Homework 6 Key

15.6.1) Let F be a field of characteristic 0. Let $f \in F[x]$ and let g be an irreducible polynomial that divides f and f'. Since g divides f, write $f = gh$ for some $h \in F[x]$. Applying the product rule,

$$f' = gh' + g'h.$$

Since g divides gh' and g divides f', it must be the case that g divides $g'h$. Since $F[x]$ is a UFD, either g divides g' or g divides h. The former is impossible since F has characteristic 0, so $h = gp$ for some $p \in F[x]$. Thus $f = g^2p$, so g^2 divides f.

15.6.2) (a) Let $a \in F$ with $F(\sqrt{a})$ a quadratic extension. Then $\{1, \sqrt{a}\}$ is a basis, so for each $z \in F(\sqrt{a}), z = x + y\sqrt{a}$. then $z^2 = (x^2 + y^2 a) + 2xy\sqrt{a}$. In order to have $z^2 \in F$ we must have $2xy\sqrt{a} = 0$, so $x = 0$ or $y = 0$. Then the square elements are those of the form x^2 or $y^2 a$ for $x, y \in F$.

(b) Since $\mathbb{Q}$ has characteristic 0, an extension K is quadratic iff $K = \mathbb{Q}(\sqrt{a})$ for some $a = \frac{p}{q} \in \mathbb{Q}$ with $\sqrt{a} \notin \mathbb{Q}$. Notice that $\sqrt{\frac{p}{q}} = \frac{\sqrt{pq}}{q}$, so $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{pq})$, and from this we conclude that the only quadratic extensions of $\mathbb{Q}$ are those of the form $\mathbb{Q}(\sqrt{d})$ for $d \in \mathbb{Z}$, d not a square.

15.6.3) Let α be a primitive nth root of unity that is in a quadratic extension $\mathbb{Q}(\sqrt{d})$. Then the minimal polynomial of has degree at most 2 over $\mathbb{Q}$. The nth cyclotomic polynomial is irreducible, so $\varphi(n) \leq 2$, where φ is Euler's phi function. Then $n \in \{1, 2, 3, 4, 6\}$.

Every quadratic number field contains a root of unity for $n = 1, 2$ since they all contain 1 and -1.

We also see that $\mathbb{Q}(\sqrt{-1})$ contains i, which is a 4th root of unity.

We see that $\mathbb{Q}(\sqrt{-3})$ contains $\frac{-1+i\sqrt{3}}{2}$ $\frac{1+i\sqrt{3}}{2}$, primitive 3rd and 6th roots of unity respectively. Thus $n = 1, 2, 3, 4, 6$ all work, and these are all such n.

15.7.1) $\mathbb{F}_4^+$ is a group with 4 elements, and there are exactly two such groups. $\mathbb{F}_4^+$ is not cyclic since $\alpha + \alpha = 0$ for each $\alpha \in \mathbb{F}_4^+$, so it must be the case that $\mathbb{F}_4^+$ is isomorphic to the Klein four-group.

15.7.7) Let K be a finite field with q elements, so K is isomorphic to $\mathbb{F}_q$. Then every nonzero element of K is a root of the polynomial $x^{q-1} - 1$, so

$$x^{q-1} - 1 = \prod_{\alpha \in K^\times} (x - \alpha).$$

Comparing coefficients, we see that $-1 = (-1)^{q-1} \prod_{\alpha \in K^\times} \alpha$. When q is odd, $(-1)^{q-1} = 1$, and when q is even, K has characteristic 2, so $(-1)^{q-1} = -1 = 1$, and we are done.

15.7.8) Let $K = \mathbb{F}_2(\alpha)$ and $L = \mathbb{F}_2(\beta)$. We define a homomorphism $\varphi : K \to L$ by $\alpha \mapsto \beta + 1$, is a homomorphism since

$$\varphi(\alpha^3 + \alpha + 1) = (\beta + 1)^3 + (\beta + 1) + 1 = \beta^3 + \beta^2 + 1 = 0.$$

This map is an isomorphism because it is invertible. Any isomorphism must map α to a root of g, and there are three distinct roots of g, so there are three possible isomorphisms.

15.7.9) Let $F = \mathbb{F}_p$.

(a) Notice that F has order p, so there are p^2 total monic polynomials of degree 2 in $\mathbb{F}[x]$. Such a polynomial is reducible if and only if it is a product of 2 linear factors. There are p was to choose the same linear factor twice and $\binom{p}{2}$ ways to choose two different linear factors, so $p + \binom{p}{2}$ such polynomials. Thus there are $p^2 - p - \binom{p}{2} = \binom{p}{2}$ monic irreducible polynomials of degree 2.

(b) By 15.6.2, K is a field and the residue of x, call it α is a root of f in K. α must have degree 2 over F, so K is a quadratic extension, so $[K : F] = 2$, so $|K| = p^2$. Then K has basis $\{1, \alpha\}$, meaning the elements of K are of the form $a + b\alpha$ with $a, b \in F$. The degree of an element over F must divide $[K : F] = 2$, and if $b \neq 0$, the element is not in F, so such an element must have degree 2. Thus such an element is a root of an irreducible quadratic polynomial in $\mathbb{F}[x]$.

(c) From (b), every element in $K \setminus F$ is the root of an irreducible polynomial of degree 2 in $F[x]$. There are $p^2 - p$ elements in $K \setminus F$, and $\frac{p^2-p}{2}$ monic irreducible polynomials of degree in $F[x]$, each of which accounts for two of these $p^2 - p$ elements, so every monic irreducible polynomial of degree 2 has a root in K, and thus every irreudicble polynomial of degree 2 does as well.

(d) Let g be another irreducible polynomial of degree 2 in $F[x]$, and let $L = F[x]/(g)$. By part (c), f has a root β in $L \setminus F$. Then α and β have the same irreducible polynomial over F, so the field extensions $F(\alpha)$ and $F(\beta)$ are isomorphic. Since $F(\alpha) \cong K$ and $F[\beta] \cong L$, we get that $K \cong L$.

15.M.4) (a) Let p be an odd prime. Then $\mathbb{F}_p^\times$ is a cyclic group with size $p-1$ with generator α, so the elements of α are precisely the elements α^n for $0 \leq \alpha \leq p-1$. Then the square elements are precisely the elements of the form α^{2m} for $0 \leq m < \frac{p-1}{2}$, because for elements of the form α^{2m+1}, if there were a β with $\beta^2 = \alpha$, then $\beta = \alpha^k$ for some k, so $2k = 2m+1$, a contradiction. Thus $\frac{p-1}{2}$ elements of $\mathbb{F}_p^\times$ are squares, which is exactly have of the elements.

Now assume that a, b are non-square elements. Then they are of the form α^n and α^m respectively, for m, n odd. The product is then $ab = \alpha^{m+n}$, and $m+n$ is even, so ab is square.

(b) The proof of part (a) holds verbatim if p is replaced by a power of p.

(c) Let $q = 2^n$ for $n \geq 1$. Then $\mathbb{F}_q^\times$ is a cyclic group of order $p-1$ with generator α. Any element of the form α^{2m} is clearly a square. For any element of the form α^{2m+1}, notice that $(\alpha^{\frac{2m+q}{2}})^2 = \alpha^{2m+1+q-1} = \alpha^{2m+1}$, so these elemlents are squares as well. Finally, $0^2 = 0$, so 0 is a square.

(d) The irreducible polynomial for $\gamma = \sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$ is

$$p(x) = x^4 - 10x^2 + 1.$$

We show that this is reducible in $\mathbb{F}_p$ for each prime p. If 2 is a square, then there is an element α with $\alpha^2 = 2$, so

$$x^4 - 10x^2 + 1 = (x^2 - 1 - 2\alpha x)(x^2 - 1 + 2\alpha x).$$

If 3 is a square, then there is an element β with $\beta^2 = 3$, and then

$$x^4 - 10x^2 + 1 = (x^2 + 1 - 2\beta x)(x^2 + 1 + 2\beta x).$$

Finally, if 3 and 2 are not squares, then by part (a), their product 6 must be a square, so there is some δ with $\delta^2 = 6$, and then

$$x^4 - 10x^2 + 1 = (x^2 - 5 - 2\delta)(x^2 - 5 + 2\delta).$$

In each case, p is reducible.