KMB, v3, 24/3/16

M3P11 Galois Theory, Problem Sheet 6

[version 3: typos fixed in Q7 and Q8 (and solutions added)]

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 one of the previous parts. Meta-hint: if you're ever stuck on a part of an example sheet or an exam question, consider using one of the previous parts.

(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 $[E : \mathbb{Q}] = 2$.

(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. 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 $\mathbb{Q}$?

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. Let V be a finite-dimensional vector space over an infinite field K, and say W_1, W_2, ..., W_n are finitely many subspaces of V, with $W_i \neq V$ for all i. This question leads you through a proof of the fact that the union of the W_i cannot be all of V. We used this purely linear-algebra fact in the proof of the theorem of the primitive element (Corollary 6.11).

a) Say $w \in W_1$. Choose $v \notin W_1$ and consider the elements $v + \lambda w$ for $\lambda \in K$. Prove that none of these elements are in W_1.

b) Deduce that if V is the union of the W_i then (with notation as in (a)) there is some $i > 1$ such that W_i contains w (hint: find W_i that contains $v + \lambda w$ for two values of λ).

c) Proceed by induction on n to get a contradiction.

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 normal. Prove N/E is finite and normal. (hint: splitting field). Next assume L/E and M/E are finite and Galois. Prove that N/E is finite and Galois.

(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?

7. Let's prove that an extension by radicals always lives in an extension by radicals which is furthermore normal. In fact let's prove that if L/K is a finite extension of fields of characteristic zero which is an extension by radicals, and if M/K is its normal closure, then M/K is also an extension by radicals. We can even do more: let's assume that L/K is constructed by taking n'th roots only for integers n in some finite set S; then we'll show that the normal closure can also be constructed by taking n'th roots only for $n \in S$.

Here is a precise statement, made to set up some notation. Let K be a field of characteristic zero, say S is a finite set of positive integers, and say $K = L_0 \subseteq L_1 \subseteq L_2 \subseteq \cdots \subseteq L_q = L$ with $L_{i+1} = L_i(\alpha_i)$, and $\alpha_i^{n_i} \in L_i$ for some $n_i \in S$. The claim is that the normal closure M/K of L/K can be written $K = M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots \subseteq M_r = M$ with $M_{j+1} = M_j(\beta_j)$, and $\beta_j^{m_j} \in M_j$ for some $m_j \in S$.

a) Let $\overline{L}$ be an algebraic closure of L. Prove that there are only finitely many field maps $L \to \overline{L}$ which are the identity on K.

b) Let A_1, A_2, ..., A_N be the image of these field maps. Let M be the smallest subfield of $\overline{L}$ containing all the A_i. Prove that M is the normal closure of L/K. The definition of normal closure is on Sheet 4, Q6.

c) Say A, B and C are all subfields of a large field, and and $B = A(\alpha)$ for some $\alpha \in B$ such that $\alpha^n \in A$ for some positive integer n. Say $D = AC$, the smallest subfield containing A and C, and $E = BC$. Prove that $E = D(\alpha)$ and $\alpha^n \in D$.

d) Use (b) and (c) to prove the result we need.

8. (a) (mostly for people who have done or are doing the group theory course.) Regard S_3 (permutations of $\{1, 2, 3\}$) as a subgroup of S_4 (permutations of $\{1, 2, 3, 4\}$) in the obvious way. Prove that there is no subgroup H of order 12 in S_4 such that H contains S_3. Hint: if you've been to the group theory course then consider an element of H not in S_3 and ask where it sends 4. Now consider what the orbit of 4 must be under H. Now consider the stabiliser of 4 in H and convince yourself that it has order 3 but contains S_3, a contradiction.

(b) Let us *assume* that the polynomial $f(x) = x^4 - x - 1 \in \mathbb{Q}[x]$ is irreducible and that its splitting field $L/\mathbb{Q}$ has Galois group S_4. In fact I will remark that if you choose a random polynomial of degree 4 in $\mathbb{Q}[x]$ then with probability 1 (in some meaningful sense) it will be irreducible and the Galois group of its splitting field will be S_4, so in practice such polynomials are not hard to find! If you have access to a computer algebra package that will compute Galois groups of splitting fields of polynomials (for example pari-gp) then you can try this yourself.

Under this assumption, convince yourself that there an element $\alpha \in \mathbb{R}$ such that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ but that $\mathbb{Q}(\alpha)$ has no subfield of degre 2 over $\mathbb{Q}$. Indeed, for the polynomial $f(x) = x^4 - x - 1$ above, check that it has a real root (by evaluating $f(0)$) and show that letting α be a real root of $f(x)$ works.

(c) Prove that if E is a field of characteristic zero, and $E = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_n = F$ are a collection of field extensions such that $[F_{i+1} : F_i] = 2$ for all i, then the normal closure of F/E is Galois, with Galois group a group of 2-power order. Hint: Q7 of this sheet.

(d) Deduce that the statement "if (α, β) is constructible then $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}]$ is a power of 2" is not an iff (assuming that the splitting field of $x^4 - x - 1$ has Galois group S_4).

(e) To finish the job, read Keith Conrad's notes at `http://www.math.uconn.edu/~kconrad/blurbs/galoistheory/cubicquartic.pdf`, Example 3.2, to justify my assertion about the Galois group in (b).