

موعد تحویل: سه شنبه ۱۶ آذر ساعت ۱۶ (توجه: تمرین ها با تأخیر پذیرفته نخواهد شد).

پرسش های فصل ۲- قسمت سوم

۱- جدول میدان  $GF(2^5)$  را بر اساس چندجمله ای اولیه  $p(X)=1+X^2+X^5$  ایجاد نمایید. فرض کنید  $\alpha$  یک عنصر اولیه ی  $GF(2^5)$  باشد. چندجمله ای کمینه  $\alpha^3$  و چند جمله ای کمینه  $\alpha^7$  را بیابید.

۲- فرض کنید  $\beta$  عنصری از  $GF(2^m)$  باشد و  $e$  کوچکترین عدد صحیح نامنفی باشد که به ازای آن تساوی  $\beta^{2^e} = \beta$  برقرار باشد. اثبات کنید  $\beta^2$ ،  $\beta^{2^2}$ ، ، و  $\beta^{2^{e-1}}$  همگی مزدوج های متمایزی از  $\beta$  هستند.

۳- فرض کنید  $\alpha$  یک عنصر اولیه از میدان  $GF(2^4)$  باشد. چندجمله ای

$f(X)=\alpha^3X^7+\alpha X^6+\alpha^7X^4+\alpha^2X^2+\alpha^{11}X+1$  روی  $GF(2^4)$  را بر چندجمله ای  $g(X)=X^4+\alpha^3X^2+\alpha^5X+1$  روی  $GF(2^4)$  تقسیم کنید و باقیمانده و خارج قسمت آن را بیابید. از جدول ۲-۸ که قبلا به شما داده شده است استفاده نمایید.

۴- فرض کنید  $S$  یک زیرمجموعه از فضای برداری  $V_n$  (تمامی  $n$ -تایی ها روی  $GF(2)$ ) باشد. اثبات کنید  $S$  یک زیرفضا از  $V_n$  است اگر به ازای هر بردار  $u$  و  $v$  عضو  $S$ ،  $u+v$  نیز برداری عضو  $S$  باشد. (راهنمایی: نشان دهید در این صورت  $\delta$  شرط فضای برداری بودن  $S$  برقرار است. از صورت مسأله مشخص است که فضای برداری  $S$  روی گروه  $GF(2)$  تعریف شده است.)

۵- اثبات کنید مجموعه چندجمله ای ها روی  $GF(2)$  از درجه  $n-1$  یا کمتر یک فضای برداری روی  $GF(2)$  با بعد  $n$  تشکیل می دهد.

۶- اثبات کنید  $GF(2^m)$  یک فضای برداری روی  $GF(2)$  تشکیل می دهد.

۷- فضای برداری ۳-تایی ها روی  $GF(2)$  یعنی  $V_3$  را بسازید. یک زیرفضای دو بعدی از این فضا را یافته و فضای پوچی (فضای دوگان) آنرا مشخص کنید.

۸- ماتریس های زیر داده شده اند. نشان دهید فضای سطری ماتریس  $G$  فضای پوچی  $H$  است و برعکس.

$$G = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}, \quad H = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

۹- نشان دهید اگر  $S_1$  و  $S_2$  دو زیرفضا از فضای برداری  $V$  باشند در این صورت اشتراک آنها نیز یک زیرفضا از  $V$  تشکیل می دهد.

پیروز باشید.