Nepal Algebra Project(NAP)
Fields and Galois Theory "multiple hands" course in Nepal
Central Department of Mathematics
Tribhuvan University,Kirtipur, Kathmandu, Nepal
Course Instructor: Roger and Sylvia Wiegand

NAP: Module -2, Lecture -5, Wednesday, 24 May, 2017

- We finished the proof of Artin's Theorem (which should probably be called a lemma). The lemma (Theorem 3.4) is the technical crux of the argument, but the real theorem is Corollary 3.5: For a finite group G of automorphisms of a field E we have $G = \mathrm{Aut}(E/E^G)$. Also, we pointed out that the inequality in Theorem 3.4 is actually an equality: $[E : E^G] = |G|$.

- We did Proposition 3.2.

- We defined "separable", "normal", and "Galois" extensions and gave several examples to illustrate. Informally, "Galois" means that there are enough automorphisms to make the fixed field as small as possible. To get enough automorphisms, you need enough roots, and "separable" and "normal" help provide these roots.

- These ideas become formalized in Theorem 3.10, which we stated and proved. The part of the argument (in proving (b) $\implies$ (c)) involving symmetric polynomials might have been a little hard going for people not familiar with these things. Another approach might be to point out that G acts on $E[X]$ by taking X to X. The elements $\alpha_1, \ldots, \alpha_m$ are the distinct images of α under the action of G, and the action of G just permutes these elements. Therefore $g(X) = (X - \alpha_1) \cdots (X - \alpha_m)$ is fixed by the action of G and hence is in $F[X]$. Milne is a bit careless in the proof that (c) $\implies$ (a). It could happen that $f_1 = f_2$, for example, and this would prevent the product f from being separable. Easy remedy: Just define f as the product of the *distinct* polynomials among the f_i. Then, for $i \neq j$, the polynomials f_i and f_j, being distinct monic irreducible polynomials, are relatively prime, and hence by "permanence of gcd" cannot have a common root in any extension.

- We did Corollary 3.13: If $E \supset M \subset F$ is a tower of fields and E/F is Galois, then so is E/M. (However, the example $\mathbb{Q}(\sqrt[3]{2}) \supset \mathbb{Q}(\sqrt[3]{2}) \supset \mathbb{Q}$ shows that M/F is not necessarily Galois.)

- We gave a brief "preview" of FTGT (the fundamental theorem) and mentioned that the terminology "normal" for field extensions is not an accident; it has to do with normality of subgroups. Next time: FTGT and illustrations.

- Confession: The solution we gave for Problem 9 in Homework #1 was not quite in line with the instructions, since we had extensions $\mathbb{Q}(\alpha_1, \alpha_2)$ and $\mathbb{Q}(\alpha_1, \alpha_3)$. The repetition of $\alpha 1$ was definitely bad form. Mahdav Sharma pointed out that $X^8 - 2$ works: The eight roots are $\zeta^j \alpha\,, 0 \leq j \leq 7$, where $\alpha = \sqrt[8]{2}$ and $\zeta = \frac{1}{\sqrt{2}}(1 + i)$. Now take these four roots: $\zeta\alpha, -\zeta\alpha = \zeta^4\alpha, \alpha, i\alpha = \zeta^2\alpha$. Then $[\mathbb{Q}(\zeta\alpha, -\zeta\alpha) : \mathbb{Q}] = 8$, while $[\mathbb{Q}(\alpha, i\alpha) = 16$. Probably there are examples with $\deg f = 6$. Are there examples with $\deg f = 4$? (We don't know.)