Solutions to Ireland, Rosen “A Classical Introduction to Modern Number Theory”

Richard Ganaye

October 11, 2019

Chapter 7

Ex. 7.1 *Use the method of Theorem 1 to show that a finite subgroup of the multiplicative group of a field is cyclic.*

A solution is already given in Ex. 4.15

Ex. 7.2 *Find the finite subgroups of* $\mathbb{R}^*$ *and* $\mathbb{C}^*$ *and show directly that they are cyclic.*

Proof. If G is a finite subgroup of $\mathbb{R}$ or $\mathbb{C}$, and $n = |G|$, then from Lagrange's Theorem, $x^n = 1$ for all $x \in G$.

• If G is a finite subgroup of $\mathbb{R}^*$, then the solutions of $x^n = 1$ are in $\{-1, 1\}$, so $\{1\} \subset G \subset \{-1, 1\}$: $G = \{1\}$ or $G = \{-1, 1\}$, both cyclic.

• If G is a finite subgroup of $\mathbb{C}^*$, then $G \subset \mathbb{U}_n = \{e^{2ik\pi/n} \mid 0 \le k \le n-1\}$. As $|G| = |\mathbb{U}_n| = n$, then $G = \mathbb{U}_n \simeq \mathbb{Z}/n\mathbb{Z}$ is cyclic. □

Ex. 7.3 *Let* F *a field with* q *elements and suppose that* $q \equiv 1 \pmod n$*. Show that for* $\alpha \in \mathbb{F}^*$*, the equation* $x^n = \alpha$ *has either no solutions or* n *solutions.*

Proof. This is a particular case of Prop. 7.1.2., where $d = n \wedge (q-1) = n$: the equation $x^n = \alpha$ has solutions iff $\alpha^{(q-1)/n} = 1$. In this case, there are exactly $d = n$ solutions.

We give here a direct proof.

Let g a generator of F^*. Write $x = g^y, \alpha = g^a$. Then

$$x^n = \alpha \iff g^{ny} = g^a \iff q - 1 \mid ny - a.$$

Suppose that there exists $x \in F$ such that $x^n = \alpha$. Then there exists $y \in \mathbb{Z}$ such that $q - 1 \mid ny - a$. Since $n \mid q - 1$, then $n \mid a$.

$$q - 1 \mid ny - a \iff \frac{q-1}{n} \mid y - \frac{a}{n} \iff y = \frac{a}{n} + k\frac{q-1}{n}, k \in \mathbb{Z}.$$

As $\frac{a}{n} + (k+n)\frac{q-1}{n} = \frac{a}{n} + k\frac{q-1}{n}, k \in \mathbb{Z}$, the values $k = 0, 1 \cdots, n-1$ are sufficient :

$$x^n = \alpha \iff y = \frac{a}{n} + k\frac{q-1}{n}, k \in \{0, 1, \cdots, n-1\}.$$

Moreover, these solutions are all distinct : if $k, l \in \{0, 1, \cdots, n-1\}$,

$$\begin{aligned} g^{\frac{a}{n}+k\frac{q-1}{n}} = g^{\frac{a}{n}+l\frac{q-1}{n}} &\Rightarrow g^{(k-l)\frac{q-1}{n}} = 1 \\ &\Rightarrow q-1 \mid (k-l)\frac{q-1}{n} \\ &\Rightarrow n \mid k-l \\ &\Rightarrow k \equiv l \ [n] \Rightarrow k = l. \end{aligned}$$

Conclusion : if F is a field with q elements and $n \mid q-1$, the equation $x^n = \alpha$ has either no solutions or n solutions in F.

Remark :

$$\exists x \in F^*, x^n = \alpha \iff n \mid a \iff \alpha^{(q-1)/n} = 1.$$

Indeed, if $x^n = \alpha$ has a solution, we have proved that $n \mid a$, thus $\alpha^{(q-1)/n} = (g^{a/n})^{q-1} = 1$.

Reciprocally, if $\alpha^{(q-1)/n} = 1$, $g^{a.(q-1)/n} = 1$, thus $q-1 \mid a(q-1)/n$, so $n \mid a$: $\alpha = x^n$, with $x = g^{n/a}$. □

Ex. 7.4 *(continuation) Show that the set of $\alpha \in F^*$ such that $x^n = \alpha$ is solvable is a subgroup with $(q-1)/n$ elements.*

Proof. Here $n \mid q-1$.

Let $\varphi = F^* \to F^*$ the application defined by $\varphi(x) = x^n$. φ is a morphism of groups, and $\ker\varphi$ is the set of solutions of $x^n = 1$. As $n \mid q-1$, $x^n = 1$ has exactly n solutions (Prop 7.1.1, Corollary2, or Ex 7.3 with $\alpha = 1$). So $|\ker\varphi| = n$.

Thus $\mathrm{Im}\varphi \simeq F^*/\ker\varphi$ is a subgroup with cardinality $|F^*|/|\ker\varphi| = (q-1)/n$, and $\mathrm{Im}\varphi$ is the set of α such that $x^n = \alpha$ is solvable.

Conclusion : the set of $\alpha \in F^*$ such that $x^n = \alpha$ is solvable is a subgroup with $(q-1)/n$ elements.

□

Ex. 7.5 *(continuation) Let K be a field containing F such that $[K : F] = n$. For all $\alpha \in F^*$, show that the equation $x^n = \alpha$ has n solutions in K. [Hint: Show that $q^n - 1$ is divisible by $n(q-1)$ and use the fact that $\alpha^{q-1} = 1$.]*

Proof. As $q \equiv 1 \ [n]$, $\frac{q^n-1}{q-1} = 1 + q + \cdots + q^{n-1} \equiv 0 \ [n]$, then $n \mid \frac{q^n-1}{q-1}$:

$$q^n - 1 = kn(q-1), k \in \mathbb{N}.$$

Since $\alpha \in F^*$, $\alpha^{q-1} = 1$, so

$$\alpha^{(q^n-1)/n} = (\alpha^{q-1})^k = 1.$$

As $|K| = q^n$, Prop. 7.1.2 (or the final remark in Ex.7.3) show that there exists $x \in K^*$ such that $x^n = \alpha$. Then, from Ex.7.3, we know that there exist n solutions in K.

Conclusion : if $[K : F] = n$, the equation $x^n = \alpha$ has n solutions in K.

□

Ex. 7.6 *Let $K \supset F$ be finite fields with $[K:F] = 3$. Show that if $\alpha \in F$ is not a square in F, it is not a square in K.*

Proof. Let $q = |F|$. Then $|K| = q^3$.

If the characteristic of F is 2, $q = 2^k$, and for all $x \in F$, $x = x^q = \left(x^{2^{k-1}}\right)^2$. So all elements in F or K are squares. We can now suppose that the characteristic of F is not 2, and consequently $1 \neq -1$ in F.

As α is not a square in F, $\alpha^{(q-1)/2} \neq 1$ (Prop. 7.1.2). From $0 = \alpha^{q-1} - 1 = (\alpha^{(q-1)/2} - 1)(\alpha^{(q-1)/2} + 1)$, we deduce $\alpha^{(q-1)/2} = -1$. Then

$$\alpha^{(q^3-1)/2} = (\alpha^{(q-1)/2})^{q^2+q+1} = (-1)^{q^2+q+1} = -1,$$

since $q^2 + q + 1$ is always odd.

$\alpha^{(q^3-1)/2} \neq 1$: this implies (Prop. 7.1.2) that α is not a square in K. □

Ex. 7.7 *Generalize Exercise 6 by showing that if α is not a square in F, it is not a square in any extension of odd degree and is a square in every extension of even degree.*

Proof. Write $q = [K : F]$, and $q = \text{Card } F$.

As α is not a square in F, the characteristic of F is not 2 (see Ex.7.6), and $\alpha^{(q-1)/2} \neq 1$. Since $\alpha^{q-1} = 1$, $\alpha^{(q-1)/2} = -1$.

$$\alpha^{(q^n-1)/2} = (\alpha^{(q-1)/2})^{1+q+\cdots+q^{n-1}} = (-1)^{1+q+\cdots+q^{n-1}}.$$

• If n is odd, $1+q+\cdots+q^{n-1} \equiv 1 \pmod 2$, thus $\alpha^{(q^n-1)/2} = -1 \neq 1$, and consequently α is not a square in K.

• If n is even, as q is odd ($\text{char}(F) \neq 2$), $1 + q + \cdots + q^{n-1} \equiv 0 \pmod 2$, thus $\alpha^{(q^n-1)/2} = 1$, so α is a square in K. □

Ex. 7.8 *In a field with 2^n elements, what is the subgroup of squares.*

Let F a field with $q = 2^n$ elements.

Proof 1

Proof. $d = (q-1) \wedge 2 = (2^n - 1) \wedge 2 = 1$, thus each $\alpha \in F^*$ verifies $\alpha^{(q-1)/d} = \alpha^{q-1} = 1$. Theorem 7.1.2 show that α is a square in F, of exactly one root. □

Proof 2

Proof. For all $x \in F$, $x = x^q = \left(x^{2^{n-1}}\right)^2$. So all elements in F or K are squares. □

Ex. 7.9 *If $K \supset F$ are finite fields, $|F| = q, \alpha \in F, q \equiv 1 \pmod n$, and $x^n = \alpha$ is not solvable in F, show that $x^n = \alpha$ is not solvable in K if $(n, [K:F]) = 1$.*

Proof. Let $k = [K : F]$. From hypothesis, $k \wedge n = 1$, so there exist integers u, v such that $uk + vn = 1$.

As $n \mid q - 1$, $n \wedge (q-1) = n$, so the hypothesis "$x^n = \alpha$ is not solvable in F" implies that $\alpha^{(q-1)/n} \neq 1$ (Prop. 7.1.2).

Write $\omega = \alpha^{(q-1)/n}$, so $\omega \neq 1$ and $\omega^n = 1$.

As $n \mid q-1$, $n \mid q^k - 1$ and

$$\alpha^{(q^k-1)/n} = (\alpha^{(q-1)/n})^{1+q+q^2+\cdots+q^{k-1}} = \omega^{1+q+q^2+\cdots+q^{k-1}}.$$

Moreover $1+q+\cdots+q^{k-1} \equiv k \pmod{n}$, and $\omega^n = 1$, so $\alpha^{(q^k-1)/n} = \omega^k$.

If $\omega^k = 1$, then $\omega = \omega^{uk+vn} = (\omega^k)^u(\omega^n)^v = 1$, which is in contradiction with $\omega = \alpha^{(q-1)/n} \neq 1$.

So $\alpha^{(q^k-1)/n} = \omega^k \neq 1$, and consequently the equation $x^n = \alpha$ has no solution in K. □

Ex. 7.10 *If $K \supset F$ be finite fields and $[K : F] = 2$. For $\beta \in K$, show that $\beta^{1+q} \in F$ and moreover that every element in F is of the form β^{1+q} for some $\beta \in K$.*

Proof. If $\beta = 0$, $\beta^{1+q} = 0 \in F$, and if $\beta \in K^*$, $\beta^{q^2-1} = 1$, so $\left(\beta^{1+q}\right)^{q-1} = 1$, thus $\beta^{1+q} \in F$ (Prop. 7.1.1, Corollary 1).

Let g a generator of $K^* : K^* = \{1, g, g^2, \cdots, g^{q^2-2}\}$.

For every in integer $k \in \mathbb{Z}$,

$$g^k \in F^* \iff (g^k)^{q-1} = 1 \iff g^{k(q-1)} = 1 \iff q^2 - 1 \mid k(q-1) \iff q+1 \mid k.$$

Thus $F^* = \{1, g^{q+1}, g^{2(q+1)}, \cdots, g^{(q-2)(q+1)}\}$. I $\alpha \in F^*$, there exists $i, 0 \leq i \leq q-1$ such that $\alpha = g^{i(q+1)}$. If we write $\beta = g^i$, then $\alpha = \beta^{1+q}$ (and for $\alpha = 0$, we take $\beta = 0$).

Conclusion : if K is a quadratic extension of F (F, K finite fields), every element in F is of the form β^{1+q} for some $\beta \in K$. □