بسمه تعالی

پاسخ سری سوم تمرین‌ها ــ ــ درس جبرخطی ۱ ــ دانشگاه صنعتی شریف

علیرضا توفیقی محمدی ــ رشته علوم کامپیوتر ــ شماره‌ی دانشجویی: ۹۶۱۰۰۳۶۳

۱ سوال ۲۶

۱.۱ الف

فرض کنید $v_1, ..., v_n$ پایه‌ای برای این فضا باشد. بین اعضای این فضا و ترکیب‌های خطی این پایه مثل $t_1.v_1 + ... + t_n.v_n$ تناظری یک‌به‌یک است؛ پس تعداد اعضای این فضا برابر با تعداد ترکیب‌خطی‌های این پایه است که هر ضریب چون عضوی از $\mathbb{Z}_p$ است p حالت دارد پس طبق اصل ضرب در کل p^n حالت برای ضریب‌ها داریم پس p^n ترکیب خطی از اعضای پایه و p^n عضو برای فضای V داریم.

۲.۱ ب

با کمک دو لم این قسمت را اثبات می‌کنیم.

۱.۲.۱ لم ۱

تعداد اعضای هر زیرفضای k بعدی از V برابر با p^k است.

فرض کنید T یک زیرفضای k بعدی از V بوده و $v_1, ..., v_k$ پایه‌ای برای این زیر فضا باشد. بین اعضای این زیر فضا و ترکیب‌های خطی این پایه مثل $t_1.v_1 + ... + t_n.v_n$ تناظری یک‌به‌یک است؛ پس تعداد اعضای این زیرفضا برابر با تعداد ترکیب‌خطی‌های این پایه است که هر ضریب چون عضوی از $\mathbb{Z}_p$ است p حالت دارد پس طبق اصل ضرب در کل p^k حالت برای ضریب‌ها داریم پس p^k عضو برای زیرفضای T داریم.

۲.۲.۱ لم ۲

اگر در فضایی n بعدی دلخواه مانند V، تعداد اعضای هر زیرفضای m بعدی برابر با $f(m)$ باشد، تعداد زیرفضاهای $k+1$ بعدی شامل یک زیرفضای k بعدی در V برابر با $\frac{f(n)-f(k)}{f(k+1)-f(k)}$ است.

فرض کنید T یک زیرفضای k بعدی دلخواه از V بوده و $v_1, ..., v_k$ پایه‌ای برای آن باشد، برای گسترش این فضا به یک فضای $k+1$ بعدی کافی‌است یه عضو مانند $w \in V$ که $w \notin T$ است را انتخاب کرده و به عنوان پایه‌ی $k+1$ام به T اضافه کنیم.

برای این‌کار $|V| - |T| = f(n) - f(k)$ حالت داریم که ادعا می‌کنیم هر زیرفضای $k+1$ بعدی

همچون U به تعداد $f(k+1)-f(k)$ بار شمرده می‌شود. برای اثبات این ادعا زیرفضای U را در نظر بگیرید، هر مجموعه به شکل $v_1, ..., v_k, w$ است که $w \notin T$ و $w \in U$ پایه‌ای برای U است (و اگر $w \notin V$ و $w \notin U$ این مجموعه پایه‌ای برای U نیست.) پس U در $f(k+1)-f(k)$ که تعداد حالت‌های انتخاب w است ساخته می‌شود پس هر زیرفضا در $f(k+1)-f(k)$ حالت ساخته شده و تعداد زیرفضاها برابر با $\frac{f(n)-f(k)}{f(k+1)-f(k)}$ است و حکم ثابت شد.

۳.۲.۱ مسئله‌ی اصلی

حال طبق لم ۱ و ۲ تعداد زیرفضاهای $k+1$ بعدی شامل یک زیرفضای k بعدی در V برابر است با:

$$\frac{p^n-p^k}{p^{k+1}-p^k} = \frac{p^k(p^{n-k}-1)}{p^k(p-1)} = \frac{p^{n-k}-1}{p-1}$$

و حکم ثابت شد.

۳.۱ ج

اگر بدانیم تعداد پایه‌های یک زیرفضای k بعدی برابر با $g(k)$ است و تعداد کل مجموعه مستقل‌های k تایی از فضای V برابر با $h(k)$ است، تعداد زیرفضاهای k بعدی برابر با $\frac{h(k)}{g(k)}$ است، زیرا هر زیرفضای برداری $g(k)$ بار در پایه‌ها شمرده شده‌است.
حال در ادامه به شمارش $g(k)$ و $h(k)$ می‌پردازیم.
فرض کنید در مجموعه‌ها ترتیب مهم است.
برای انتخاب یک پایه برای یک فضای k بعدی، از روش گسترش فضا استفاده می‌کنیم، ابتدا زیرفضای $\{0\}$ را در نظر گرفته و در هر مرحله یک عضو که داخل آن نیست را به آن اضافه می‌کنیم، طبق لم ۱ در قسمت ب، تعداد اعضای این زیرفضای برداری p^k است، پس در مرحله‌ی اول p^k-1 انتخاب داریم، حال مجموعه مستقل ساخته شده مولد زیرفضایی با p عضو است، پس برای عضو بعدی p^k-p عضو داریم و ... و در مرحله‌ی i ام برای عضو i ام p^k-p^{i-1} انتخاب داریم پس تعداد پایه‌های یک زیرفضای k بعدی برابر با $g(k)=(p^k-1)(p^k-p)...(p^k-p^{k-1})$ است.

حال می‌خواهیم تعداد کل مجموعه مستقل‌های kتایی از فضای V را بشماریم، برای اینکار همچون بند قبل مجموعه‌ی $\{0\}$ را در نظر گرفته و از روش گسترش مجموعه‌ی مستقل استفاده می‌کنیم تا به مجموعه مستقل kتایی برسیم، برای عضو اول p^n-1 حالت و ... و برای عضو iام p^n-p^i حالت و ... و برای عضو kام p^n-p^k حالت داریم. (مشابه استدلال بند قبل)، پس در کل تعداد مجموعه‌های مسقل k تایی برابر با $h(k)=(p^n-1)(p^n-p)...(p^n-p^{k-1})$ است.

پس جواب مسئله برابر است با:

$$\frac{h(k)}{g(k)} = \frac{(p^n-1)(p^n-p)...(p^n-p^{k-1})}{(p^k-1)(p^k-p)...(p^k-p^{k-1}}$$

۲ سوال ۲۷

پاسخ برابر با خیر است. به طور مثال $\mathbb{Z}_2$ را در نظر بگیرید. اگر فضای برداری V روی $\mathbb{Z}_2$ داشته باشیم، و v عضوی دلخواه از آن باشد، داریم:

$$0.v = 0$$

و از طرفی:

$$0.v = (1 + 1).v = 1.v + 1.v = v + v$$

پس باید $v + v = 0$ باشد. حال مجموعه‌ی $\{0, 1, 2, 3\}$ با عمل جمعی که همان عمل جمع اعداد صحیح در پیمانه‌ی ۴ باشد در نظر بگیرید. این یک گروه ۴ عضوی است که در آن داریم:

$$1 + 1 = 2 \neq 0$$

پس شرط $v + v = 0$ در آن برقرار نیست و نمی‌تواند یک فضای برداری روی $\mathbb{Z}_2$ باشد و مثال نقضی برای حکم شد.

۳ سوال ۲۸

۱.۳ اثبات وجود n

برای اثبات دنباله‌ی زیر را در نظر بگیرید: $a_0 = 0$ و $a_i = a_{i-1} + 1; i > 0$ چون میدان متناهی است، دنباله‌ی $\{a_i\}_0^\infty$ دارای عضو تکراری است. فرض کنید $a_x = a_y, y > x$ باشد. پس $a_y = a_x + 1 + 1 + ... + 1 = a_x + n$ که تعداد یک‌ها برابر با $y - x$ تاست و $n = y - x = 1 + 1 + ... + 1$ تعریف می‌کنیم. پس $a_x = a_x + n$ حال داریم:

$$0 = a_x+(-a_x) = (a_x+n)+(-a_x) = (n+a_x)+(-a_x) = n+(a_x+(-a_x)) = n+0 = n$$

که n جمع n تا عدد یک است طبیعی بوده و برابر با صفر است، پس چنین n ای وجود دارد.

۲.۳ اثبات اول بودن

۱.۲.۳ لم

اگر یک میدان داشته باشیم $a.b = 0$ آنگاه یا $a = 0$ یا $b = 0$ است.

اثبات: اگر $a = 0$ باشد که لم حل است، اگر $a \neq 0$ پس

$$b = 1.b = (a^{-1}.a).b = a^(-1).(a.b) = a^{-1}.0 = 0$$

و در نتیجه $b = 0$ است.

۲.۲.۳ مسئله‌ی اصلی

کوچک‌ترین n طبیعی را در نظر بگیرید، ثابت می‌کنیم این n اول است، برای این‌کار از برهان خلف استفاده می‌کنیم، با فرض اول نبودن n اعداد طبیعی $1 < a, b < n$ وجود دارد که $n = a.b$ باشد. پس:

$$0 = n = a.b$$

و طبق لم یکی از a و b صفر اند که این با کوچکترین بودن n در تناقض است پس فرض خلف باطل و n اول است.

۳.۳ اثبات فضای برداری بودن روی $\mathbb{Z}_n$

برای این‌کار تنها کافی‌است $x.v = (1 + 1 + ... + 1).v = v + v + ... + v$ که جاهایی که سه نقطه گذاشتم تعداد xتاست، تعریف کنیم، حال بررسی می‌کنیم که همه‌ی احکام برقرار است:

$$\begin{aligned}(st).v = v + v + ... + v \text{ (st times)} &= \\ (v + v + ... + v(\text{t times})) + ... + (v + v + ... + v(\text{t times}))(\text{s times}) &= \\ (t.v) + ... + (t.v)(\text{s times}) = s.(t.v)\end{aligned}$$

$$\begin{aligned}1.v &= v \\ t.(v + u) = (v + u) + ... + (v + u)(\text{t times}) &= \\ (v + v + ... + v(\text{t times})) + (u + ... + u(\text{t times})) &= t.v + t.u\end{aligned}$$

$$\begin{aligned}(s + t).v = v + v + ... + v(\text{s+t times}) &= \\ (v + ... + v(\text{s times})) + (v + ... + v(\text{t times})) &= s.v + t.v\end{aligned}$$

پس احکام مربوط به جمع و ضرب اسکالر هم برقرار شد و فضا برداری شد.

۴.۳ اثبات تعداد اعضا برابر با p^k بودن

حال طبق بخش‌های قبل مشخصه‌ی میدان عددی اول مانند p است و این میدان یک فضای برداری روی $\mathbb{Z}_p$ است و طبق بخش الف اگر بعد آن k باشد دارای p^k عضو است.

۴ سوال ۲۹

اگر $n = 1$ باشد حکم بدیهی است.
حال فرض کنید $n \geq 2$ است، دوتا از زیرفضاها را V و U به‌نامید و اشتراک آن‌ها را X بنامید. حال طبق قضیه‌ی رابطه‌ی بعد ها داریم: $\dim(V+U) = \dim(V) + \dim(U) - \dim(V \cap U) =$ $k+k-(k-1) = k+1$ پس اگر فقط دو زیرفضا هم داشتیم حکم برقرار است. حال فرض کنید $n > 2$ است و زیرفضا دیگری مانند W در نظر بگیرید. $W \cap V = X, W \cap U = Y$ را در نظر بگیرید. اگر $X = Y$باشد داریم: $W \cap V \cap U = X$ و حکم برقرار است. حال اگر $X \neq Y$ باشد، هر کدام از X, Y دارای $k-1$ بعد اند و چون مساوی نیستند اشتراک آن‌ها حداکثر بعد $k-2$ دارد، پس $\dim(X+Y) = \dim(X) + \dim(Y) - \dim(X \cap Y) \geq k-1+k-1-k+2 = k$ است و چون $X + Y \subseteq W$ است و $\dim(W) = k$ است پس $W = X + Y$ همچنین چون $X \subset V, Y \subset U \to X+Y \subset V+U$ است و در نتیجه $W \subseteq V+U$ است. پس در این حالت نیز همه در فضای $k+1$ بعدی قرار دارند. حال اگر $n > 3$ بود، با انتخاب Wهای متفاوت یکی از دو نتیجه‌ی بالا برای هر ۳ تایی به دست می‌آید که به سادگی می‌توان به این نتیجه رسید که یا اشتراک همه برابر است یا همه در یک فضای $k+1$بعدی قرار دارند.

۵ سوال ۳۰

تنها با فرض اینکه V دارای تولید متناهی است سوال را حل کرده و فرض می‌کنیم $\dim(V) = n$.

برای اثبات این مسئله از برهان خلف استفاده می‌کنیم، فرض کنید مجموعه‌ی S از زیرفضاهای اکید فضای V روی میدان F داشته باشیم که $|S| < |F|$ است و $\bigcup_{T \in S} T = V$ باشد.
حال ادعا می‌کنیم هر مجموعه‌ی متناهی در نظر بگیریم، زیرمجموعه‌ی یکی از اعضای S است و در نتیجه پایه‌ی V نیز زیرمجموعه‌ی یکی از اعضای S بوده و در نتیجه آن عضو V را تولید می‌کند و زیرفضای اکید نیست و این با فرض مسئله در تناقض است و فرض خلف باطل و حکم ثابت می‌شود.
تنها کافی‌ست ادعایی را که کردیم ثابت کنیم.
برای اثبات ادعا روی تعداد عضوهای مجموعه استقرا می‌زنیم استقرا می‌زنیم.
اگر مجموعه یک عضوی باشد، چون اجتماع برابر با کل شده‌است، پس این عضو در یکی از مجموعه‌ها قرار دارد و این مجموعه‌ی یک عضوی زیر مجموعه‌ی آن مجموعه است.
حال فرض کنید حکم را برای همه‌ی مجموعه‌های کمتر از k عضوی ثابت کرده‌اند.
یک مجموعه‌ی k عضوی دلخواه مثل T را در نظر بگیرید و اعضای آن را $t_1, ..., t_k$ بنامید. حال مجموعه های $\{t_1, ..., t_{n-1} + rt_n\}$ را در نظر بگیرید، به ازای هر کدام از این مجموعه‌ها طبق فرض استقرا (چون $k-1$ عضوی اند) یک عضو از S وجود دارد که زیرمجموعه‌ی آن است و چون تعداد این مجموعه‌ها $|F|$ و تعداد اعضای مجموعه کمتر از $|F|$ است پس دو مثل $\{t_1, ..., t_{n-1} + rt_n\}$ و

از اعضای مجموعه‌ی X زیرفضایی مانند $\{t_1, ..., t_{n-1}+r't_n\}$ وجود دارند که هردو زیرمجموعه‌ی S باشند. پس : $t_{n-1} + rt_n \in X, t_{n-1} + r't_n \in X \to t_{n-1} + rt_n - t_{n-1} - r't_n \in X \to (r - r')t_n \in X \to t_n \in X$ پس $\{t_1, ..., t_{n-1}, t_n\} \subset X$ و حکم ثابت شد.

۶ سوال ۳۱

برای اثبات وجود از حکم سوال ۳۰ استفاده می‌کنیم، برای ساختن ماتریس ابتدا یک پایه از میدان F^n را انتخاب کرده و n ستون اول این ماتریس قرار می‌دهیم. حال هر $n-1$ ستون از این ماتریس را انتخاب کنیم یک پایه برای زیرفضا از فضای F^n است، چون این زیرفضاها زیرفضای اکید فضای F^n اند، اجتماع همه‌ی این زیرفضاها را در نظر بگیرید، چون متناهی هستند، طبق قضیه‌ی سوال قبل حداقل یک بردار مانند v وجود دارد که در آن نیست، این بردار را ستون جدید این ماتریس قرار می‌دهیم و به همین نحو ادامه می‌دهیم، یعنی در مرحله‌ی iام $n+i-1$ ستون ساخته شده‌است که هر n ستون، مستقل خطی هستند. پس هر $n-1$ تا ستون در نظر بگیریم یک زیرفضای اکید از F^n است، چون تعداد ستون‌های $n-1$ تایی برابر با $\binom{n+i-1}{n-1}$ در این مرحله است، پس تعداد آن‌ها متناهی و طبق حکم سوال قبل اجتماع آن‌ها شامل کل فضا نمی‌شود، پس برداری مانند v_i وجود دارد که در این اجتماع نیست، v_i را به عنوان ستون جدید این ماتریس اتخاذ می‌کنیم. چون v_i در هیچ کدام از زیرفضاها با پایه‌ی $n-1$ تا ستونی نبوده، پس با توسط ترکیب خطی‌ای از آن‌ها ساخته نمی‌شود و تشکیل مجموعه‌ی مستقل خطی می‌دهد. پس با این روند می‌توانیم ماتریس را بسازیم.