Math 123 Problem Set 3 Solutions.

§2, #1a. We know $[\mathbb{Q}(\beta):\mathbb{Q}] = 2$, and since $\mathbb{Q}(\beta) \subset \mathbb{R}$, $1 < [\mathbb{Q}(\alpha,\beta):\mathbb{Q}(\beta)] \leq 2$, hence $[\mathbb{Q}(\alpha,\beta):\mathbb{Q}] = 2 \cdot 2 = 4$. We also know that the 4 embeddings of $\mathbb{Q}(\alpha,\beta)$ into $\mathbb{C}$ must go through all possible combinations of $\alpha \mapsto \pm\alpha, \beta \mapsto \pm\beta$, and thus all of them take $\alpha+\beta$ to different elements of $\mathbb{C}$, and hence by one of our lemmas in the proof of P.E.T., $\alpha+\beta$ is a primitive element.
b. $[\mathbb{Q}(\alpha,\beta):\mathbb{Q}] \leq 2 \cdot 3 = 6$. However, we know $\gamma = 2^{\frac{1}{6}} = \frac{\beta}{\alpha} \in \mathbb{Q}(\alpha,\beta)$, and that the irreducible polynomial of γ over $\mathbb{Q}$ is $X^6 - 2$. (It is irreducible by Eisenstein on 2.) Hence γ is a primitive element.
c. We check that both polynomials are irreducible by reducing mod 2 and finding no roots. Hence $[\mathbb{Q}(\alpha,\beta):\mathbb{Q}] = 6$ by a problem from PS2, since 2 and 3 are relatively prime, and $\{1,\alpha,\beta,\alpha\beta,\alpha^2,\alpha^2\beta\}$ form a basis for $\mathbb{Q}(\alpha,\beta)$ over $\mathbb{Q}$. We check that 1, $\alpha\beta, (\alpha\beta)^2 = \alpha^2 + \alpha^2\beta$, and $(\alpha\beta)^3 = (\alpha-1)(\beta+1)(\beta) = (\alpha-1)(2\beta+1)$ are linearly independent over $\mathbb{Q}$, and so $[\mathbb{Q}(\alpha\beta):\mathbb{Q}] > 3$. Since the degree must divide 6, it must be equal to 6, and hence we have a primitive element.
d. We again note that neither of the polynomials are reducible over $\mathbb{Q}$, since they have no roots (rational root theorem and checking the finitely many allowable values), and hence $[\mathbb{Q}(\alpha,\beta):\mathbb{Q}] = 6$. The same reasoning as in part c works here: we have a basis, and we can check that 1, $\alpha\beta, (\alpha\beta)^2$, and $(\alpha\beta)^3$ are linearly independent over $\mathbb{Q}$, and so $\alpha\beta$ is a primitive element.

Note: Obviously, there are many different primitive elements for each of these fields. For parts a and b, however, I cannot think of easier ways of proving that a particular element is primitive. For parts c and d, there might be slicker ways of finding a primitive element; I chose $\alpha\beta$ for the ease of taking its powers.

#2. Let $p(X)$ be the irreducible polynomial of β over F, and let γ be a root of p in A not equal to β; define a map on $F(\beta)$ into A which is the identity on F and sends β to γ. This clearly works.

#3a. Let $p(X)$ be the irreducible polynomial of α over F, and let $\alpha_1, \ldots, \alpha_d$ be the roots of $p(X)$ in A. Given any i, we have a map ϕ_i from $F(\alpha)$ to A taking α to α_i. We also know that given any of those embeddings ϕ_i, there are exactly $m = [E : F(\alpha)]$ embeddings, $\psi_{i,1}, \ldots, \psi_{i,m}$ of E into A which restrict to ϕ_i on $F(\alpha)$; these give all embeddings of E over F (called σ_i in the problem). Hence the trace of α is just

$$\sum_{i=1}^{d}\sum_{j=1}^{m}\psi_{i,j}\alpha = \sum_{i=1}^{d} m\cdot\phi_i\alpha = m\sum_{i=1}^{n}\phi_i\alpha.$$

However, $\sum_i \phi_i\alpha$ is just the sum of the roots of $p(X)$, and as such is (up to a sign) the coefficient of the X^{d-1} term in $p(X)$, which is in F. Hence $\mathrm{Tr}_F^E(\alpha)\in F$. For the norm, we argue similarly:

$$\prod_{i=1}^{d}\prod_{j=1}^{m}\psi_{i,j}\alpha = \prod_{i=1}^{d}(\phi_i\alpha)^m = \left(\prod_{i=1}^{d}\phi_i\alpha\right)^m.$$

We know $\prod_i \phi_i\alpha$ is the product of the roots of $p(X)$, which is (up to a sign) the constant term of $p(X)$, which is in F. Hence $N_F^E(\alpha)\in F$.
b. This is trivial; plug $\alpha+\beta$ (resp. $\alpha\cdot\beta$) into the formula(s) and watch everything work out.

Note: Many people tried variants on the technique of applying σ_i to the norm and the trace. This fails, because we do not know that the norm and the trace are actually in the field E; all we know is that the σ_i take elements of E into A.

#4. Just follow the proof from #3; note that here, the d we used above is just n, and m from above is 1.

§3, #1a. We check that if α is a root, then given $a\in\mathbb{Z}_p$, $f(\alpha+a) = (\alpha+a)^p-\alpha-a-c = \alpha^p+a^p-\alpha-a-c = f(\alpha)+a^p-a = 0$. (Since the field is of characteristic p, raising to the pth power preserves addition, and also $a^p-a=0$.) Hence if there is one root α in F, $\alpha+a$ give all p roots. If f is reducible, then it can be factored into $f(X)=g(X)\cdot h(X)$, where the degree of g is less than p. We know that over a splitting field of f, $g(X)$ must split into linear factors $\prod_{i=1}^{d}(X-\alpha_i)$, where the α_i are roots of f. In fact, if we choose a specific root of f and call it α, we know that each α_i is α plus some $a_i\in\mathbb{Z}_p$. Hence the coefficient of the X^{d-1} term in $g(X)$ must be $-\sum_{i=1}^{d}(\alpha+a_i) = -d\alpha+a$, for some $a\in\mathbb{Z}_p\subset F$. But the coefficient is in F, and $a\in F$, hence $-d\alpha\in F$. Since $d<p$, d is invertible in F, and hence $\alpha\in F$, and F contains all roots of $f(X)$, q.e.d.
b. We know if F has any root a, then $a+(-a)=0$ is also a root; but $f(0)=-c\neq 0$.

c. The splitting field of $f(X)$ certainly must contain $F(\alpha)$, but since all roots of $f(X)$ are contained in $F(\alpha)$ (by part a), $F(\alpha)$ is the splitting field.
d,e. $F(\alpha)$ is a splitting field, so it is normal; hence all $[F(\alpha) : F] = p$ embeddings of $F(\alpha)$ into A are actually automorphisms, and so the group of automorphisms of $F(\alpha)$ over F is of size p. All such groups are isomorphic to $\mathbb{Z}_p$.

#2. The roots of the polynomial are $\alpha\cdot\zeta^i$ for $0 \leq i < n$, and hence all of them are in the field $F(\alpha,\zeta)$. However, the splitting field contains α and $\alpha\cdot\zeta$, and hence contains their quotient ζ, hence $F(\alpha,\zeta)$ is exactly the splitting field.

#3a. Let ζ be a primitive pth root of unity and α a root of the polynomial. Then the roots of the polynomial are $\alpha\cdot\zeta^i$. If we can factor $t^p - a = g(t)\cdot h(t)$, with degree of g equal to d, then the constant term of $g(t)$ will be (up to sign) a product of d of the roots, and will look something like $\alpha^d\zeta^j$ for some $j \in Z$. Since $d < p$, we can write $j \equiv d\cdot k \bmod p$ for some $k \in \mathbb{Z}$, and hence the constant term will be $(\alpha\zeta^k)^d$. We note that this must be in F. However, we also note that $(\alpha\zeta^k)^p = a \in F$. We see that the set S of integers c such that $(\alpha\zeta^k)^c \in F$ is an ideal in $\mathbb{Z}$, and that $d, p \in S$, and since p prime and $0 < d < p$, $1 \in S$, and $\alpha\zeta^k \in F$. But then we have a pth root of a in F, a contradiction.
b. This will be combined with the proof of #4.

#4. We prove that if $t^m - a$ is irreducible for odd $m > 1$, and a is not a pth power in F, then $t^{pm} - a$ is irreducible; this will prove both 3b and 4 by induction (the base case of m prime is done in 3a). Look at a root of $t^m - a$, α. We know that $[F(\alpha) : F] = m$. Assume that there is a $\beta \in F(\alpha)$ such that $\beta^p = \alpha$. We know that the norm (taken from $F(\alpha)$ to F) of α is therefore the pth power of the norm of β. But the norm of α is just $(-1)^m(-a)$, by §2, #4, which is a since m is odd, and the norm of β is some element of F; this says that a is a pth power in F, a contradiction. Hence α is not a pth power in $F(\alpha)$, and hence the polynomial $X^p - \alpha \in F(\alpha)[X]$ is irreducible by 3a. Adjoin a root of that polynomial, β. We get that $[F(\alpha,\beta) : F(\alpha)] = p$, and hence $[F(\alpha,\beta) : F] = p\cdot m$. But since $\beta^p = \alpha$, $\alpha \in F(\beta)$, and hence $F(\alpha,\beta) = F(\beta)$; therefore the degree of β over F is pm. But we know that $\beta^{pm} = \alpha^m = a$, so β satisfies the polynomial $t^{pm} - a$ in $F[t]$, and hence that polynomial must be the irreducible polynomial of β over F. In particular, it is irreducible.