1. (**25 points**)

(a) $9x^{100} + 25x^4 - 15$ is irreducible over $\mathbf{Q}$ by the Eisenstein Criterion with $p = 5$ as 5 divides $15, 25$, 5 does not divide 9, and 5^2 does not divide 15. (**9**).

(b) We can apply the mod 2 test to $11x^4 - 21x + 27$ as it reduces to $f(x) = x^4 + x^2 + 1 \in \mathbf{Z}_2[x]$ of the same degree (**4**). $f(0) = 1 = f(1)$ means $f(x)$ has no linear factors (**4**). If $f(x)$ is reducible it is a product of irreducible quadratic factors, hence $f(x) = (x^2 + x + 1)(x^2 + x + 1) = x^4 + x^2 + 1$, contradiction. Thus $f(x)$ is irreducible over $\mathbf{Z}_2$ (**4**) and $11x^4 - 21x + 27$ is irreducible over $\mathbf{Q}$ (**4**).

2. (**25 points**)

(a) Suppose $a|b$. Then $ac = b$ for some $c \in R$ (**4**). Since b is irreducible either a or c is a unit. Since a is irreducible, a is not a unit (**4**). Therefore c is a unit (**4**). Therefore a and b are associates.

(b) By assumption $ab = cd$. Suppose that a is prime. Then $a|cd$ (**4**). Thus $a|c$, in which case a and c are associates (**3**) or $a|d$, in which case a and d are associates (**3**), by part (a). Since a and c, and a and d, are not associates, $a \not| c$ and $a \not| d$. Therefore a is not prime (**3**).

3. (**25 points**)

(a) Suppose $r = r'r''$, where $r', r'' \in R$. By assumption $N(r) = p$ is a prime integer. Since $N(0) = 0$ and $N(u) = 1$ for all $u \in R^\times$, r is not zero and not a unit (**2**). Now $N(r')N(r'') = N(r'r'') = N(r) = p$ (**3**) implies $N(r') = 1$, in which case r' is a unit, or $N(r'') = 1$, in which case r'' is a unit. Therefore r is irreducible. (**3**)

(b) $r = m + n\sqrt{5}$ for some $m, n \in \mathbf{Z}$. Now $p = N(r) = |m^2 - 5n^2| = |(m + \sqrt{5})(m - \sqrt{5})|$ so $p = (m+\sqrt{5})(m-\sqrt{5})$ or $p = (m+\sqrt{5})(-m+\sqrt{5})$ (**4**). Since $p = N(m+n\sqrt{5}) = N(m-n\sqrt{5}) = N(-m+n\sqrt{5})$ it follows that p is the product of two irreducibles in either case by part (a). Thus p is reducible. (**4**) Prime implies irreducible in domains; thus p is not prime in $\mathbf{Z}[\sqrt{5}]$ (**4**).

(c) $11 = 16 - 5 = N(4 + \sqrt{5})$, or $11 = |9 - 20| = N(3 + 2\sqrt{5})|$, for example (**5**).

4. (**25 points**) Let n_p denote the number of Sylow p-subgroups of G.

(a) Since $|G| = 825 = 3{\cdot}5^2{\cdot}11$ there are Sylow p-subgroups for $p = 3, 5, 11$ by Sylow's First Theorem. By Sylow's Third Theorem it follows n_{11} divides $3{\cdot}5^2$ (**3**) and $n_{11} \equiv 1 \pmod{11}$ (**2**). Thus $n_{11} \in \{1, 3, 5, 15, 25, 75\}$. As these integers are congruent to $1, 3, 5, 4, 3, 9$ mod 11 respectively, $n_{11} = 1$. (**3**) Let K be the Sylow 11-subgroup of G. Then $K \trianglelefteq G$ (**2**) by the corollary to Sylow's Third Theorem.

By Sylow's first Theorem (or Cauchy's Theorem) there exists $H \leq G$ of order 5 (**3**). $K \trianglelefteq G$ implies $KH \leq G$. Since $|H \cap K|$ divides $|H|$ and $|K|$ by Lagrange's Theorem, that is 5 and 11, necessarily $|H \cap K| = 1$ (**2**). Therefore $|HK| = |H||K|/|H \cap K| = 5{\cdot}11/1 = 55$ (**2**).

(b) Now let H be a Sylow 3-subgroup of G. Then $|H| = 3$. By the argument for part (b) $HK \subseteq G$ and has order $3{\cdot}11 = 33$ (**4**). Since $3, 11$ are primes and $11 \not\equiv 1 \pmod 3$, HK is cyclic, and hence has an element of order 33 (**4**).

5. (**25 points**) $E = \mathbf{Q}(3^{1/4}, 19^{1/7})$.

(a) $3^{1/4}, 19^{1/7}$ are roots of $x^4 - 3, x^7 - 19 \in \mathbf{Q}[x]$ respectively (**2**). These monic polynomials are irreducible by the Eisenstein Criterion with $p = 3, 19$ respectively (**2**). Therefore $x^4 - 3$ is the minimal polynomial of $3^{1/4}$ over $\mathbf{Q}$, so $[\mathbf{Q}(3^{1/4}) : \mathbf{Q}] = 4$ and likewise $[\mathbf{Q}(19^{1/7}) : \mathbf{Q}] = 7$ (**2**). Thus $4, 7$ divide $[E : \mathbf{Q}]$ so 28 divides $[E : \mathbf{Q}]$ (**2**). Since$[E : \mathbf{Q}] \leq 28$, $[E : \mathbf{Q}] = 28$ (**2**).

(b) $f(x) = x^5 + 27x^2 - 21 \in \mathbf{Q}[x]$ is irreducible by the Eisenstein Criterion with $p = 3$ (**4**). Suppose $a \in E$ is a root of $f(x)$. Then $f(x)$ is the minimal polynomial of a over $\mathbf{Q}$ and thus $[\mathbf{Q}(a) : \mathbf{Q}] = 5$. But then 5 divides 28, a contradiction. Thus $f(x)$ has no root in E. (**4**).

(c) $3^{1/8}$ is a root of $x^8 - 3 \in \mathbf{Q}[x]$ which is irreducible by the Eisenstein Criterion with $p = 3$ (**3**). We follow then argument of part (b). If $3^{1/8} \in E$ then $[\mathbf{Q}(3^{1/8}) : \mathbf{Q}] = 8$ divides 28, a contradiction. Thus $3^{1/8} \notin E$. (**4**)

6. (**25 points**)

(a) $x^4 - 19 = (x^2 - 19^{1/2})(x^2 + 19^{1/2}) = (x - 19^{1/4})(x + 19^{1/4})(x - \imath 19^{1/4})(x + \imath 19^{1/4})$ (**3**), hence $E = \mathbf{Q}(19^{1/4}, \imath)$ (**3**). Now $[\mathbf{Q}(19^{1/4}) : \mathbf{Q}] = 4$ since $19^{1/4}$ has minimal polynomial $x^4 - 19$ over $\mathbf{Q}$ as $19^{1/4}$ is a root of it, it is monic, and it is irreducible by the Eisenstein Criterion with $p = 19$ (**2**). Also $[E : \mathbf{Q}(19^{1/4})] = [\mathbf{Q}(19^{1/4})(\imath) : \mathbf{Q}(19^{1/4})] \leq 2$ since $\imath^2 + 1 = 0$. Since $\mathbf{Q}(19^{1/4}) \subseteq \mathbf{R}$ and $\imath \notin \mathbf{R}$, $[E : \mathbf{Q}(19^{1/4})] = 2$. (**2**). Thus $[E : \mathbf{Q}] = [E : \mathbf{Q}(19^{1/4})][\mathbf{Q}(19^{1/4}) : \mathbf{Q}] = 2{\cdot}4 = 8$ (**2**).

(b) Since $\{1, 19^{1/4}, 19^{2/4}, 19^{3/4}\}$ is a basis of $\mathbf{Q}(19^{1/4})$ over $\mathbf{Q}$ and $\{1, \imath\}$ is a basis of $E = \mathbf{Q}(19^{1/4})(\imath)$ over $\mathbf{Q}(19^{1/4})$, the set of products $\{1, 19^{1/4}, 19^{2/4}, 19^{3/4}, 1\imath, 19^{1/4}\imath, 19^{2/4}\imath, 19^{3/4}\imath\}$ is a basis for E over $\mathbf{Q}$ (**6**).

(c) σ and τ generators (**2**); relations $\sigma^4 = \tau^2 = e$ (**2**) and $(\tau\sigma)^2 = e$ (**3**). The last relation could have been expressed as $\tau\sigma\tau = \sigma^3$ or $(\sigma\tau)^2 = e$.

7. (**25 points**) $E = \mathbf{Q}(\sqrt{3}, \imath\sqrt{7}) = \mathbf{Q}(\sqrt{3})(\imath\sqrt{7})$ and $\alpha = 2\sqrt{3} - \imath\sqrt{7}$. If $[F(a) : F] = n$ and $f(x) \in F[x]$ is monic of degree n and $f(a) = 0$ then $\min(a, F) = f(x)$.

(a) Since $x^2 + 7$ is irreducible over $\mathbf{Q}(\sqrt{3})$ and has root $\imath\sqrt{7}$, $[\mathbf{Q}(\sqrt{3})(\imath\sqrt{7}) : \mathbf{Q}(\sqrt{3})] = 2$ (**3**). $x^2 - 3$ has root $\sqrt{3}$ and is irreducible over $\mathbf{Q}$ by the Eisenstein Criterion with $p = 3$. Therefore $[\mathbf{Q}(\sqrt{3}) : \mathbf{Q}] = 2$ (**2**) which means $[E : \mathbf{Q}] = [\mathbf{Q}(\sqrt{3})(\imath\sqrt{7}) : \mathbf{Q}(\sqrt{3})][\mathbf{Q}(\sqrt{3}) : \mathbf{Q}] = 2{\cdot}2 = 4$ (**3**).

(b) $\sqrt{3}, \imath\sqrt{7} \in \mathbf{Q}(\sqrt{3}, \imath\sqrt{7})$. Thus $2\sqrt{3} - \imath\sqrt{7} \in \mathbf{Q}(\sqrt{3}, \imath\sqrt{7})$ so $\mathbf{Q}(2\sqrt{3} - \imath\sqrt{7}) \subseteq \mathbf{Q}(\sqrt{3}, \imath\sqrt{7})$. To show equality we need only show the reverse inclusion which will follow from $\sqrt{3}, \imath\sqrt{7} \in \mathbf{Q}(2\sqrt{3} - \imath\sqrt{7})$. $(2\sqrt{3} - \imath\sqrt{7})\overline{(2\sqrt{3} - \imath\sqrt{7})} = (2\sqrt{3} - \imath\sqrt{7})(2\sqrt{3} + \imath\sqrt{7}) = 4{\cdot}3 + 7 = 19$ shows that $\alpha^{-1} = (1/19)(2\sqrt{3} + \imath\sqrt{7})$. Thus $\sqrt{3} = (1/4)(\alpha + 19\alpha^{-1}), \imath\sqrt{7} = (1/2)(-\alpha + 19\alpha^{-1}) \in \mathbf{Q}(2\sqrt{3} - \imath\sqrt{7})$. (**6**)

$(\alpha - 2\sqrt{3})^2 = (\imath\sqrt{7})^2$ so $\alpha^2 - 4\sqrt{3}\alpha + 12 = -7$, $\alpha^2 - 4\sqrt{3}\alpha + 19 = 0$ (**3**). $(\alpha^2 + 19)^2 = (4\sqrt{3}\alpha)^2$, $\alpha^4 + 38\alpha^2 + 361 = 48\alpha^2$, and $\alpha^4 - 10\alpha^2 + 361 = 0$ (**4**). $\min(\alpha, \mathbf{Q}) = x^4 - 10x^2 + 361$ (**2**).

(c) From the calculations above $\min(\alpha, \mathbf{Q}(\sqrt{3})) = x^2 - 4\sqrt{3}x + 9$ (**2**).

8. (**25 points**)

(a) By the commentary $\mathrm{Gal}(E/F) \simeq H \leq \mathrm{Sym}(S) \simeq S_3$; therefore $|\mathrm{Gal}(E/F)|$ divides 6. Since $3 < [E : F] = |\mathrm{Gal}(E/F)|$ necessarily $|H| = |\mathrm{Gal}(E/F)| = 6 = |\mathrm{Sym}(S)|$. Therefore $H = \mathrm{Sym}(S)$ and $\mathrm{Gal}(E/F) \simeq S_3$. (**8**)

(b) $d = [K : F]$, $6 = [E : K][K : F]$ and thus $|\mathrm{Gal}(E/K)| = [E : K] = 6/d$. $d = 1$; $\boxed{1}$ (**2**). $d = 2$; $\boxed{1}$ (**3**). $d = 3$; $\boxed{3}$ (**5**). $d = 6$; $\boxed{1}$ (**2**).

(c) Let $a \in L\backslash F$. Then $2 \leq [F(a) : F] \leq [L : F] = 2$ implies $[F(a) : F] = [L : F] = 2$ and thus $F(a) = L$. Let $p(x) \in F[x]$ be the minimal polynomial of a over F. Then $\mathrm{Deg}\, p(x) = 2$. Since $p(a) = 0$, $p(x) = (x - a)q(x)$ for some $q(x) \in L[x]$. Thus $q(x)$ is monic and $\mathrm{Deg}\, q(x) = 1$ which means $q(x) = x - b$ for some $b \in L$. Thus $p(x) = (x - a)(x - b)$ and $L = F(a)$ is a splitting field of $p(x)$ over F. (**5**)