רשימת משפטים למבחן מבנים.

1. לכל מספר שלם a ולכל מספר חיובי b מתקיים
א. קיימים מספרים שלמים r ו q כך ש

$$a = bq + r, 0 \le r < b$$

ב . ישנו זוג יחיד של המספרים r ו q שמקיימים את א'.

3. יהיו a, b שני שלמים שלפחות אחד מהם שונה מאפס. אז קיימים מספרים שלמים x, y כך ש- $ax + by = \gcd(a, b)$.

4. איבר $[a]_n \in \mathbf{Z}_n$ יהיה הפיך אם ורק אם $\gcd(a, n) = 1$.

5. חוג $\mathbf{Z}_n$ יהיה שדה אם ורק אם n מספר ראשוני.

6. תת-קבוצה $H \ne \emptyset$ תהיה תת-חבורה אם ורק אם היא מקיימת: $\forall a \in H\ \forall b \in H \quad ab^{-1} \in H$.

7. יהי $f: G \to H$ הומומורפיזם של חבורות. אז
א. $f(e_G) = e_H$.
ב. $\forall g \in G \quad f(g^{-1}) = (f(g))^{-1}$.
ג. $\forall g \in G \quad \forall n \in \mathbf{Z} \quad f(g^n) = (f(g))^n$.

8. יהי $f: G \to H$ הומומורפיזם של חבורות:

א. תהי K חבורה חלקית של G. אז התמונה $f(K)$ היא חבורה חלקית של H.
ב. תהי L חבורה חלקית של H. אז התמונה ההפוכה $f^{-1}(L)$ היא חבורה חלקית של G.

9. תהי H תת-חבורה כלשהי של חבורה G. אז:
*1. $\forall g \quad g \in g * H$
*2. $g_1 \in g_2 * H \Leftrightarrow g_1 * H = g_2 * H$.
3. $\forall g_1\ \forall g_2 \quad (g_1 * H = g_2 * H) \vee (g_1 * H \cap g_2 * H = \emptyset)$.
4. $\forall g \quad |g * H| = |H|$.

10. תהי H תת-חבורה כלשהי של חבורה סופית G. אז $[G:H]=\frac{|G|}{|H|}$.

11. אם $H \le G$ ו G חבורה סופית, אז $|H|$ מחלק את $|G|$.

א. נתון איבר g של החבורה G בעל סדר אינסופי אז השוויון $g^m = g^n$ מתקיים אם ורק אם $m=n$.

ב. נתון איבר g של החבורה G בעל סדר k אז השוויון $g^m = g^n$ מתקיים אם ורק אם $k\,|\,(m-n)$.

ג. נתון איבר g של החבורה G בעל סדר k אז $o(g^m)=\frac{k}{\gcd(k,m)}$.

12.

13. אם $g \in G$ איבר מסדר סופי, אז $|<g>|=o(g)$ ו $<g>=\{g^0, g^1, ..., g^{o(g)-1}\}$..

14. כל חבורה מסדר ראשוני ציקלית.

15. יהי $g \in G$ איבר כלשהו. אז

א. אם $o(g)=\infty$ אז $(<g>,*) \cong (\mathbf{Z},+)$.

ב. אם $o(g)=n<\infty$ אז $(<g>,*) \cong (\mathbf{Z}_n,+)$.

16. כל תת-חבורה של חבורה ציקלית היא גם חבורה ציקלית.

17. אם $f(x), g(x) \in F[x]$ שני פולינומים כלשהם, $g(x) \neq 0(x)$, אז קיימים שני פולינומים יחידים $q(x), r(x) \in F[x]$ כך ש:

$$f(x)=q(x)g(x)+r(x), 0 \le \deg(r(x)) < \deg(g(x))$$

18. נתונים שני פולינומים $f(x), g(x) \in F[x]$, , אז קיימים שני פולינומים $a(x), b(x) \in F[x]$ כך ש:

$$a(x)f(x)+b(x)g(x)=\gcd(f(x),g(x)).$$

19. נתון פולינום $f(x) \in F[x]$. אז קימים פולינומים בלתי פריקים $p_1(x), ..., p_n(x) \in F[x]$ כך שמתקיים $f(x) = p_1(x) * ... * p_n(x).$. כמו כן ההצגה יחידה. אם $f(x) = p_1(x) * ... * p_n(x) = q_1(x) * ... * q_m(x).$ גם כן הצגה אז חיב להתקים m=n וכמו כן לכל $i, 1 \le i \le n$ קים $j, 1 \le j \le m = n$ כך ש $\frac{p_i(x)}{q_j(x)} = const.$.