of order n. The generators are thence $\langle \Phi^n \rangle \leq \langle \Phi^k \rangle \leq \langle \Phi \rangle$.

Proof. (Consider Lagrange's theorem.)

Moral. What Galois groups can appear as automorphism groups of extensions of finite fields? Only cyclic groups.

Example $\mathbf{Q}(\sqrt{2}, \sqrt{3}) = \mathbf{Q}(\sqrt{2} + \sqrt{3})$.

Consider $\mathbf{F}_{p^n}$, a *simple* extension of $\mathbf{F}_p$. *Proof.* Let α be a generator of $\mathbf{F}_{p^n}^\times$. Since the finite subgroups of the group of units of a field is cyclic, and the group $\mathbf{F}_{p^n}^\times$ *is finite*. Then $\mathbf{F}_{p^n} = \mathbf{F}_p(\alpha)$.

But how to find α?

- Randomly? (c.f. stackexchange.)
- Observe that the minimal polynomial of α (such that $\mathbf{F}_p(\alpha)$ is a degree n extension) has degree n.
- Proposition. **TODO** For any n, there's a irreducible polynomial of degree n over $\mathbf{F}_p$.

Consider the tower

$$\begin{tikzcd}
\mathbf{F}_{p^n} = \mathbf{F}_p(\alpha) \arrow[d] \\
E = \mathbf{F}_p(\beta) \arrow[d] \\
\mathbf{F}_p
\end{tikzcd}$$

With the degree of α equal to n, and the degree of β equal to d, we have $d \mid n$. But also the minimal polynomials $m_\alpha(x)$ and $m_\beta(x)$ both *divide* $x^{p^n} - x \in \mathbf{F}_p[x]$.

Proof. Suppose $m(x)$ is an irreducible factor of $x^{p^n} - x$. Let γ be a root of $m(x)$ in $\mathbf{F}_{p^n}$ of degree d. Consider:

$$\begin{tikzcd}
\mathbf{F}_{p^n} \arrow[dd, "n"'] \arrow[dr, "n/d"] & \\
& \mathbf{F}_p(\gamma) \arrow[dl, "d"] \\
\mathbf{F}_p &
\end{tikzcd}$$

Thence $d \mid n$.

Conversely, if we have an irreducible polynomial of degree d over $\mathbf{F}_p$ and $d \mid n$, then every element of $\mathbf{F}_p(\gamma)$ has degree dividing d.

$$\gamma^{p^d} - \gamma = 0 \quad \gamma \in \mathbf{F}_{p^d}.$$

Example. Factorize $x^8 - x$ over $\mathbf{F}_2$. Consider $x^{2^3} - x$. We've a degree 8 polynomial. So consider

$$\begin{aligned} x^8 - x &= x(x^{-}1) \\ &= x(x-1)(x^6 + x^5 + \cdots + 1). \end{aligned}$$

What a chore?! Instead with $p = 2$ and $n = 3$. We've have a table

poly	irreduc?
$x^3 + 1$	no (-1 is a root)
$x^3 + x^2 + 1$	yes
$x^3 + x + 1$	yes
$x^3 + x^2 + x + 1$	no (-1 is a root)

Therefore $x(x+1)(x^3 + x + 1)(x^3 + x^2 + 1) = x^8 - x$. $\square$

Example $x^4+1 \in \mathbf{Z}[x]$. TODO Show that this polynomial is reducible, but modulo any prime p, irreducible.