itself) which can occur as the group of real points? Give an example of each.

2. How many points $P$ of order $n$ (i.e., $nP = O$) are there on an elliptic curve defined over $\mathbf{C}$? How about on an elliptic curve over $\mathbf{R}$?
3. Give an example of an elliptic curve over $\mathbf{R}$ which has exactly 2 points of order 2, and another example which has exactly 4 points of order 2.
4. Let $P$ be a point on an elliptic curve over $\mathbf{R}$. Suppose that $P$ is not the point at infinity. Give a geometric condition that is equivalent to $P$ being a point of order (a) 2; (b) 3; (c) 4.
5. Each of the following points has finite order on the given elliptic curve over $\mathbf{Q}$. In each case, find the order of $P$.
(a) $P = (0, 16)$ on $y^2 = x^3 + 256$.
(b) $P = (\frac{1}{2}, \frac{1}{2})$ on $y^2 = x^3 + \frac{1}{4}x$.
(c) $P = (3, 8)$ on $y^2 = x^3 - 43x + 166$.
(d) $P = (0, 0)$ on $y^2 + y = x^3 - x^2$ (which can be written in the form (1) by making the change of variables $y \longrightarrow y - \frac{1}{2}$, $x \longrightarrow x + \frac{1}{3}$).
6. Derive addition formulas similar to (4)–(5) for elliptic curves in characteristic 2, 3 (see Equations (2)–(3)).
7. Prove that there are $q + 1$ $\mathbf{F}_q$-points on the elliptic curve
(a) $y^2 = x^3 - x$ when $q \equiv 3 \ mod \ 4$;
(b) $y^2 = x^3 - 1$ when $q \equiv 2 \ mod \ 3$ (where $q$ is odd);
(c) $y^2 + y = x^3$ when $q \equiv 2 \ mod \ 3$ ($q$ may be even here).
8. For all odd prime powers $q = p^r$ up to 27 find the order and type of the group of $\mathbf{F}_q$-points on the elliptic curves $y^2 = x^3 - x$ and $y^2 = x^3 - 1$ (in the latter case when $p \neq 3$). In some cases you will have to check how many points have order 3 or 4.
9. Let $q = 2^r$, and let the elliptic curve $E$ over $\mathbf{F}_q$ have equation $y^2 + y = x^3$.
(a) Express the coordinates of $-P$ and $2P$ in terms of the coordinates of $P$.
(b) If $q = 16$, show that every $P \in E$ is a point of order 3.
(c) Show that any point of $E$ with coordinates in $\mathbf{F}_{16}$ actually has coordinates in $\mathbf{F}_4$. Then use Hasse's Theorem with $q = 4$ and 16 to determine the number of points on the curve.
10. Compute the zeta-functions of the two curves in Exercise 8 over $\mathbf{F}_p$ for $p = 5, 7, 11, 13$.
11. Compute the zeta function of the curve $y^2 + y = x^3 - x + 1$ over $\mathbf{F}_p$ for $p = 2$ and 3. (First show that $N_1 = 1$ in both cases.) Letting $\mathbf{N}(x) = x \cdot \bar{x}$ denote the norm of a complex number, find a simple formula for $N_r$.

## References for § VI.1

1. W. Fulton, *Algebraic Curves*, Benjamin, 1969.