Password Entropy

Password entropy is a measurement of how unpredictable a password is.
The formula for entropy is:

$E = \log_2\left(R^L\right)$

where $E =$ password entropy, $R =$ pool of unique characters,
and $L =$ number of characters in your password.

Then $R^L =$ the number of possible passwords and

$\log_2\left(R^L\right) =$ the number of bits of entropy.

E stands for "entropy," which is the opposite of an ordered pattern. Entropy is good: the bigger the E, the harder a password is to crack.

We calculate password entropy by first looking at the pool of characters a password is made from.
For example, the password **password** would have a possible pool of 26 characters from the English alphabet.
Changing the password to **Password** would increase your pool to 52 characters. I made a table below to outline the rest.

Type	Pool of Characters Possible
Lowercase	26
Lower & Upper Case	52
Alphanumeric	36
Alphanumeric & Upper Case	62
Common ASCII Characters	30
Diceware Words List	7,776
English Dictionary Words	171,000

Password strength is determined with this chart:

- < 28 bits = Very Weak; might keep out family members
- 28 - 35 bits = Weak; should keep out most people, often good for desktop login passwords
- 36 - 59 bits = Reasonable; fairly secure passwords for network and company passwords
- 60 - 127 bits = Strong; can be good for guarding financial information
- 128+ bits = Very Strong; often overkill

While a password with 40-50 bits of entropy may be semi-safe now, it is only a matter of time until GPUs become more powerful, and password cracking takes less time!

Here is an example:

If your keyboard has 95 unique characters and you are randomly constructing a password from that whole set, then R = 95.
If you have a 12-character password, then L = 12.
The number R to the L power is 540,360,087,662,636,962,890,625 -- which is how many passwords you have.
That's the same as $2^{78.9}$ -- and the $\log_2$ of that is 78.9. In info-security lingo, it's 78.9 bits of entropy. That approaches the "exponential wall," where a password could take ages to crack.

Now calculate password entropy for the following passwords:

_____ 1. password
R = 26 since its pool of characters is just the 26 lower case letters
and L = 8 (the length)

_____ 2. Password

_____ 3. qwerty

_____ 4. abc123

_____ 5. MrP*MathPage
R = 82 since it uses upper and lower case and ASCII characters

_____ 6. 123456

_____ 7. starwars

_____ 8. Baseball

_____ 9. P33e=7a*E6m

_____ 10. Q77a&-2kB4R2

_____ 11. If the password entropy of an eight character password is 34.9 bits,
what is the pool of characters?

_____ 12. If the password entropy of a twelve character password is 55.7 bits,
what is the pool of characters?