1. Let $E = F(\alpha)$ where α is algebraic over F and of odd degree. Show that $E = F(\alpha^2)$.
Solution: Let $f \in F[X]$ be the irreducible polynomial of α. The degree of f is odd. Let $f = X^d + f_{d-1}x^{d-1} + \cdots + f_0, f_i \in F$. Then, $\alpha^d + f_{d-1}\alpha^{d-1} + \cdots + f_0 = 0$. Separating the even and odd powers it is easy to see that there exists $h, g \in F[X]$ with h monic, such that, $\alpha h(\alpha^2) = g(\alpha^2)$. This shows that, $\alpha \in F(\alpha^2)$ and hence $F(\alpha) = F(\alpha^2)$.

2. Let α be a real number such that $\alpha^4 = 5$ and i a square-root of -1.

   (a) Prove that $\mathbb{Q}(i\alpha^2)$ is normal over $\mathbb{Q}$.
   Solution: Since, $(i\alpha^2)^2 = -5$, $\mathbb{Q}(i\alpha^2)$ is an extension of degree at most 2, but since $i\alpha^2 \notin \mathbb{Q}$, it is of degree exactly 2 and all extensions of degree 2 are normal (justify).

   (b) Prove that $\mathbb{Q}(\alpha + i\alpha)$ is normal over $\mathbb{Q}(i\alpha^2)$.
   Solution: Again, since $(\alpha + i\alpha)^2 = 2(i\alpha^2)$, $\mathbb{Q}(\alpha + i\alpha)$ is an extension of degree at most 2 over $\mathbb{Q}(i\alpha^2)$.

   On the other hand $(\alpha+i\alpha)^4 = -20$ and since the polynomial X^4+20 is irreducible (why?) over $\mathbb{Q}$, $[\mathbb{Q}(\alpha + i\alpha) : \mathbb{Q}] \geq 4$ and hence, $[\mathbb{Q}(\alpha + i\alpha) : \mathbb{Q}(i\alpha^2)] \geq 2$ and hence, $[\mathbb{Q}(\alpha + i\alpha) : \mathbb{Q}(i\alpha^2)] = 2$ and the extension is normal.

   (c) Prove that $\mathbb{Q}(\alpha + i\alpha)$ is not normal over $\mathbb{Q}$.
   Solution: Suppose that $\mathbb{Q}(\alpha + i\alpha)$ is a normal extension over $\mathbb{Q}$. Since, $\alpha + i\alpha$ is a root of $X^4 + 20$ this would imply that $X^4 + 20$ must split in $\mathbb{Q}(\alpha + i\alpha)$ and hence, $\alpha - i\alpha \in \mathbb{Q}(\alpha+i\alpha)$. But, this would imply that $\alpha, i\alpha, i$ are all in $\mathbb{Q}(\alpha+i\alpha)$. This means that $\mathbb{Q}(\alpha, i) \subset \mathbb{Q}(\alpha + i\alpha)$. Since $i \notin \mathbb{Q}(\alpha)$, and $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$, this implies that $[\mathbb{Q}(\alpha, i) : \mathbb{Q}] \geq 8$, which is a contradiction since, $[\mathbb{Q}(\alpha + i\alpha) : \mathbb{Q}] = 4$. Hence, Suppose that $\mathbb{Q}(\alpha + i\alpha)$ is not a normal extension over $\mathbb{Q}$.

3. Let f be a polynomial of degree n with coefficients in a field k. Let L be a splitting field of f over k. Prove that $[L : k]$ is a divisor of $n!$.
Solution: We prove this by induction on n. The statement is clearly true when $n = 1$, since in this case $L = k$.

   Now, first assume that f is irreducible over k and let $\alpha_1, \ldots, \alpha_n$ be the roots of f in the algebraic closure of k. Then, $f = (X - \alpha_1)g(X)$, where $g(X) \in k(\alpha_1)(X)$ is of degree $n-1$. Now, $[k(\alpha_1) : k] = n$, and $[k(\alpha_1)(\alpha_2, \ldots, \alpha_n) : k(\alpha_1)] | (n-1)!$ by induction hypothesis. Hence, $[k(\alpha_1, \ldots, \alpha_n) : k] = [k(\alpha_1)(\alpha_2, \ldots, \alpha_n) : k(\alpha_1)][k(\alpha_1) : k] | n!$.

   If f is not irreducible, let $f = gh$ where g is a polynomial of degree $p > 0$, and h a polynomial of degree $n - p$. Let L_g be the splitting field of g over k, and L the splitting field of h over L_g. Then, L is the splitting field of f over k, and $[L : k] = [L : L_g][L_g : k]$. Now, $[L_g : k]!p!$, and $[L : L_g] | (n - p)!$ by induction hypothesis. Hence, $[L : k] = [L : L_g][L_g : k] | (n - p)!p!$ but $(n - p)!p! | n!$.

4. Let k be a field of characteristic $\neq 2, 3$. Prove that the following statements are equivalent:

(a) Any sum of squares in k is itself a square.

(b) Whenever a cubic polynomial f factors completely in k, so does its derivative f'.

Solution: (a) $\Rightarrow$ (b): Let $f(X) = (X-a)(X-b)(X-c)$, with $a, b, c \in k$. Then, $f'(X) = 3X^2 - 2(a+b+c)X + (ab+bc+ca)$. Consider, the discriminant of f' namely,

$$4(a+b+c)^2 - 12(ab+bc+ca) = 2((a-b)^2 + (b-c)^2 + (c-a)^2).$$

The righthand side is a sum of square and hence itself a square say d^2. Then, $f'(X) = 3(X - \frac{2(a+b+c)+d}{6})(X - \frac{2(a+b+c)-d}{6})$.

(b) $\Rightarrow$ (a): Let $\alpha, \beta \in k$. Consider the cubic polynomial, $f(X) = (X-\alpha)(X-\beta)(X+\alpha)$. Since, the discriminant of f' has to be a square we have that, $2((\alpha-\beta)^2 + (\beta+\alpha)^2 + (2\alpha)^2) = 4(3\alpha^2 + \beta^2)$ is a square. Hence, $3\alpha^2 + \beta^2$ is square for all $\alpha, \beta \in k$.

Now, let $x, y \in$. Then, $x^2 + y^2 = 3(x^2/3) + y^2$. We claim that, $x^2/3$ is a square. This is true because, $x^2/3 = 3(x/3)^2 + 0^2$ which is a square as proved earlier. Thus, $x^2 + y^2 = 3(x^2/3) + y^2$ is a square too. The rest follows by induction on the number of terms in the sum of squares.

5. Suppose $K \subset L \subset M$ be fields and L is generated over K by some of the roots of a polynomial f with coefficients in K. Prove that M is a splitting field of f over K if and only if M is a splitting field of f over L.
Solution: Very easy.

6. Let k be any finite field and n a positive integer. Prove that there exists an irreducible polynomial over k of degree n.
Solution: Let $k = F_q$. Then, there is an algebraic extension F_{q^n} of degree n. The number of intermediate subfields is finite. Apply the primitive element theorem to deduce that, $F_{q^n} = F_q[\theta]$. Then, θ has an irreducible polynomial of degree n.

7. Prove that in a finite field any element can be written as a sum of at most two squares.
Solution: Consider the finite field F_q of characteristic $\neq 2$. Let F_q^2 be the set of squares. Now, for every non-zero $x \in F_q$, $x^2 = (-x)^2$ and $x^2 = y^2 \Rightarrow x = \pm y$.

   Thus, $|F_q^2| = (q-1)/2 + 1 = (q+1)/2$.

   Let $x \in F_q$ and consider the set of elements, $S_x = \{x - a^2 | a \in F_q\}$. Then, $|S_x| = |F_q^2| = (q+1)/2$.

   Since, F_q has only q elements, $S_x \cap F_q^2$ must intersect.

   What about characteristic 2 ?

8. Complete the course evaluation form available online at:
www.coursesurvey.gatech.edu (between 6AM and midnight everyday till Dec 6).