Mathematics W4043 Algebraic Number Theory
Assignment # 1

Benjamin Church

October 17, 2017

1. (a) By Euler's Criterion: $\left(\frac{7}{13}\right) \equiv 7^{\frac{13-1}{2}} \bmod 13$ but $7^{\frac{13-1}{2}} = 7^6 = 49^3 \equiv (-3)^3 \bmod 13$ and $(-3)^3 = -27 \equiv -1 \bmod 13$ so $\left(\frac{7}{13}\right) = -1$

   (b) By Euler's Criterion: $\left(\frac{13}{7}\right) \equiv 13^{\frac{7-1}{2}} \bmod 7$ but $13^{\frac{7-1}{2}} = 13^3 \equiv -1 \bmod 7$ so $\left(\frac{13}{7}\right) = -1$.

   Thus, $\left(\frac{7}{13}\right)\left(\frac{13}{7}\right) = 1 = (-1)^{\frac{13-1}{2}\frac{7-1}{2}}$ since $6 \cdot 3$ is even.

   (c) By Euler's Criterion: $\left(\frac{23}{19}\right) \equiv 23^{\frac{19-1}{2}} \bmod 19$ but $23^{\frac{19-1}{2}} = 23^9 \equiv 4^9 \bmod 19$ and $4^9 = 64^3 \equiv 7^3 \bmod 19$ and $7^3 = 49 \cdot 7 \equiv 11 \cdot 7 \bmod 19$ and $11 \cdot 7 = 77 \equiv 1 \bmod 19$ so $\left(\frac{23}{19}\right) = 1$.

   (d) By Euler's Criterion: $\left(\frac{19}{23}\right) \equiv 19^{\frac{23-1}{2}} \bmod 23$ but $19^{\frac{23-1}{2}} = 19^{1}1 \equiv 19 \cdot 16^5 \bmod 23$ and $19 \cdot 16^5 = 19 \cdot 16 \cdot 16^4 \equiv 19 \cdot 16 \cdot 3^2 \bmod 23$ and $19 \cdot 16 \cdot 9 = 2736 \equiv -1 \bmod 23$. Therefore, $\left(\frac{23}{19}\right) = -1$.

   Thus, $\left(\frac{23}{19}\right)\left(\frac{19}{23}\right) = -1 = (-1)^{\frac{23-1}{2}\frac{19-1}{2}}$ since $11 \cdot 9$ is odd.

2. (a) For $g \in \mathbb{F}_{17}^{\times}$, $\text{ord}(g) \mid 17 - 1 = 16$ so $\text{ord}(g) = 2^k$ for some $k \in \{0, 1, 2, 3, 4\}$. If g is not a primitive root i.e. $\text{ord}(g) \neq 2^4$ then $\text{ord}(g) = 2^k$ for $k \leq 3$ so $g^{\frac{17-1}{2}} = g^{\text{ord}(g) 2^{3-k}} = (g^{\text{ord}(g)})^{2^{3-k}} = 1$. Therefore, by Euler's Criterion, if $\left(\frac{g}{17}\right) = -1$ then g is a primitive root.

   Now guess $g = 3$. $\left(\frac{3}{17}\right)\left(\frac{17}{3}\right) = (-1)^{\frac{17-1}{2}\frac{3-1}{2}} = (-1)^8 = 1$ but $\left(\frac{17}{3}\right) = \left(\frac{2}{3}\right) = -1$ so $\left(\frac{3}{17}\right) = -1$ so 3 is a primitive root of $\mathbb{F}_{17}^{\times}$.

   (b) For $g \in \mathbb{F}_{23}^{\times}$, $\text{ord}(g) \mid 23 - 1 = 22$ so $\text{ord}(g) \in \{1, 2, 11, 22\}$. The only element of order 1 is 1 and by uniqueness of subgroups of cyclic groups, $\langle -1 \rangle$ is the unique subgroup of order 2 and therefore, the only element of order 2 is -1. Any other non-primitive root must have order 11. Thus, if $g \in \mathbb{F}_{23}^{\times} \setminus \{1, -1\}$ is not a primitive root then $g^{11} = 1$ but $11 = \frac{23-1}{2}$ so by Euler's Criterion $\left(\frac{g}{23}\right) = 1$. Thus, if $\left(\frac{g}{13}\right) = -1$ and $g \neq \pm 1$ then g is a primitive root of $\mathbb{F}_{23}^{\times}$.

   Guess $g = 3$. $\left(\frac{3}{23}\right)\left(\frac{23}{3}\right) = (-1)^{\frac{23-1}{2}\frac{3-1}{2}} = (-1)^{11} = -1$ but $\left(\frac{23}{3}\right) = \left(\frac{2}{3}\right) \equiv 2^1 \bmod 3$. Thus, $\left(\frac{2}{3}\right) = -1$ so $\left(\frac{3}{23}\right) = 1$ try again!

   Guess $g = 5$. $\left(\frac{5}{23}\right)\left(\frac{23}{5}\right) = (-1)^{\frac{23-1}{2}\frac{5-1}{2}} = (-1)^{22} = 1$ but $\left(\frac{23}{5}\right) = \left(\frac{3}{5}\right) \equiv 2^2 \bmod 5$. Thus, $\left(\frac{23}{5}\right) = -1$ so $\left(\frac{5}{23}\right) = -1$ thus 5 is a primitive root in $\mathbb{F}_{23}^{\times}$.

3. (a) $\mathbb{Q}(\sqrt{d}) = \{a+b\sqrt{d} \mid a, b \in \mathbb{Q}\}$. By construction, $\{1, \sqrt{d}\}$ spans $\mathbb{Q}(\sqrt{d})$ and if $a+b\sqrt{d} = 0$ then $\sqrt{d} = -\frac{a}{b}$ which contradicts d being a non-square in $\mathbb{Q}$. Thus, $[\mathbb{Q}(\sqrt{d}) : \mathbb{Q}] = 2$ because $\{1, \sqrt{d}\}$ is a basis for $\mathbb{Q}(\sqrt{d})$ over $\mathbb{Q}$.

Now, let K be any quadratic extension of $\mathbb{Q}$ then take $x \in K \backslash \text{span}\{1\}$. Then $|\{1, x\}| = 2$ and is independent so it is a basis. Thus, $\exists a, b \in \mathbb{Q} : x^2 = a + bx$ so $x = \frac{1}{2}(b \pm \sqrt{b^2 + 4a})$. Since $a, b \in \mathbb{Q}$, $b^2 + 4a = \frac{p}{q} \in \mathbb{Q}$. Since $x = \frac{b}{2} \cdot 1 + (\pm\frac{1}{2q})\sqrt{pq}$, both x and 1 can be reexpressed in the new basis: $\{1, \sqrt{b^2 - 4ac}\}$ therefore, $K = \mathbb{Q}(\sqrt{pq})$ with $pq \in \mathbb{Z}$.

Let $d \in \mathbb{Z}$ be a non-square so $x^2 - d$ is irreducible over $\mathbb{Q}$. Since $\pm\sqrt{d} \in \mathbb{Q}(\sqrt{d})$, $x^2 - d$ splits over $\mathbb{Q}(\sqrt{d})$. But $\mathbb{Q}(\sqrt{d})$ is an extension of $\mathbb{Q}$ of order 2 so it is the minimal field over which $x^2 - d$ splits. Thus $\mathbb{Q}(\sqrt{d})$ is the splitting field of $x^2 - d$ and therefore $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ is a Galois extension.

Since $|Gal(\mathbb{Q}(\sqrt{d})/\mathbb{Q})| = [\mathbb{Q}(\sqrt{d}) : \mathbb{Q}] = 2$ then $Gal(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$. Besides the identity automorphism, there is $\sigma \in Gal(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$ given by $\sigma : a + b\sqrt{d} \mapsto a - b\sqrt{d}$ and $\sigma^2 = \text{id}$.

(b) Let $d/d' = q^2 \in \mathbb{Q}$ be a square. $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\} =$
$\{a + b\sqrt{q^2 d'} \mid a, b \in \mathbb{Q}\} = \{a + bq\sqrt{d'} \mid a, b \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{d'})$

Let $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{d'})$ then for any $a, b \in \mathbb{Q}$, $a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{d'})$. $\sqrt{d} \in \mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{d'})$ so $\exists a, b \in \mathbb{Q} : \sqrt{d} = a + b\sqrt{d'}$. Then, $d = a^2 + 2ab\sqrt{d'} + b^2 d'$ so if $a \neq 0$ then $\sqrt{d'} = \frac{d - a^2 - b^2 d'}{2ab}$ which is impossible since $\sqrt{d'} \notin \mathbb{Q}$. Thus $a = 0$ and therefore, $\sqrt{d} = b\sqrt{d'}$ so $d/d' = b^2$ with $b \in \mathbb{Q}$.

If K is a quadratic extension of $\mathbb{Q}$ then $\exists q \in \mathbb{Z}$ s.t. $K = \mathbb{Q}(\sqrt{q})$ then write the prime factorization, $q = p_1^{a_1} \ldots p_k^{a_k}$. Let $q' = p_1^{\tilde{a}_i} \ldots p_k^{\tilde{a}_i}$ where $\tilde{a}_i = a_i \text{mod} 2$ so $q/q' = p_1^{a_i - \tilde{a}_i} \ldots p_k^{a_i - \tilde{a}_i}$ which is a square since
$a_i \equiv \tilde{a}_i \bmod 2$ therefore, $\mathbb{Q}(\sqrt{q}) = \mathbb{Q}(\sqrt{q'})$ so every quadratic extension is $\mathbb{Q}(\sqrt{p_1 \ldots p_k})$ with distinct primes p_i since every $\tilde{a}_i = 0, 1$.

(c) Let $P(x) = ax^2 + bx + c \in Z[x]$ be irreducible over $\mathbb{Q}$. Then $r_\pm = \frac{1}{2}(-b \pm \sqrt{b^2 - 4ac})$ are the roots of P. Let $\Delta = b^2 - 4ac$ then $r_\pm \in \mathbb{Q}(\sqrt{\Delta})$ so P splits over $\mathbb{Q}(\sqrt{\Delta})$. Since $\mathbb{Q}(\sqrt{\Delta})$ is a quadratic extension over $\mathbb{Q}$, there are no proper subfields besides $\mathbb{Q}$ thus $\mathbb{Q}(\sqrt{\Delta})$ is the splitting field of P. Also, $\Delta \equiv b^2 \bmod 4$ so Δ is a quadratic residue modulo 4. Thus, $\Delta \equiv 0, 1 \bmod 4$.

(d) Let $d \in \mathbb{Z}$ be a square-free integer. If $d \equiv 1 \bmod 4$ then for any b s.t. $2 \not| b$ we have that $b^2 \equiv 1 \bmod 4$ so $d - b^2 \equiv 0 \bmod 4$ then $d = b^2 - 4c$ for $c \in \mathbb{Z}$. Take $Q(x) = x^2 + bx + c$ then $\Delta = b^2 - 4c = d$ so $\mathbb{Q}(\sqrt{d})$ is the splitting field of Q. In particular, let $b = 1$ then $c = (1 - d)/4$ so $Q(x) = x^2 + x + \frac{1-d}{4}$

If $d \not\equiv 1\ mod\ 4$ then take $Q(x) = x^2 - d$ so $\Delta = 4d$ and by above $\mathbb{Q}(\sqrt{d})$ is the splitting field of Q.