**Rep#2a: Finite subgroups of multiplicative groups of fields**

Darij Grinberg

[not completed, not proofread]

This note is mostly an auxiliary note for Rep#2. We are going to prove a fact which is used rather often in algebra:

**Theorem 1.** Let $A$ be a field, and let $G$ be a finite subgroup of the multiplicative group $A^{\times}$. Then, $G$ is a cyclic group.

This theorem generalizes the (well-known) fact that the multiplicative group of a finite field is cyclic. Most proofs of this fact can actually be used to prove Theorem 1 in all its generality, so there is not much need to provide another proof here. But yet, let us sketch a proof of Theorem 1 that requires only basic number theory. The downside is that it is very ugly. First, an easy number-theoretical lemma:

**Lemma 2.** Let $i$, $g$ and $a$ be three integers such that $a$ is positive, such that $g \mid a$, and such that $i$ is coprime to $g$. Then, there exists an integer $I$ such that $I \equiv i \bmod g$ and such that $I$ is coprime to $a$.

*Proof of Lemma 2.* For every integer $n$, let us denote by $\operatorname{PF} n$ the set of all prime divisors of $n$. By the unique factorization theorem, for any positive integer $n$, the set $\operatorname{PF} n$ is finite and satisfies $n = \prod\limits_{p \in \operatorname{PF} n} p^{v_p(n)}$.

Clearly, $a \neq 0$ (since $a$ is positive) and $g \neq 0$ (since $a \neq 0$ and $g \mid a$). Now, $g \mid a$ yields $\operatorname{PF} g \subseteq \operatorname{PF} a$. We have

$$a = \prod_{p \in \operatorname{PF} a} p^{v_p(a)} = \prod_{p \in \operatorname{PF} g} p^{v_p(a)} \cdot \prod_{p \in \operatorname{PF} a \setminus \operatorname{PF} g} p^{v_p(a)} \qquad (\text{since } \operatorname{PF} g \subseteq \operatorname{PF} a).$$

In other words, $a = a_1 a_2$, where $a_1 = \prod\limits_{p \in \operatorname{PF} g} p^{v_p(a)}$ and $a_2 = \prod\limits_{p \in \operatorname{PF} a \setminus \operatorname{PF} g} p^{v_p(a)}$.

The number $g$ is not divisible by any prime $p \in \operatorname{PF} a \setminus \operatorname{PF} g$ (because if $g$ is divisible by a prime $p$, then $p \in \operatorname{PF} g$, so that $p$ cannot lie in $\operatorname{PF} a \setminus \operatorname{PF} g$). Hence, $g$ is coprime to $p^{v_p(a)}$ for every $p \in \operatorname{PF} a \setminus \operatorname{PF} g$. Consequently, $g$ is coprime to the product $\prod\limits_{p \in \operatorname{PF} a \setminus \operatorname{PF} g} p^{v_p(a)}$. In other words, $g$ is coprime to $a_2$ (since $\prod\limits_{p \in \operatorname{PF} a \setminus \operatorname{PF} g} p^{v_p(a)} = a_2$). Thus, by Bezout's Theorem[1], there exist integers $\rho_1$ and $\rho_2$ such that $\rho_1 g + \rho_2 a_2 = 1$. Thus, $1 - \rho_1 g = \rho_2 a_2 \equiv 0 \bmod a_2$. Now, let $I = i - (i-1)\rho_1 g$. Then, $I = i - (i-1)\rho_1 g \equiv i \bmod g$. Hence, $I$ is coprime to $g$ (since $i$ is coprime to $g$). Hence, $I$ is not divisible by any prime $p \in \operatorname{PF} g$. Thus, $I$ is coprime to $p^{v_p(a)}$ for every $p \in \operatorname{PF} g$. Consequently, $I$ is coprime to the product $\prod\limits_{p \in \operatorname{PF} g} p^{v_p(a)}$. In other words, $I$ is coprime to $a_1$ (since $\prod\limits_{p \in \operatorname{PF} g} p^{v_p(a)} = a_1$). On the other hand, $I$ is coprime to $a_2$ (since

$$I = i - (i-1)\rho_1 g = i \underbrace{(1 - \rho_1 g)}_{\equiv 0 \bmod a_2} + \rho_1 g \equiv \rho_1 g \equiv \rho_1 g + \rho_2 a_2 = 1 \bmod a_2$$

[1]**Bezout's theorem** states that if $\lambda_1$ and $\lambda_2$ are two coprime integers, then there exist integers $\rho_1$ and $\rho_2$ such that $\rho_1 \lambda_1 + \rho_2 \lambda_2 = 1$.

). Hence, $I$ is coprime to $a_1 a_2$ (since $I$ is coprime to $a_1$ and to $a_2$). In other words, $I$ is coprime to $a$ (since $a_1 a_2 = a$). This proves Lemma 2.

*Proof of Theorem 1.* We first notice that

$$\text{if } \alpha \text{ and } \beta \text{ are two elements of } G\text{, then there exists } \gamma \in G \text{ such that } \alpha \in \langle \gamma \rangle \text{ and } \beta \in \langle \gamma \rangle . \tag{1}$$

*Proof of (1).* Let $a$ be the order of $\alpha$ in $G$, and let $b$ be the order of $\beta$ in $G$. Let $g$ be $\gcd(a, b)$. Then, $g \mid a$ and $g \mid b$. Thus, $(a/g) \mid a$ and $(b/g) \mid b$.

The order of $\alpha$ in $G$ is $a$. Hence, the order of $\alpha^{a/g}$ in $G$ is $\dfrac{a}{a/g} = g$ (since $(a/g) \mid a$). Consequently, the elements $\left(\alpha^{a/g}\right)^0$, $\left(\alpha^{a/g}\right)^1$, ..., $\left(\alpha^{a/g}\right)^{g-1}$ are pairwise distinct, and we have $\left(\alpha^{a/g}\right)^g = 1$. Now, for every $i \in \{0, 1, ..., g-1\}$, we have $\left(\left(\alpha^{a/g}\right)^i\right)^g = \Bigg(\underbrace{\left(\alpha^{a/g}\right)^g}_{=1}\Bigg)^i = 1$, and thus the element $\left(\alpha^{a/g}\right)^i$ is a root of the polynomial $X^g - 1 \in A[X]$. In other words, the elements $\left(\alpha^{a/g}\right)^0$, $\left(\alpha^{a/g}\right)^1$, ..., $\left(\alpha^{a/g}\right)^{g-1}$ are roots of the polynomial $X^g - 1 \in A[X]$. Since we know that these elements $\left(\alpha^{a/g}\right)^0$, $\left(\alpha^{a/g}\right)^1$, ..., $\left(\alpha^{a/g}\right)^{g-1}$ are pairwise distinct, we thus see that the elements $\left(\alpha^{a/g}\right)^0$, $\left(\alpha^{a/g}\right)^1$, ..., $\left(\alpha^{a/g}\right)^{g-1}$ are pairwise distinct roots of the polynomial $X^g - 1 \in A[X]$. But the polynomial $X^g - 1 \in A[X]$ can only have at most $g$ roots (since any nonzero polynomial of degree $g$ over a field can only have at most $g$ roots), so these roots $\left(\alpha^{a/g}\right)^0$, $\left(\alpha^{a/g}\right)^1$, ..., $\left(\alpha^{a/g}\right)^{g-1}$ must be all the roots of the polynomial $X^g - 1 \in A[X]$. Consequently, the polynomial $X^g - 1$ equals a constant times $\left(X - \left(\alpha^{a/g}\right)^0\right)\left(X - \left(\alpha^{a/g}\right)^1\right) ... \left(X - \left(\alpha^{a/g}\right)^{g-1}\right)$. But the constant just mentioned must be 1 (since the polynomials $X^g - 1$ and $\left(X - \left(\alpha^{a/g}\right)^0\right)\left(X - \left(\alpha^{a/g}\right)^1\right) ... \left(X - \left(\alpha^{a/g}\right)^{g-1}\right)$ have the same leading term); hence, this becomes

$$X^g - 1 = \left(X - \left(\alpha^{a/g}\right)^0\right)\left(X - \left(\alpha^{a/g}\right)^1\right) ... \left(X - \left(\alpha^{a/g}\right)^{g-1}\right).$$

In other words, $X^g - 1 = \prod_{i=0}^{g-1} \left(X - \left(\alpha^{a/g}\right)^i\right)$. Applying this identity to $X = \beta^{b/g}$, we obtain $\left(\beta^{b/g}\right)^g - 1 = \prod_{i=0}^{g-1} \left(\beta^{b/g} - \left(\alpha^{a/g}\right)^i\right)$. Since $\left(\beta^{b/g}\right)^g - 1 = \beta^b - 1 = 0$ (since $b$ is the order of $\beta$, and thus $\beta^b = 1$), this becomes $0 = \prod_{i=0}^{g-1} \left(\beta^{b/g} - \left(\alpha^{a/g}\right)^i\right)$. Hence, there must exist some $i \in \{0, 1, ..., g-1\}$ such that $\beta^{b/g} - \left(\alpha^{a/g}\right)^i = 0$ (because if a product of elements of a field is zero, then one of the factors must be zero). Consequently, this $i \in \{0, 1, ..., g-1\}$ satisfies $\beta^{b/g} = \left(\alpha^{a/g}\right)^i$. Similarly, there exists some $j \in \{0, 1, ..., g-1\}$ satisfying $\alpha^{a/g} = \left(\beta^{b/g}\right)^j$. Thus, $\alpha^{a/g} = \Bigg(\underbrace{\beta^{b/g}}_{=\left(\alpha^{a/g}\right)^i}\Bigg)^j =$

$\left(\left(\alpha^{a/g}\right)^i\right)^j = \left(\alpha^{a/g}\right)^{ij}$, so that $1 = \dfrac{\left(\alpha^{a/g}\right)^{ij}}{\alpha^{a/g}} = \left(\alpha^{a/g}\right)^{ij-1}$. Since the order of the element $\alpha^{a/g}$ is $g$, this yields $g \mid ij-1$, so that $ij \equiv 1 \bmod g$. Hence, $ij$ is coprime to $g$, so that $i$ must also be coprime to $g$. Thus, by Lemma 2, there exists an integer $I$ such that $I \equiv i \bmod g$ and such that $I$ is coprime to $a$. Since $I \equiv i \bmod g$, we have $g \mid I-i$, and thus $\left(\alpha^{a/g}\right)^{I-i} = 1$ (since $g$ is the order of $\alpha^{a/g}$), so that

$$\left(\alpha^{a/g}\right)^I = \left(\alpha^{a/g}\right)^{(I-i)+i} = \underbrace{\left(\alpha^{a/g}\right)^{I-i}}_{=1} \left(\alpha^{a/g}\right)^i = \left(\alpha^{a/g}\right)^i = \beta^{b/g}. \tag{2}$$

Now, the integers $a/g$ and $b/g$ are coprime (since $\gcd(a/g, b/g) = \underbrace{\gcd(a,b)}_{=g}/g = g/g = 1$); hence, by Bezout's Theorem, there exist integers $u$ and $v$ such that $u \cdot a/g + v \cdot b/g = 1$. Now, let $\gamma = \alpha^{Iv}\beta^u$. Then, $\gamma \in G$ and

$$\gamma^{b/g} = \left(\alpha^{Iv}\beta^u\right)^{b/g} = \underbrace{\left(\alpha^{Iv}\right)^{b/g}}_{=\alpha^{Iv\cdot b/g}} \underbrace{\left(\beta^u\right)^{b/g}}_{=\left(\beta^{b/g}\right)^u} = \alpha^{Iv\cdot b/g} \left(\underbrace{\beta^{b/g}}_{\substack{=\left(\alpha^{a/g}\right)^I \\ \text{(by (2))}}}\right)^u = \alpha^{Iv\cdot b/g} \underbrace{\left(\left(\alpha^{a/g}\right)^I\right)^u}_{=\left(\alpha^{a/g}\right)^{Iu}=\alpha^{Iu\cdot a/g}}$$
$$= \alpha^{Iv\cdot b/g}\alpha^{Iu\cdot a/g} = \alpha^{Iv\cdot b/g + Iu\cdot a/g} = \alpha^I$$

(since $Iv \cdot b/g + Iu \cdot a/g = I \underbrace{(u \cdot a/g + v \cdot b/g)}_{=1} = I$). Since $I$ is coprime to $a$, there exist integers $x$ and $y$ such that $xI + ya = 1$ (according to Bezout's theorem). Thus,

$$\alpha = \alpha^1 = \alpha^{Ix+ay} \qquad \text{(since } 1 = xI + ya = Ix + ay\text{)}$$
$$= \underbrace{\alpha^{Ix}}_{=(\alpha^I)^x} \underbrace{\alpha^{ay}}_{=(\alpha^a)^y} = \left(\underbrace{\alpha^I}_{=\gamma^{b/g}}\right)^x \left(\underbrace{\alpha^a}_{\substack{=1 \text{ (since } a \text{ is} \\ \text{the order of } \alpha)}}\right)^y = \left(\gamma^{b/g}\right)^x 1^y = \left(\gamma^{b/g}\right)^x \in \langle\gamma\rangle.$$

On the other hand, since $\gamma = \alpha^{Iv}\beta^u$, we have

$$\gamma^{a/g} = \left(\alpha^{Iv}\beta^u\right)^{a/g} = \underbrace{\left(\alpha^{Iv}\right)^{a/g}}_{\substack{=\alpha^{Iv\cdot a/g} = \alpha^{(a/g)\cdot Iv} \\ =\left(\alpha^{a/g}\right)^{Iv} = \left(\left(\alpha^{a/g}\right)^I\right)^v}} \cdot \underbrace{\left(\beta^u\right)^{a/g}}_{=\beta^{u\cdot(a/g)}} = \left(\underbrace{\left(\alpha^{a/g}\right)^I}_{\substack{=\beta^{b/g} \\ \text{(by (2))}}}\right)^v \cdot \beta^{u\cdot(a/g)}$$
$$= \underbrace{\left(\beta^{b/g}\right)^v}_{=\beta^{(b/g)\cdot v} = \beta^{v\cdot(b/g)}} \cdot \beta^{u\cdot(a/g)} = \beta^{v\cdot(b/g)} \cdot \beta^{u\cdot(a/g)} = \beta^{v\cdot(b/g)+u\cdot(a/g)}$$
$$= \beta^1 \qquad \text{(since } v\cdot(b/g) + u\cdot(a/g) = u \cdot a/g + v \cdot b/g = 1\text{)}$$
$$= \beta,$$

and therefore $\beta = \gamma^{a/g} \in \langle\gamma\rangle$.

Altogether, we have proven that $\gamma \in G$, that $\alpha \in \langle \gamma \rangle$ and that $\beta \in \langle \gamma \rangle$. This proves (1).

Now, let us finally prove Theorem 1: Clearly, there exists a subset $P$ of the group $G$ such that $G = \langle P \rangle$ (in fact, the whole group $G$ is an example of such a subset $P$). Let $U$ be such a subset with the smallest number of elements.[2] Then, $U$ is a subset of the group $G$ such that $G = \langle U \rangle$, but there is no subset $U'$ of $G$ with less elements than $U$ that satisfies $G = \langle U' \rangle$.

We let $k = |U|$, and we write the set $U$ as $U = \{u_1, u_2, ..., u_k\}$, where $u_1$, $u_2$, ..., $u_k$ are the $k$ (pairwise distinct) elements of $U$. Assume now that $k > 1$. Then, $u_1$ and $u_2$ are well-defined. Now, there exists an element $\gamma \in G$ such that $u_1 \in \langle \gamma \rangle$ and $u_2 \in \langle \gamma \rangle$ (by (1), applied to $\alpha = u_1$ and $\beta = u_2$), and therefore $u_i \in \langle \gamma, u_3, u_4, ..., u_k \rangle$ for every $i \in \{1, 2, ..., k\}$ [3]. Hence, $\langle u_1, u_2, ..., u_k \rangle \subseteq \langle \gamma, u_3, u_4, ..., u_k \rangle$, so that

$$G = \langle U \rangle = \langle \{u_1, u_2, ..., u_k\} \rangle = \langle u_1, u_2, ..., u_k \rangle \subseteq \langle \gamma, u_3, u_4, ..., u_k \rangle = \langle \{\gamma, u_3, u_4, ..., u_k\} \rangle = \langle U' \rangle ,$$

where $U'$ denotes the subset $\{\gamma, u_3, u_4, ..., u_k\}$ of $G$. But clearly, also $G \supseteq \langle U' \rangle$. Thus, $G = \langle U' \rangle$. Besides, the subset $U'$ of $G$ has less elements than $U$ (because $U' = \{\gamma, u_3, u_4, ..., u_k\}$ has at most $k - 1$ elements, while $U$ has $|U| = k$ elements). This contradicts to the fact that there is no subset $U'$ of $G$ with less elements than $U$ that satisfies $G = \langle U' \rangle$. This contradiction shows that our assumption $k > 1$ was wrong. Hence, $k \leq 1$, so that $k = 1$ or $k = 0$. If $k = 0$, then $|U| = k = 0$ and thus $U = \varnothing$, which leads to $G = \langle \varnothing \rangle = 1$, so that $G$ is a cyclic group. If $k = 1$, then $|U| = k = 1$, so that $U = \{u\}$ for some $u \in G$, and therefore $G = \langle U \rangle = \langle \{u\} \rangle = \langle u \rangle$ is a cyclic group. Hence, in both cases, $G$ is a cyclic group. This proves Theorem 1.

Here is an easy consequence of Theorem 1:

**Lemma 3.** Let $A$ be a field. Let $n$ be a positive integer, and for every $i \in \{1, 2, ..., n\}$, let $\xi_i$ be a root of unity in $A$. Then, there exists some root of unity $\zeta$ of $A$ and a sequence $(k_1, k_2, ..., k_n)$ of nonnegative integers such that $\left(\xi_i = \zeta^{k_i} \text{ for every } i \in \{1, 2, ..., n\}\right)$ and $\gcd(k_1, k_2, ..., k_n) = 1$.

*Proof of Lemma 3.* Let $G$ be the subgroup $\langle \xi_1, \xi_2, ..., \xi_n \rangle$ of the multiplicative group $A^\times$. Then, the map

$$\Phi : \langle \xi_1 \rangle \times \langle \xi_2 \rangle \times ... \times \langle \xi_n \rangle \to \langle \xi_1, \xi_2, ..., \xi_n \rangle \qquad \text{defined by}$$
$$(x_1, x_2, ..., x_n) \mapsto x_1 x_2 ... x_n$$

is surjective (because every element of $\langle \xi_1, \xi_2, ..., \xi_n \rangle$ has the form $\prod\limits_{i=1}^{n} \xi_i^{f_i}$ for some $n$-tuple $(f_1, f_2, ..., f_n)$ of integer, and thus is $\Phi\left(\xi_1^{f_1}, \xi_2^{f_2}, ..., \xi_n^{f_n}\right)$), and the set $\langle \xi_1 \rangle \times \langle \xi_2 \rangle \times ... \times \langle \xi_n \rangle$ is finite (since the set $\langle \xi_i \rangle$ is finite for every $i \in \{1, 2, ..., n\}$, because $\xi_i$ is a root of unity). Hence, the set $\langle \xi_1, \xi_2, ..., \xi_n \rangle$ is finite. Thus, $G = \langle \xi_1, \xi_2, ..., \xi_n \rangle$ is a finite subgroup of

[2]Indeed, such a $U$ exists, because the set of all subsets of the group $G$ is finite (since $G$ itself is finite).

[3]In fact, three cases are possible: either $i = 1$, or $i = 2$, or $i \geq 3$. If $i = 1$, then $u_i \in \langle \gamma, u_3, u_4, ..., u_k \rangle$ follows from $u_1 \in \langle \gamma \rangle \subseteq \langle \gamma, u_3, u_4, ..., u_k \rangle$. If $i = 2$, then $u_i \in \langle \gamma, u_3, u_4, ..., u_k \rangle$ follows from $u_2 \in \langle \gamma \rangle \subseteq \langle \gamma, u_3, u_4, ..., u_k \rangle$. Finally, if $i \geq 3$, then $u_i \in \langle \gamma, u_3, u_4, ..., u_k \rangle$ is trivial. Thus, $u_i \in \langle \gamma, u_3, u_4, ..., u_k \rangle$ holds in all cases.

$A^\times$. Hence, by Theorem 1, this group $G$ is cyclic, so that there exists some $\tau \in G$ such that $G = \langle \tau \rangle$. Now, if $u$ is the order of $\tau$ in the group $G$, then $\langle \tau \rangle = \{\tau^0, \tau^1, ..., \tau^{u-1}\}$. Hence, for every $i \in \{1, 2, ..., n\}$, there exists some nonnegative integer $\ell_i$ such that $\xi_i = \tau^{\ell_i}$ (since $\xi_i \in G = \langle \tau \rangle = \{\tau^0, \tau^1, ..., \tau^{u-1}\}$). Now, let $\ell = \gcd(\ell_1, \ell_2, ..., \ell_n)$. Let $\zeta = \tau^\ell$, and let $k_i = \ell_i / \ell$ for every $i \in \{1, 2, ..., n\}$. Then, $\ell_i = \ell k_i$ for every $i \in \{1, 2, ..., n\}$.

Now we know that $\zeta$ is a root of unity (since $\zeta \in G$, and thus Lagrange's theorem yields $\zeta^{|G|} = 1$), and for every $i \in \{1, 2, ..., n\}$ we have $\xi_i = \tau^{\ell_i} = \tau^{\ell k_i} = \Bigl(\underbrace{\tau^\ell}_{=\zeta}\Bigr)^{k_i} = \zeta^{k_i}$. Finally, recall that $k_i = \ell_i / \ell$ for every $i \in \{1, 2, ..., n\}$. Thus, $\gcd(k_1, k_2, ..., k_n) = \gcd(\ell_1/\ell, \ell_2/\ell, ..., \ell_n/\ell) = \underbrace{\gcd(\ell_1, \ell_2, ..., \ell_n)}_{=\ell} / \ell = 1$. Thus, Lemma 3 is proven.