BAB 4

KESIMPULAN

Berdasarkan pembahasan dari bab-bab sebelumnya, dapat disimpulkan bahwa belum ditemukan ciri-ciri yang berlaku secara umum bagi suatu polinomial atas *finite field* untuk menjadi polinomial permutasi. Tetapi telah didapatkan ciri-ciri dari beberapa jenis polinomial yang merupakan polinomial permutasi atas *finite field*. Untuk monomial $f(x) = x^k \in GF(q)[x], \quad k < q,$ monomial tersebut akan menjadi polinomial permutasi atas $GF(q)$ jika dan hanya jika $gcd(k, q-1) = 1$ seperti ditunjukkan pada Teorema 3.2, sedangkan untuk trinomial, dengan menambahkan syarat-syarat tertentu seperti yang ditunjukkan pada Teorema 3.4, Teorema 3.7, Akibat 3.8, maupun Teorema 3.9, trinomial tersebut akan menjadi polinomial permutasi. Akhirnya untuk *mth cyclotomic polynomial* $Q_m(x)$ atas $GF(q)$ yang karakteristiknya bukan 2 akan menjadi polinomial permutasi jika dan hanya jika $m = 2$.