1. Let G be a finite group of order n. Every conjugacy class of G has size dividing n, and $\{e\}$ is a 1-element conjugacy class. (a) The conjugacy classes have sizes 1 and $n-1$ with $n-1 \mid n$, so $n = 2$ and $G \cong \mathbb{Z}_2$. (b) The conjugacy classes have sizes $1 \le c_2 \le c_3$ with $c_2, c_3 \mid n$ and $n = 1 + c_2 + c_3$. If G is abelian, then $1 = c_2 = c_3$, so $|G| = 3$ and $G \cong \mathbb{Z}_3$. Assume G is nonabelian. Then $c_3 > 1$, so $c_3 < n < 3c_3$, and $c_3 \mid n$ implies that $n = 2m$ for some $m \in \mathbb{N}$ and $c_3 = m$. Hence $c_2 = n - 1 - c_3 = 2m - 1 - m = m - 1$, and $m - 1 = c_2 \mid n = 2m = 2(m-1) + 2$ implies $m - 1 \mid 2$, so $m = 2$ or $m = 3$. The case $m = 2$ is impossible, because then $|G| = n = 2m = 4$, and G must be abelian. Thus, $m = 3$ and $|G| = n = 2m = 6$, so $G \cong D_3 \cong S_3$, and S_3 indeed has exactly 3 conjugacy classes.

2. (a) See Lec.Notes 04/28. (b) Since $S_4 = HV$, $H \cap V = \{\mathrm{id}\}$, and $H \cong S_3$ we get from the Diamond Isomorphism Theorem that $S_4/V = HV/V \cong H/(H \cap V) = H/\{e\} \cong H \cong S_3$.

3. (a) For every $a \in G$, $O_H(a) = \{ha : h \in H\} = Ha$. (b) By the Orbit-Stabilizer Theorem, $|O_H(a)| = |H|/|H_a|$ for every $a \in G$ where $H_a = \{h \in H : ha = a\}$. Since $ha = a$ implies that $h = haa^{-1} = aa^{-1} = e$, we get $H_a = \{e\}$. Thus, $|Ha| = |O_H(a)| = |H|/|H_a| = |H|/1 = |H|$. (c) Since the orbits of H partition G, part (a) implies: the right cosets of H partition G. Part (b) says: all right cosets of H have the same size as H. Thus, we get Lagrange's Theorem for the right cosets of H: $|G| = |H| \cdot (\text{number of right cosets of } H)$.

4. Let $|H| = p^h m_H$, $K = p^k m_K$ with $p \nmid m_H, m_K$; so $|H \times K| = p^{h+k} m_H m_K$ with $p \nmid m_H m_K$. By Sylow's 1st Thm, H, K have Sylow p-subgroups P_H, P_K, respectively. Since $P_H \times P_K$ is a subgroup of $H \times K$ and $|P_H| = p^h$, $|P_K| = p^k$, we see that $P_H \times P_K$ is a Sylow p-subgroup of $H \times K$. Every other Sylow p-subgroup P of $H \times K$ is conjugate to $P_H \times P_K$ by Sylow's 2nd Thm. Hence, $P = (a,b)(P_H \times P_K)(a,b)^{-1} = (aP_Ha^{-1}) \times (bP_Kb^{-1})$ for some $a \in H$, $b \in K$, where aP_Ha^{-1} and bP_Kb^{-1} are Sylow p-subgroups of H and K, respectively.

5. (a) $\varphi(R)$ is a subring of S for every homomorphism $\varphi\colon R \to S$. Thus, if φ is unital, then $1_S = \varphi(1_R) \in \varphi(R)$, so 1_S is an identity element in $\varphi(R)$, because it is an identity element in S. Conversely, if 1_S is an identity element in $\varphi(R)$, then it must be that $1_S = \varphi(1_R)$, because $\varphi(1_R)$ is also an identity element in $\varphi(R)$ (as $\varphi(1_R)\varphi(r) = \varphi(1_R r) = \varphi(r)$ and $\varphi(r)\varphi(1_R) = \varphi(r1_R) = \varphi(r)$ for all $r \in R$), and hence $1_S = 1_S\varphi(1_R) = \varphi(1_R)$. (b) Follows from part (a), because $\varphi(R) = S$ implies that 1_S is an identity element in $\varphi(R)$.

6. (a) $f = (x^2+1)^2$ and $f \nmid x^2 + 1$, therefore $x^2 + 1 + (f)$ is a nonzero element of $R = \mathbb{Z}_3[x]/(f)$, but $(x^2 + 1 + (f))(x^2 + 1 + (f)) = f + (f) = 0 + (f)$ is the zero element of R. (b) Let $g = x^2 + x - 1\,(\in \mathbb{Z}_3[x])$. It can be checked by the Euclidean Algorithm that $\gcd(f,g) = 1$. Hence, there exist $s, t \in \mathbb{Z}_3[x]$ such that $fs + gt = 1$. Thus, $1 + (f) = fs + gt + (f) = gt + (f) = (g + (f))(t + (f))$ which shows that $t + (f)$ is a multiplicative inverse of $g + (f)$ (cf. proof of Thm 2 in Lec.Notes 4/26). (c) s and t can be computed from the results of the Euclidean Algorithm on f, g: $s = 2x + 1$ and $t = x^3 + x^2 + 2x$. Hence the multiplicative inverse of $x^2 + x - 1 + (f) \in R$ is $x^3 + x^2 + 2x + (f) \in R$.

7. (a) $G = S_3$, $H = \{\mathrm{id},\ (1\,2)\}$. (b) D_4 and its subgroups $\langle r \rangle$ and $\langle r^2, j \rangle$. (c) No such example exists, since $77 = 7 \cdot 11$, 7 and 11 are primes, and $11 \not\equiv 1 \pmod 7$. (d) No such example exists, because G acts transitively on itself by left multiplication. (e) No such example exists, because $121 = 11^2$, and every group of order p^2 (p prime) is abelian. (f) No such example exists. Since p is odd, $|D_n| = 2n$ and $|\langle r \rangle| = n$ are divisible by the same powers of p. Hence a Sylow p-subgroup P of $\langle r \rangle$ is a Sylow p-subgroup of D_n. For every other Sylow p-subgroup $\bar{P}$ of D_n we have $\bar{P} = gPg^{-1}$ for some $g \in D_n$ (by Sylow's 2nd Thm). Since $\langle r \rangle \trianglelefteq D_n$, we get $\bar{P} = gPg^{-1} \le g\langle r \rangle g^{-1} = \langle r \rangle$. But the cyclic group $\langle r \rangle$ has a unique subgroup of order $|P|$, therefore $\bar{P} = P$. (g) See Lec.Notes 4.28.