KMB, December 8, 2013

M3P11 Galois Theory, Problem Sheet 6

1. Say a positive integer is *squarefree* if it is the product of distinct prime numbers.

(i) Say $a, b > 1$ are distinct squarefree integers. Prove $x^2 - a$ is irreducible, so $\mathbb{Q}(\sqrt{a})$ has degree 2 over $\mathbb{Q}$. Now prove that $\sqrt{b} \notin \mathbb{Q}(\sqrt{a})$.

(ii) Let F be the splitting field of $(x^2 - a)(x^2 - b)$ over $\mathbb{Q}$. What is $\mathrm{Gal}(F/\mathbb{Q})$? Use the fundamental theorem of Galois theory to find all the fields K with $\mathbb{Q} \subseteq K \subseteq F$. Which ones are normal over $\mathbb{Q}$?

(iii) Prove that $F = \mathbb{Q}(\sqrt{a} + \sqrt{b})$. Hint: figure out which subgroup of the Galois group this field corresponds to.

(iv) Let p, q and r be distinct primes. Prove $\sqrt{r} \notin \mathbb{Q}(\sqrt{p}, \sqrt{q})$. Hint: use the previous part. Meta-hint: if you're ever stuck on an example sheet or an exam question, consider using the previous part.

(v) Conclude that if $F = \mathbb{Q}(\sqrt{p}, \sqrt{q}, \sqrt{r})$ then $[F : \mathbb{Q}] = 8$. What is $\mathrm{Gal}(F/\mathbb{Q})$?

(vi) (long) If you can be bothered, then use the fundamental theorem of Galois theory to write down all the intermediate subfields between $\mathbb{Q}$ and F. If you can't then just write down the subfields E of F with $[E : \mathbb{Q}] = 2$ – but even that is quite tedious.

(vi) Show that (notation as in the previous part) $F = \mathbb{Q}(\sqrt{p} + \sqrt{q} + \sqrt{r})$.

(vii) Prove that if p_1, p_2,...,p_n are distinct primes, then $\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_n})$ has degree 2^n over $\mathbb{Q}$, and equals $\mathbb{Q}(\sqrt{p_1} + \sqrt{p_2} + \cdots + \sqrt{p_n})$.

2. (i) Say F is the splitting field of $x^3 - 11$ over $\mathbb{Q}$. Figure out $\mathrm{Gal}(F/\mathbb{Q})$. List all the subfields of F. Which are normal over $\mathbb{Q}$?

(ii) If F is the splitting field of $x^4 - 11$, what is $\mathrm{Gal}(F/\mathbb{Q})$?

3. Say $r = \sqrt[11]{5^{1/3} + \sqrt{8^{1/5} + 6}} + 9^{1/7}$. Find a sequence of fields $\mathbb{Q} = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_n$ with $r \in F_n$ and such that for all i we have $F_i = F_{i-1}(\alpha_i)$ with $\alpha_i^{n_i} \in F_{i-1}$ for some positive integer n_i.

4. Let p be an odd prime number, and let F be the splitting field of $x^p - 1$. Prove that there is a unique subfield K of F with $[K : \mathbb{Q}] = 2$ (hint: Q7 of previous sheet, plus the fact that $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic). Say $K = \mathbb{Q}(\sqrt{n})$ with $|n|$ squarefree. Figure out n when $p = 3$. If you're good at pentagons (i.e., if you know what $\cos(72)$ is), figure out n when $p = 5$. What do you think the answer is in general? This is a number-theoretic question rather than a field-theoretic one, and there are tricks but they're tough to spot.

5. Say $F = E(\alpha)$ with $\alpha \in F$ algebraic over E and separable. Prove F/E is separable. Hint: separable degree. Warning: the first time I stated 6.4 I got it wrong – I corrected it in the lecture afterwards. It should say "If $F = E(\alpha)$ then $[F : E]_s \leq [F : E]$ with equality iff α is separable over E" (which is what I proved).

6.

Say $E \subseteq F$, and L and M are intermediate fields (i.e. $E \subseteq L, M \subseteq F$). Let $N := LM$ denote the smallest subfield of F containing L and M.

(i) If $L = E(\alpha_1, \ldots, \alpha_n)$ then prove $N = M(\alpha_1, \ldots, \alpha_n)$.

(ii) Now assume L/E and M/E are finite and Galois. Prove N/E is finite and Galois (hint: splitting field; Q5).

(iii) Prove that restriction of functions gives a natural injective group homomorphism from $\mathrm{Gal}(N/E)$ to $\mathrm{Gal}(L/E) \times \mathrm{Gal}(M/E)$. Is it always surjective?