AC, 11/02/18

M3P11 (or M4P11 or M5P11) Galois Theory, Problem Sheet 2

1. Prove that $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{-3}, \sqrt[3]{5})$ is a normal extension. What is its degree?

2. Establish (with proofs) whether the following extensions of $\mathbb{Q}$ are normal or not.
(i) $\mathbb{Q}(\sqrt{6})$
(ii) $\mathbb{Q}(\sqrt{2}, \sqrt{3})$
(iii) $\mathbb{Q}(7^{1/3})$
(iv) $\mathbb{Q}(7^{1/3}, e^{2\pi i/3})$
(v) $\mathbb{Q}(\sqrt{1+\sqrt{7}})$
(vi) $\mathbb{Q}(\sqrt{2+\sqrt{2}})$

3. (a) Prove that if $E \subset F$ and $[F : E] = 2$ then F/E is normal.
(b) Prove that every index 2 subgroup of a group G is normal.

4. Let K be a field with $\mathrm{char}(K) \neq 3$ and such that $f(x) = x^3 - 3x + 1 \in K[x]$ is irreducible. Let $L = K(\alpha)$ where α is a root of $f(x)$. Show that f splits completely over L. [*Hint:* Factor f over $L[x]$ as $(x - \alpha)g(x)$. Now solve for $g(x) = 0$ in L observing that $12 - 3\alpha^2 = (-4 + \alpha + 2\alpha^2)^2$.]

5. Suppose that $\mathrm{char}(K) \neq 2$, and let $K \subset L$ be a field extension of degree 4. Prove that the following two conditions are equivalent:

(i) There exists a (nontrivial) intermediate field $K \subset E \subset L$;

(ii) $L = K(\alpha)$ for some $\alpha \in L$ having minimal polynomial over K of the form:

$$f = x^4 + ax^2 + b \in K[x]\,.$$

6. (a) Suppose that $a, b \in K$ are such that a is a square in $K(\sqrt{b})$. Prove that either a or ab is a square in K.

(b) Let $a, b \in K$ and suppose that b is NOT a square in K; let $L = K(\beta)$ with $\beta^2 = b$. Prove that: If one of $a + \beta$, $a - \beta$ is a square in L, then so is the other, and deduce that $c = a^2 - b$ is a square in K.

(c) Let $a, b \in K$ and set $c = a^2 - b$; suppose that none of b, c, or bc is a square in K. If L is a splitting field of the polynomial:

$$(x^2 - a)^2 - b \in K[x],$$

prove that $[L : K] = 8$. [*Hint: use Part (a) and Part (b) repeatedly.*]

7. In this question we'll find an explicit complex number z such that $\overline{z} \notin \mathbb{Q}(z)$ (by $\overline{z}$ I mean the complex conjugate of z.)

(a) Set $\omega = e^{2\pi i/3}$, so $\omega^3 = 1$, and say $\alpha = 2^{1/3} \in \mathbb{R}$ the real cube root of 2. Set $z = \omega\alpha$. What is $[\mathbb{Q}(z) : \mathbb{Q}]$? Hint: min poly.

(b) What is $[\mathbb{Q}(\omega) : \mathbb{Q}]$?

(c) Let's assume temporarily that $\overline{z} \in \mathbb{Q}(z)$. Show that this implies $\omega \in \mathbb{Q}(z)$. Why does this contradict the tower law? Deduce $\overline{z} \notin \mathbb{Q}(z)$.

(d) Let's write $z = x + iy$. Prove that none of x, i or y are in $\mathbb{Q}(z)$.

8. Suppose that $E \subset F \subset K$ are field extensions with $[F : E]$ and $[K : F]$ both finite. As we stated in class, it is immediate from the definition that: If K/E is normal, then K/F is also normal.

(a) If $E = \mathbb{Q}$, $F = \mathbb{Q}(2^{1/3})$ and $K = \mathbb{Q}(2^{1/3}, \omega)$ with $\omega = e^{2\pi i/3}$, then show that K/E is normal, but F/E is not normal.

(b) If $E = \mathbb{Q}$, $F = \mathbb{Q}(\sqrt{2})$ and $K = \mathbb{Q}(2^{1/4})$, show that K/F and F/E are normal, but K/E is not normal.

(c) Say $H \subseteq K \subseteq G$ are groups. Prove that if H is normal in G then H is normal in K. Give an example of groups with H is normal in G but K not normal in G. Now give an example with H normal in K, K normal in G, but H not normal in G. Now wonder whether this is all a coincidence or not.

9. Say $E \subseteq F$ is an extension of fields with $[F : E]$ finite, and M, N are both subfields of F containing E. Assume that M/E and N/E are both normal.

(i) Prove that $(M \cap N)/E$ is normal.

(ii) Prove that MN (this notation means "the smallest subfield of F containing both M and N") is normal over E as well.

10. Work through the following sketch of a proof of the following basic result that I may not ever discuss in class:

Proposition. If K is a field, and $G \subseteq (K^\times, \times)$ is a finite subgroup, then G is cyclic.

(a) We first do some elementary number theory. If C_n denotes the cyclic group of order n, then let $\phi(n)$ denote the number of elements of C_n that generate C_n. Recall (or prove, if you didn't know it) that the subgroups of C_n are precisely the C_d for $d \mid n$. Deduce that $\sum_{d|n} \phi(d) = n$ (hint: every element of C_n must generate *something*!).

(b) Now some elementary theory of polynomials: prove that if K is a field and $0 \neq p \in K[x]$ is a polynomial of degree $d \geq 0$, then p has at most d roots in K (hint: induct on degree).

(c) Now let G be as in the question. Say the order of G is n. We know that if $g \in G$ then the order of the element divides the order of the group, so the order of g will divide n. For $d \mid n$ let G_d denote the set of elements of G with order precisely d. Prove that if G_d is non-empty then $|G_d| = \phi(d)$ (hint: if $a \in G_d$ then show that $\langle a \rangle$ must be the d roots of $x^d - 1 = 0$).

(d) By summing over d, prove that G_d must be non-empty for all d, and in particular G_n is non-empty. Deduce the result.